This document is scheduled to be published in the Federal Register on 01/21/2021 and available online at **federalregister.gov/d/2020-27157**, and on **govinfo.gov**

53-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

45 CFR Parts 160 and 164

[Docket No.: HHS-OCR-0945-AA00]

RIN: 0945-AA00

Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement

AGENCY: Office for Civil Rights, Office of the Secretary, HHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The United States Department of Health and Human Services (HHS or "the Department") is issuing this Notice of Proposed Rulemaking (NPRM) to modify the Standards for the Privacy of Individually Identifiable Health Information (Privacy Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). These modifications address standards that may impede the transition to value-based health care by limiting or discouraging care coordination and case management communications among individuals and covered entities (including hospitals, physicians, and other health care providers, payors, and insurers) or posing other unnecessary burdens. The proposals in this NPRM address these burdens while continuing to protect the privacy and security of individuals' protected health information.

DATES: Comments due on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES:

You may submit comments to this proposed rule, identified by RIN 0945-AA00 by any of the following methods:

• *Federal eRulemaking Portal*. You may submit electronic comments at http://www.regulations.gov by searching for the Docket ID number HHS-OCR-

0945-AA00. Follow the instructions http://www.regulations.gov online for submitting comments through this method.

• *Regular, Express, or Overnight Mail*: You may mail comments to U.S. Department of Health and Human Services, Office for Civil Rights, Attention: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement NPRM, RIN 0945-AA00, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW, Washington, DC 20201.

All comments received by the methods and due date specified above will be posted without change to content to *http://www.regulations.gov*, including any personal information provided about the commenter, and such posting may occur before or after the closing of the comment period.

The Department will consider all comments received by the date and time specified in the **DATES** section above, but, because of the large number of public comments normally received on ***Federal Register*** documents, the Department is not able to provide individual acknowledgments of receipt.

Please allow sufficient time for mailed comments to be timely received in the event of delivery or security delays. Electronic comments with attachments should be in Microsoft Word or Portable Document Format (PDF).

Please note that comments submitted by fax or email and those submitted after the comment period will not be accepted.

Docket: For complete access to background documents or posted comments, go to http://www.regulations.gov and search for Docket ID number HHS-OCR-0945-AA00.

FOR FURTHER INFORMATION CONTACT: Marissa Gordon-Nguyen at (800) 368–1019 or (800) 537–7697 (TDD).

SUPPLEMENTARY INFORMATION:

The discussion below includes an executive summary, a description of the statutory and regulatory background of the proposed rule, a section-by-section discussion of the need for the proposed rule, a description of the proposed modifications, and a regulatory impact statement and other required regulatory analyses. The Department solicits public comment on all aspects of the proposed rule. The Department requests that persons commenting on the provisions of the proposed rule precede their discussion of any particular provision or topic with a citation to the section of the proposed rule being discussed.

TABLE OF CONTENTS

5. Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

6. Adjusting Permitted Fees for Access to PHI and ePHI

7. Notice of Access and Authorization Fees

8. Technical Change to General Rules for Required Business Associate Disclosures of PHI

9. Request for Comments

B. Reducing Identity Verification Burden for Individuals Exercising the Right of Access (45 CFR 164.514(h))

1. Current Provision and Issues to Address

2. Proposal

3. Request for Comments

C. Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management (45 CFR 160.103)

1. Current Provision and Issues to Address

2. Proposal

3. Request for Comments

D. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-level Care Coordination and Case Management (45 CFR 164.502(b))

1. Current Provision and Issues to Address

2. Proposal

3. Request for Comments

E. Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management that Constitutes Treatment or Health Care Operations (45 CFR 164.506)

1. Current Provisions and Issues to Address

2. Proposal

3. Request for Comments

F. Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances (45 CFR 164.502 and 164.510-514)

1. Current Provisions and Issues to Address

2. Proposals

3. Request for Comments

G. Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgment of Receipt, Establishing an Individual Right to Discuss the NPP with a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element (45 CFR 164.520)

1. Current Provision and Issues to Address

2. Proposal

3. Request for Comments

I. Executive Summary

A. Overview

In this notice of proposed rulemaking (NPRM), the Department proposes modifications to the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), issued pursuant to section 264 of the Administrative Simplification

provisions of title II, subtitle F, of HIPAA.[1] The Privacy Rule is one of several rules, collectively known as the HIPAA Rules,[2] that protect the privacy and security of individuals' medical records and other protected health information (PHI), *i.e.*, individually identifiable health information maintained or transmitted by or on behalf of HIPAA covered entities (*i.e*., health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses).

The proposals in this NPRM support the Department's Regulatory Sprint to Coordinated Care (Regulatory Sprint), described in detail below. Specifically, the proposals in this NPRM would amend provisions of the Privacy Rule that could present barriers to coordinated care and case management – or impose other regulatory burdens without sufficiently compensating for, or offsetting, such burdens through privacy protections. These regulatory barriers may impede the transformation of the health care system from a system that pays for procedures and services to a system of value-based health care that pays for quality care.

The Department, which delegated the authority to administer HIPAA privacy standards to the Office for Civil Rights (OCR), developed many of the proposals contained in this NPRM after careful consideration of public input received in response to the Department's December 2018 *Request for Information on Modifying HIPAA Rules to Improve Coordinated Care* (2018 RFI).[3]

---

[1] Subtitle F of title II of HIPAA (Pub. L. 104-191,110 Stat. 1936 (August 21, 1996)) added a new part C to title XI of the Social Security Act, Pub. L. 74-271, 49 Stat. 620 (August 14, 1935), (*see* sections 1171–1179 of the Social Security Act, 42 U.S.C. 1320d–1320d–8)), as well as promulgating section 264 of HIPAA (codified at 42 U.S.C. 1320d-2 note), which authorizes the Secretary to promulgate regulations with respect to the privacy of individually identifiable health information. The Privacy Rule has subsequently been amended pursuant to the Genetic Information Nondiscrimination Act (GINA), title I, section 105, Pub. L. 110-233, 122 Stat. 881 (May 21, 2008) and the Health information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 123 Stat. 226 (February 17, 2009).

[2] *See also* the HIPAA Security Rule, 45 CFR Parts 160 and 164, Subparts A and C, the HIPAA Breach Notification Rule, 45 CFR Part 164, Subpart D, and the HIPAA Enforcement Rule, 45 CFR Part 160, Subparts C, D, and E.

[3] 83 FR 64302 (December 14, 2018).

B. Summary of Major Provisions

The Department proposes to modify the Privacy Rule to increase permissible disclosures of PHI and to improve care coordination and case management by:

- Adding definitions for the terms electronic health record (EHR) and personal health application.
- Modifying provisions on the individuals' right[4] of access to PHI by:
    - strengthening individuals' rights to inspect their PHI in person, which includes allowing individuals to take notes or use other personal resources to view and capture images of their PHI;
    - shortening covered entities' required response time to no later than 15 calendar days (from the current 30 days) with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension);
    - clarifying the form and format required for responding to individuals' requests for their PHI;
    - requiring covered entities to inform individuals that they retain their right to obtain or direct copies of PHI to a third party when a summary of PHI is offered in lieu of a copy;
    - reducing the identity verification burden on individuals exercising their access rights;
    - creating a pathway for individuals to direct the sharing of PHI in an EHR among covered health care providers and health plans, by requiring covered health care providers and health plans to submit an

[4] Under the HIPAA Privacy Rule, and in this NPRM, an individual's rights generally include the ability of the individual's personal representative to exercise those rights on the individual's behalf. *See* 45 CFR 164.502(g).

individual's access request to another health care provider and to receive back the requested electronic copies of the individual's PHI in an EHR;

- requiring covered health care providers and health plans to respond to certain records requests received from other covered health care providers and health plans when directed by individuals pursuant to the right of access;
- limiting the individual right of access to direct the transmission of PHI to a third party to electronic copies of PHI in an EHR;[5]
- specifying when electronic PHI (ePHI) must be provided to the individual at no charge;
- amending the permissible fee structure for responding to requests to direct records to a third party; and
- requiring covered entities to post estimated fee schedules on their websites for access and for disclosures with an individual's valid authorization[6] and, upon request, provide individualized estimates of fees for an individual's request for copies of PHI, and itemized bills for completed requests.

- Amending the definition of health care operations to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitute health care operations.
- Creating an exception to the "minimum necessary" standard for individual-level care coordination and case management uses and disclosures. The

[5] This proposed rule uses the terms "electronic copies" and "in an electronic format" interchangeably.
[6] This proposed rule uses the term "authorization" to refer to an authorization under 45 CFR 164.508.

minimum necessary standard generally requires covered entities to limit uses and disclosures of PHI to the minimum necessary needed to accomplish the purpose of each use or disclosure. This proposal would relieve covered entities of the minimum necessary requirement for uses by, disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management activities with respect to an individual, regardless of whether such activities constitute treatment or health care operations.

- Clarifying the scope of covered entities' abilities to disclose PHI to social services agencies, community-based organizations, home and community based service (HCBS) providers,[7] and other similar third parties that provide health-related services, to facilitate coordination of care and case management for individuals.
- Replacing the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on their "professional judgment" with a standard permitting such uses or disclosures based on a covered entity's good faith belief that the use or disclosure is in the best interests of the individual. The proposed standard is more permissive in that it would presume a covered entity's good faith, but this presumption could be overcome with evidence of bad faith.

---

[7] For purposes of this proposed rule, the Department refers to home and community-based services (HCBS) providers as they are described and referenced in the context of the Medicaid program. *See* generally 42 CFR part 441 subparts G, K, and M. *See also* National Quality Forum stating that HCBS "refers to an array of services and supports delivered in the home or other integrated community setting that promote the independence, health and well-being, self-determination, and community inclusion of a person of any age who has significant, longer-term physical, cognitive, sensory, and/or behavior health needs." "Quality in Home and Community Based Service to Support Community Living: Addressing Gaps in Performance Measurement Final Report" (September 2016), available at https://www.qualityforum.org/Publications/2016/09/Quality_in_Home_and_Community-Based_Services_to_Support_Community_Living__Addressing_Gaps_in_Performance_Measurement.aspx. .

- Expanding the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current stricter standard which requires a "serious and imminent" threat to health or safety.
- Eliminating the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP).
- Modifying the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.
- Expressly permitting disclosures to Telecommunications Relay Services (TRS) communications assistants for persons who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, and modifying the definition of business associate to exclude TRS providers.
- Expanding the Armed Forces permission to use or disclose PHI to all uniformed services, which then would include the U.S. Public Health Service (USPHS) Commissioned Corps and the National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps.

The Department carefully considered the extent to which each proposed modification would impact privacy protections compared to the likely benefit of making PHI more available for coordination of care or case management. These and other considerations are fully described for each proposal below.

C. Effective and Compliance Dates

The effective date of a final rule would be 60 days after publication. Covered entities and their business associates would have until the "compliance date" to establish and implement policies and practices to achieve compliance with any new or modified standards. Except as otherwise provided, 45 CFR 160.105 provides that covered entities

and business associates must comply with the applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change. The Department previously noted that the 180-day general compliance period for new or modified standards would not apply where a different compliance period is provided in the regulation for one or more provisions.[8]

The Department believes that compliance with the proposed modifications should require no longer than the standard 180-day period provided in 45 CFR 160.105, and thus propose a compliance date of 180 days after the effective date of a final rule.[9] Accordingly, OCR would begin enforcement of the new and revised standards 240 days after publication of a final rule.

The Department requests comment on whether the 180-day compliance period is sufficient for covered entities and business associates to revise existing policies and practices and complete training and implementation. For proposed modifications that would be difficult to accomplish within the 180-day timeframe, the Department requests information about the types of entities and proposed modifications that would necessitate a longer compliance period, how much longer such compliance period would need to be to address such issues, as well as the complexity and scope of changes and the impact on entities and individuals of a longer compliance period.

D. Care Coordination and Case Management Described

On January 30, 2017, President Donald Trump issued Executive Order (EO) 13771, "Presidential Executive Order on Reducing Regulation and Controlling Regulatory

[8] *See* 78 FR 5566, 5569 (Jan 25, 2013).
[9] *See* 45 CFR 160.104(c)(1), which requires the Secretary to provide at least a 180-day period for covered entities to comply with modifications to standards and implementation specifications in the HIPAA Rules.

Costs,"[10] followed by EO 13777, "Enforcing the Regulatory Reform Agenda." These executive orders make clear "the policy of the United States to alleviate unnecessary regulatory burdens placed on the American people . . ."[11] In several public speeches, Secretary of Health and Human Services Alex M. Azar II identified the value-based transformation of the Nation's healthcare system as one of his top priorities for the Department, and described how it relates to a reduction of regulatory burden. In a 2018 speech to the Federation of American Hospitals, Secretary Azar committed to addressing "government burdens that may be getting in the way of integrated, collaborative, and holistic care for the patient, and of structures that may create new value more generally."[12] Secretary Azar also explained the need for regulatory reform in his remarks to the Better Medicare Alliance: "the barriers to effective coordination among providers are much steeper than just excessive paperwork. . . . Addressing these regulations that impede care coordination are part of a much broader regulatory reform effort at HHS."[13]

In support of this priority, HHS Deputy Secretary Eric D. Hargan explained, before the Joint Commission on May 29, 2019, that care coordination is a necessary component of achieving value-based care:

> It's about coordination, above all—we're focused on understanding how regulations are impeding coordination among providers that can provide better, lower cost patient care, and then reforming these regulations consistent with the laws and their intents. And, finally, it's about care. Regulating health care means

---

[10] Available at https://www.whitehouse.gov/presidential-actions/presidential-executive-order-reducing-regulation-controlling-regulatory-costs/.
[11] Available at https://www.govinfo.gov/content/pkg/FR-2017-03-01/pdf/2017-04107.pdf.
[12] Remarks on Value-Based Transformation to the Federation of American Hospitals, Alex M. Azar II, Federation of American Hospitals, March 5, 2018, available at https://www.hhs.gov/about/leadership/secretary/speeches/2018-speeches/remarks-on-value-based-transformation-to-the-federation-of-american-hospitals.html.
[13] Remarks on the Trump Administration Healthcare Vision, Secretary Alex M. Azar II, Better Medicare Alliance, July 23, 2019, available at https://www.hhs.gov/about/leadership/secretary/speeches/2019-speeches/remarks-on-the-trump-administration-healthcare-vision.html.

regulating some of the most intimate decisions and relationships in our lives—deciding where and when to seek health care, how to make decisions with our doctors and family members, and more.[14]

More recently, the Secretary praised the advancement of coordinated care with the publication of final rules on interoperability, access to health information, and certification of electronic health record technology. The Secretary stated, "These rules are the start of a new chapter in how patients experience American healthcare, opening up countless new opportunities for them to improve their own health, find the providers that meet their needs, and drive quality through greater coordination." [15] And, when announcing the publication of a final rule modifying regulations on the confidentiality of substance use disorder treatment records, the Secretary stated, "This reform will help make it easier for Americans to discuss substance use disorders with their doctors, seek treatment, and find the road to recovery."[16]

The Department intends for this proposed rule to support the full scope of care coordination and case management activities to further the Department's goal of achieving value-based health care. Although neither care coordination nor case management has a precise, commonly agreed upon definition, both refer broadly to a set of activities aimed at promoting cooperation among members of an individual's health care delivery team, including family members, caregivers, and community based organizations. To encompass these broad categories of activities, the Department offers a non-exhaustive list of examples for understanding care coordination and case management in the context of this

---

[14] *See* the full text of Deputy Secretary Hargan's remarks at https://www.hhs.gov/about/leadership/eric-d-hargan/speeches/remarks-to-the-joint-commission-board.html (May 29, 2019).
[15] *See* the full text of Secretary Azar's remarks at https://www.cms.gov/newsroom/press-releases/hhs-finalizes-historic-rules-provide-patients-more-control-their-health-data.
[16] *See* the full text of Secretary Azar's remarks available at https://www.hhs.gov/about/news/2020/07/13/health-privacy-rule-42-cfr-part-2-revised-modernizing-care-coordination-americans-seeking-treatment.html.

NPRM, rather than proposing limited definitions. The Department welcomes comment on the examples and descriptions herein and on any additional definitions, examples, or scenarios that would be helpful for regulated entities and the public to understand what constitutes care coordination and case management.

For example, the Department's Office of Inspector General (OIG), in conjunction with the Department, issued a proposed rule as part of the Department's Regulatory Sprint to Coordinated Care. Under proposed safe harbors for the anti-kickback statute, OIG proposes to define "coordination and management of care" as the "deliberate organization of patient care activities and sharing of information between two or more value-based enterprise (VBE) participants or VBE participants and patients, tailored to improving the health outcomes of the target patient population, in order to achieve safer and more effective care for the target population."[17]

Additionally, as noted by the Centers for Medicare & Medicaid Services (CMS) in a recent RFI, "care coordination is a key aspect of systems that deliver value."[18] As CMS describes in guidance on the Medicaid benefit for children and adolescents, "care coordination" includes a range of activities that link individuals to services and improve communication flow. The guidance states that the various definitions of this term share three key concepts: comprehensive coordination (involving coordination of all services, including those delivered by systems other than the health system), patient-centered coordination (designed to meet the needs of the patient), and access and follow-up (described as ensuring the delivery of appropriate services and information flow among providers and back to the primary care provider).[19] In 2019 CMS issued a fact sheet

---

[17] 84 FR 55694, 55762 (October 17, 2019).
[18] 83 FR 29524 (June 25, 2018).
[19] "Making Connections: Strengthening Care Coordination in the Medicaid Benefit for Children & Adolescents," Centers for Medicare and Medicaid Services, page 3 (September 2014), available at https://www.medicaid.gov/medicaid/benefits/downloads/epsdt-care-coordination-strategy-guide.pdf.

associated with the Medicaid health home benefit, which includes six mandatory core elements for access to and coordination of care: comprehensive care management, care coordination, health promotion, comprehensive transitional care and follow-up, individual and family support, and referral to community and social services. The term "case management" is defined in the Medicaid context for state plans as "services furnished to assist individuals, eligible under the (Medicaid) State plan who reside in a community setting or are transitioning to a community setting, in gaining access to needed medical, social, educational, and other services."[20] In the context of HCBS waivers, case management "usually entails (but is not limited to) conducting the following functions: evaluation and/or re-evaluation of level of care, assessment and/or reassessment of the need for waiver services, development and/or review of the service plan, coordination of multiple services and/or among multiple providers, linking waiver participants to other federal, state and local programs, monitoring the implementation of the service plan and participant health and welfare, addressing problems in service provision, and responding to participant crises."[21]

The Department's Agency for Healthcare Research and Quality (AHRQ) describes care coordination as "the deliberate organization of patient care activities between two or more participants (including the patient) involved in a patient's care to facilitate the appropriate delivery of health care services."[22] AHRQ describes a broad approach to care coordination as involving commonly used practices to improve health care delivery, including teamwork, care management, medication management, health information

---

[20] 42 CFR 440.169.

[21] "Instructions, Technical Guide and Review Criteria, Application for § 1915(c) Home and Community Based Waiver" (January 2019*)* available at https://www.nasddds.org/uploads/documents/Version3.6InstructionsJan2019.pdf.

[22] "Care Coordination, Quality Improvement, Agency for Healthcare Research and Quality" (2014)*,* available at https://www.ahrq.gov/research/findings/evidence-based-reports/caregaptp.html (citing McDonald KM, Sundaram V, Bravata DM, et al., "Closing the Quality Gap: A Critical Analysis of Quality Improvement Strategie*s*: Volume 7 – Care Coordination, Technical Reviews," No. 9.7, conducted for AHRQ (2007)).

technology, and patient-centered medical homes. AHRQ also describes a "specific care coordination" approach that closely aligns with individual patient needs. Examples include creating a proactive care plan, patient monitoring and follow-up, supporting patient self-management goals, and linking to community resources.[23]

Another frequently cited definition comes from the National Quality Forum (NQF), the consensus-based entity recognized by the Department, which defines "care coordination" as "a multidimensional concept that includes effective communication among healthcare providers, patients, families, and caregivers; safe care transitions; a longitudinal view of care that considers the past, while monitoring present delivery of care and anticipating future needs; and the facilitation of linkages between communities and the healthcare system to address medical, social, educational, and other support needs that align with patient goals."[24]

Definitions of "case management" are equally varied. The Case Management Society of America (CMSA) defines case management as "a collaborative process of assessment, planning, facilitation, care coordination, evaluation and advocacy for options and services to meet an individual's and family's comprehensive health needs through communication and available resources to promote patient safety, quality of care, and cost effective outcomes."[25] The American Case Management Association (ACMA) describes case management in hospital and health care systems as "a collaborative practice model including patients, nurses, social workers, physicians, other practitioners, caregivers and

---

[23] *Ibid*.

[24] "Care Coordination Endorsement Maintenance Project 2016-2017," available at http://www.qualityforum.org/Projects/c-d/Care_Coordination_2016-2017/Care_Coordination_2016-2017.aspx, discussing a multi-phased effort to provide guidance and measurement of care coordination activities, including endorsing a 2006 definition of care coordination as "a function that helps ensure that the patient's needs and preferences for health services and information sharing across people, functions, and sites are met over time." See the full definition at https://www.tnaap.org/documents/nqf-definition-and-framework-for-measuring-care-co.pdf.

[25] "What Is A Case Manager?" Case Management Society of America *(2017),* available at http://www.cmsa.org/who-we-are/what-is-a-case-manager/.

the community." The ACMA's approach to case management encompasses communication and seeks to facilitate care along a continuum through effective resource coordination. The goals of case management include the achievement of "optimal health, access to care and appropriate utilization of resources, balanced with the patient's right to self-determination."[26]

II. Statutory Authority[27] and Regulatory History

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA Rules

The Administrative Simplification provisions of HIPAA provide for the establishment of national standards to protect the privacy and security of individuals' health information and established civil money and criminal penalties for violations of the requirements, among other provisions.[28] Under HIPAA, the Administrative Simplification provisions originally applied to three types of entities, known as "covered entities": health care providers who transmit health information electronically in connection with any transaction for which the Department has adopted an electronic transaction standard, health plans, and health care clearinghouses.[29] As discussed more fully below, through a

---

[26] "Definition of Case Management," American Case Management Association, available at https://www.acmaweb.org/section.aspx?sID=4.

[27] While not relevant to this rulemaking, the Department also has authority to modify the Privacy Rule under GINA.

[28] *See* 42 U.S.C. 1320d-1 – 1320d-9. With respect to privacy standards, Congress directed HHS to "address at least the following: (1) The rights that an individual who is a subject of individually identifiable health information should have. (2) The procedures that should be established for the exercise of such rights. (3) The uses and disclosures of such information that should be authorized or required." 42 U.S.C. 1320d-2 note.

[29] *See* 42 U.S.C. 1320d-1 (applying administrative simplification provisions to covered entities).

subsequent statute and its implementing regulations, some of the provisions of the Privacy Rule now also directly apply to the business associates[30] of covered entities.[31]

The Department issued its first regulation to implement HIPAA, the Privacy Rule, on December 28, 2000.[32] The Department has modified the Privacy Rule several times since then to address new statutory requirements and to strengthen, refine, or add flexibility to privacy requirements in specific circumstances.[33]

The Privacy Rule protects individuals' medical records and other individually identifiable health information created, received, maintained, or transmitted by or on behalf of covered entities, which are collectively defined as PHI. The Privacy Rule protects individuals' PHI by regulating the circumstances under which covered entities and their business associates may use or disclose PHI and by requiring covered entities to have safeguards in place to protect the privacy of PHI. As part of these protections, covered entities are required to have contracts or other arrangements in place with business associates that use PHI to perform functions for or on behalf of, or provide services to, the covered entity and that require access to PHI to ensure that these business associates also protect the privacy of PHI. The Privacy Rule also establishes the rights of individuals with respect to their PHI, including the right to receive adequate notice of a covered entity's privacy practices, the right to request restrictions of uses and disclosures, the right to access (*i.e.,* to inspect and obtain a copy of) their PHI, the right to request an amendment of their PHI, and the right to receive an accounting of disclosures.[34]

---

[30] A business associate is a person, other than a workforce member, that performs certain functions or activities for or on behalf of a covered entity, or that provides certain services to a covered entity involving the disclosure of PHI to the person. *See* 45 CFR 160.103.
[31] *See* 42 U.S.C. 17934 and HHS Office for Civil Rights Fact Sheet on Direct Liability of Business Associates under HIPAA, (May 2019), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.
[32] 65 FR 82462 (December 28, 2000).
[33] *See* 67 FR 53182 (August 14, 2002), 78 FR 5566 (January 25, 2013), 79 FR 7289 (February 6, 2014) and 81 FR 382 (January 6, 2016).
[34] *See* 45 CFR 164.520, 164.522, 164.524, 164.526 and 164.528.

The Department established the right of individuals to access their PHI in the 2000 Privacy Rule,[35] 45 CFR 164.524, "Access of individuals to protected health information." Section 164.524 included requirements for timely action by covered entities, form and format of copies, the denial of access, and documentation. Certain provisions, such as the requirement for covered entities to provide individuals access to PHI in the form or format requested by the individual if readily producible, and the permission for covered entities to impose a reasonable, cost-based fee for copies, were expanded through the subsequent enactment of the HITECH Act and the 2013 Omnibus Final Rule modifying the Privacy Rule (the 2013 Omnibus Rule).[36]

OCR has delegated authority from the Secretary to make decisions regarding the implementation, interpretation, and enforcement of the Privacy Rule. Under this authority, OCR also administers and enforces the Security Rule, which requires covered entities and their business associates to implement certain administrative, physical, and technical safeguards to protect ePHI; and the Breach Notification Rule, which requires covered entities to provide notification to affected individuals, the Secretary of HHS, and, in some cases, the media, following a breach of unsecured PHI, and requires a covered entity's business associate that experiences a breach of unsecured PHI to notify the covered entity of the breach.

With respect to the HIPAA Enforcement Rule, which contains provisions addressing compliance, investigations, the imposition of civil money penalties for violations of the HIPAA Rules, and procedures for hearings, OCR also acts based on its delegated authority.

B. The Health Information Technology for Economic and Clinical Health (HITECH) Act and the 2013 Omnibus Rule

[35] 65 FR 82462 (December 28, 2000).
[36] 78 FR 5566 (January 25, 2013).

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009,[37] enacted February 17, 2009, is designed to promote the widespread adoption and standardization of health information technology (health IT). Subtitle D of title XIII, entitled "Privacy," contains amendments to sections 1176 and 1177 of the Social Security Act designed to strengthen the privacy and security protections established under HIPAA. These provisions extended the applicability of certain Privacy Rule requirements and all of the Security Rule requirements to the business associates of covered entities; required HIPAA covered entities and business associates to provide for notification of breaches of unsecured PHI (implemented by the Breach Notification Rule); established new limitations on the use and disclosure of PHI for marketing and fundraising purposes; prohibited the sale of PHI; required consideration of whether a limited data set can serve as the minimum necessary amount of information for uses and disclosures of PHI; and expanded individuals' rights to access electronic copies of their PHI in an EHR, to receive an accounting of disclosures of their PHI with respect to ePHI, and to request restrictions on certain disclosures of PHI to health plans. In addition, subtitle D strengthened and expanded HIPAA's enforcement provisions.

Section 13405(e) of the HITECH Act strengthened the Privacy Rule's right of access with respect to covered entities that use or maintain an EHR. Under Subtitle D of Title XIII of the HITECH Act, "The term "electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."[38] The HITECH Act does not define the term "clinician." Section 13405(e) provides that when a covered entity uses or maintains an EHR with respect to PHI of an individual, the individual shall have a right to

---

[37] Pub. L. 111-5, 123 Stat. 115 (February 17, 2009) (codified at 42 U.S.C. 201 note).
[38] *See* 42 U.S.C. 17921(5), definition of "Electronic health record."

obtain from the covered entity a copy of such PHI in an electronic format, and that the individual may direct the covered entity to transmit such copy directly to the individual's designee, provided that any such choice is clear, conspicuous, and specific. Section 13405(e) also provides that any fee imposed by the covered entity for providing such an electronic copy shall not be greater than the entity's labor costs in responding to the request for the copy.

On July 14, 2010, the Department issued an NPRM to modify the HIPAA Rules consistent with the HITECH Act (2010 NPRM).[39] Among other changes, the 2010 NPRM proposed to modify the Privacy Rule to address individual access rights to certain electronic PHI, including proposed requirements with respect to the form, format, and manner of access requested; the ability of the individual to direct a copy to a designee; and fee limitations for providing the requested access. In the 2010 NPRM, the Department acknowledged that section 13405(e) of the HITECH Act "applies by its terms" only to PHI in EHRs.[40] However, the Department proposed to rely on its broad statutory authority under HIPAA section 264(c) to issue regulations expanding the HITECH Act requirements to avoid "a complex set of disparate requirements for access" such as different requirements for access to paper versus electronic records.[41] The Department further explained its proposed implementation of the HITECH Act provisions:

> As such, the Department proposes to use its authority under section 264(c) of HIPAA to prescribe the rights individuals should have with respect to their individually identifiable health information to strengthen the right of access as provided under section 13405(e) of the HITECH Act more uniformly to all protected health information in one or more designated record sets

[39] *See* 75 FR 40868 (July 14, 2010).
[40] 75 FR 40868, 40901 (July 14, 2010).
[41] *Ibid.*

electronically, regardless of whether the designated record set is an electronic health record.[42]

The 2013 Omnibus Rule finalized 45 CFR 164.524(c)(2)(ii), providing that if the individual's requested PHI is maintained in one or more designated record sets[43] "electronically", and if the individual requests an electronic copy, the covered entity must provide the individual with access to his or her PHI in the electronic form and format requested by the individual if it is readily producible in such form and format.[44] Alternatively, if the form and format of the PHI are not readily producible, the covered entity must provide the PHI in a readable electronic form and format as agreed to by the covered entity and individual.[45] The Department also noted that the Privacy Rule, as first finalized in 2000, already applied the right of access to PHI held in designated record sets, and required a covered entity to provide the PHI in the "form and format" requested by the individual, including electronically, if "readily producible."[46]

The 2013 Omnibus Rule also finalized 45 CFR 164.524(c)(3)(ii) providing that covered entities must transmit a copy of an individual's PHI directly to a third party designated by the individual if the individual's request for access directs the covered entity to do so.[47] The Department noted that, in contrast to other access requests by individuals pursuant to 45 CFR 164.524, requests to transmit a copy of PHI to a third party must be in writing, signed by the individual, and clearly identify the designated third party and where

---

[42] *Ibid*.
[43] A "Designated record set" is defined as (1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. 45 CFR 164.501.
[44] 78 FR 5566, 5633 (January 25, 2013).
[45] *Ibid*.
[46] *Ibid.*
[47] *Id*. at 5634.

to send the copy of the PHI. In finalizing this provision, the Department cited section 13405(e) of the HITECH Act and section 264(c) of HIPAA, and stated that the finalized provision was consistent with its prior interpretation and would apply without regard to whether the PHI was in electronic or paper form.[48]

With respect to fees for access, the 2000 Privacy Rule permitted a covered entity to impose only a reasonable, cost-based fee for a copy of PHI under the right of access, which was limited to: (1) the costs of supplies and labor for copying; (2) postage to mail the copy; and (3) preparation of a summary or explanation of PHI if agreed to by the individual.[49] As noted above, section 13405(e)(2) of the HITECH Act provided that, where a covered entity uses or maintains an EHR, any fee for providing electronic copies (or summary or explanation) of PHI shall not be greater than the entity's labor costs in responding to the request. Therefore, to implement the fee provisions of the HITECH Act, the 2013 Omnibus Rule amended 45 CFR 164.524(c)(4) to provide that fees could include, in addition to postage and preparation of a summary or explanation when applicable, only the following: (i) labor for copying the PHI requested by the individual, whether in paper or electronic form; and (ii) supplies for creating the paper or electronic media if the individual requested the PHI be provided on portable format.[50]

In the 2013 Omnibus Rule, the Department described the labor for copying PHI, whether in paper or electronic form, as one factor that may be included in a reasonable, cost-based fee.[51] It also noted that rather than propose more detailed considerations for this factor in regulatory text, it retained all prior interpretations of labor with respect to paper copies – that is, that the labor cost of copying does not include costs associated with searching and retrieval of requested PHI.[52] For example, labor for copying PHI may

---

[48] *Ibid*.
[49] *See Id*. at 5635.
[50] *Id*. at 5635-36.
[51] *Id*. at 5636.
[52] *Ibid*.

include the labor necessary to reproduce and transfer the PHI in the form and format and manner requested or agreed to by the individual, such as by converting electronic information in one format to the format requested by or agreed to by the individual, or transferring electronic PHI from a covered entity's data system(s) to portable electronic media or e-mail. The Department also explained that the reorganization and addition of the phrase "electronic media" reflected its understanding that section 13405(e)(2) of the HITECH Act allowed for the inclusion of only labor costs in the fee for electronic copies, and by implication, excluded costs for supplies that are used to create the electronic copy (*e.g.*, computers, scanners). Finally, the Department explained that its interpretation of the HITECH Act would permit a covered entity to charge a reasonable and cost-based fee for any electronic media it provided, as requested or agreed to by an individual.[53]

In 2016, to educate the public about the individual right of access and clarify covered entities' obligations to fulfill this right, OCR issued extensive guidance (2016 Access Guidance) on how OCR interprets and implements 45 CFR 164.524. The 2016 Access Guidance comprises a comprehensive fact sheet and a set of frequently asked questions (FAQs) that provide additional detail.[54]

Among other clarifications, the guidance included the Department's interpretation and intention that, as an expansion of the individual right of access, the right to direct a copy of PHI to a third party incorporated the general access right's pre-existing conditions and requirements, including its fee limitations. Accordingly, the guidance expressly stated that the access fee limitation applied, regardless of whether the individual requested that the copy of PHI be sent to the individual, or directed the copy of PHI to a third party designated by the individual.

---

[53] *Ibid.*

[54] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html for the full text of the 2016 Access Guidance.

On January 23, 2020, by memorandum opinion and order in *Ciox Health, LLC v. Azar, et al*. (*Ciox v. Azar*),[55] the U.S. District Court for the District of Columbia vacated: (1) the Department's expansion of the HITECH Act's "third-party directive" (*i.e.,* the right of an individual to direct a copy of PHI to a third party) beyond requests for an electronic copy of PHI in an EHR; and (2) the extension of the individual "patient rate" for fees for copies of PHI directed to third parties. More specifically, the court held that 45 CFR 164.524(c)(3)(ii), as added to the Privacy Rule by the 2013 Omnibus Rule, exceeded the statutory authority in section 13405(e)(2) of the HITECH Act, which granted a limited right to individuals to direct a copy of ePHI in an EHR to a third party in an electronic format. Further, the court ruled that the Department impermissibly broadened the application of the access fee limitation (known as the "patient rate") to apply to copies of PHI directed to third parties, insofar as the Department failed to subject this requirement, first expressly stated in the 2016 Access Guidance, to notice and comment rulemaking.

Consistent with the court's opinion, which the Department did not appeal, the Department takes the opportunity of this NPRM to seek public comment on proposals to: (1) narrow the scope of the access right to direct records to a third party to only electronic copies of PHI in an EHR; and (2) apply new fee limitations to the access right to direct a copy of PHI to a third party, as described more fully below.

C. 21st Century Cures Act

The 21st Century Cures Act (Cures Act)[56] was enacted on December 13, 2016, to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes. The Cures Act added certain provisions to the Public Health Service Act

---

[55] No. 18-cv-0040-APM (D.D.C. January 23, 2020).
[56] Pub. L. 114-255, 130 Stat. 1033 (December 13, 2016) (codified at 42 U.S.C. 201 note). Cures Act Title IV – Delivery amended the PHSA, 42 U.S.C. 201 et seq.

(PHSA)[57] relating to health IT.[58] While the Department is not proposing a rule under the Cures Act in this NPRM, the proposals in this NPRM take into consideration certain provisions of the Cures Act that facilitate the exchange of health information, and thus provide helpful context for this rulemaking. Section 4004 of the Cures Act added section 3022 of the PHSA (42 U.S.C. 300jj–52), the "information blocking" provision. Section 3022(a)(1) defines information blocking as a "practice that, except as required by law or specified by the Secretary pursuant to rulemaking, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." The definition of information blocking also includes two different knowledge requirements. If a practice is conducted by a health IT developer, exchange, or network, the definition requires that such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage access to, exchange of, or use of, electronic health information. If a practice is conducted by a health care provider, the definition requires that such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access to, exchange of, or use of, electronic health information. Section 3022(a)(1)(A) excludes from the definition of information blocking practices that are required by law, and reasonable and necessary activities identified by the Secretary in rulemaking.

The Office of the National Coordinator for Health Information Technology (ONC) published a final rule[59] that implements the statutory definitions of the information blocking provision and finalizes the proposed eight reasonable and necessary activities (referred to as exceptions) that do not constitute information blocking for purposes of the

---

[57] 42 U.S.C. 201 et seq.
[58] *See generally* Cures Act sections 4003 Interoperability (amending section 3000 of the PHSA (42 U.S.C. 300jj)); and 4004 Information Blocking (amending Subtitle C of title XXX of the PHSA by adding 42 U.S.C. 300jj-52).
[59] *See* 85 FR 25642 (May 1, 2020) available at https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-07419.pdf.

definition set forth in section 3022(a)(1). These regulatory exceptions are finalized in the ONC rule, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" (ONC Cures Act Final Rule), and include the Privacy Exception, which expressly applies to a practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy when the practice meets all of the requirements of at least one of the sub-exceptions in 45 CFR 171.202.[60]

Based on authority granted to it by the Cures Act, the OIG has proposed a rule that addresses enforcement.[61] Section 3022(b)(1) of the PHSA authorizes OIG to investigate any claim that a health IT developer of certified health IT or other entity offering certified health IT, a health care provider, or a health information exchange or network, engaged in information blocking. Section 3022(b)(2)(A) provides for civil monetary penalties for a health IT developer of certified health IT or other entity offering certified health IT, as well as for a health information exchange or network, that is determined to have committed information blocking. Section 3022(b)(2)(B) of the PHSA provides that any health care provider that is determined to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking. The OIG's proposed rule would codify these authorities.[62]

The Cures Act also requires health IT developers participating in the ONC Health IT Certification Program[63] (Certification Program) to publish application programming

---

[60] *See* 45 CFR 171.202.
[61] *See* proposed rule, 85 FR 22979 (June 23, 2020). Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules. https://www.federalregister.gov/d/2020-08451/p-17.
[62] *Ibid.*
[63] In general, the HITECH Act provides the National Coordinator with the authority to establish a program or programs for the voluntary certification of health IT, and requires the Secretary to adopt certification criteria. *See* 42 U.S.C. 300jj-11.

interfaces (APIs) and allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.[64] ONC's Cures Act rule carries out this charge.

For example, by requiring developers of certified health IT, including EHR technology, to make secured, standards-based APIs (certified APIs) available, ONC's rule creates mechanisms by which individuals can readily exercise their Privacy Rule right of access, thus empowering individuals to electronically access, share, and use their electronic health information. This approach gives individuals the ability to electronically access and share their health information with mobile applications of the individuals' choice. Likewise, CMS's new interoperability rule contains requirements similar to the ONC Cures Act Final Rule.[65] Finally, section 4006 of the Cures Act directs ONC and OCR to jointly promote patient access to health information in a manner that would ensure the information is available in a form convenient for the patient, in a reasonable manner, without burdening the health care provider involved.

Taken together, implementation of the above Cures Act requirements through the ONC and CMS rules will support covered entities (and their business associates) that use health information technology in a manner that enables them to respond more timely to individual requests for access to ePHI. Further, the ONC Cures Act Final Rule requirements for certified health IT to use secure, standards-based APIs will allow individuals to more readily access their ePHI and support disclosures of PHI by covered health care providers and health plans for individual-level care coordination and case management purposes. This regulatory context informs the proposals that follow.

---

[64] *See* Cures Act section 4002 (amending section 3001(c)(5) of the PHSA).
[65] *See* 85 FR 25510 (May 1, 2020).

III. Need for the Proposed Rule and Proposed Modifications

In light of ongoing concerns that regulatory barriers across the Department impede effective delivery of coordinated, value-based health care, in June 2018, the Department launched the Regulatory Sprint to Coordinated Care to promote care coordination and facilitate a nationwide transformation to value-based health care. The Department initiated the Sprint by publishing a series of RFIs to solicit public input on regulatory barriers to coordinated care that it should modify, remove, or clarify through guidance and subsequent proposed regulations. After considering public comment, on August 26, 2019, the Department published a NPRM to modify 42 CFR Part 2, the regulatory scheme protecting the confidentiality of substance use disorder (SUD) treatment information held by HHS-funded treatment programs.[66] On October 17, 2019, the HHS Office of Inspector General (OIG) published a NPRM, "Revisions to the Safe Harbors Under the Anti-Kickback Statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements."[67] On the same day, CMS published a NPRM, "Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations."[68]

This NPRM, proposing modifications to the Privacy Rule, continues the Department's Regulatory Sprint, taking into consideration public comment received on the 2018 RFI published by OCR. The 2018 RFI solicited public input on 53 questions asking whether and how the Department could modify the HIPAA Rules to support care coordination and case management, and promote value-based care, while preserving the privacy and security of PHI. The Department organized the 2018 RFI questions around several key themes for which it sought input and examples of how best to address care coordination through three specific content areas:

---

[66] 84 FR 44568 (August 26, 2019).
[67] 84 FR 55694 (October 17, 2019).
[68] 84 FR 55766 (October 17, 2019).

- *Promoting information disclosure for care coordination and case management.* The 2018 RFI sought input on individuals' right to access their own PHI in accordance with the provisions contained in 45 CFR 164.524, and the amount of time covered entities should be permitted to respond to individuals' requests for access. The RFI also solicited input on whether health care clearinghouses should be subject to the individual access requirements, and whether disclosures of PHI for care coordination and case management to non-provider covered entities should be excepted from the minimum necessary requirements. Further, the RFI asked for public input on whether the Privacy Rule should require covered entities and business associates to disclose PHI when requested by another covered entity for treatment, payment, health care operations, or some combination or subset of these categories of disclosures. Finally, the RFI asked whether there should be an express regulatory permission for HIPAA covered entities to disclose PHI to social services agencies and/or community based organizations.
- *Promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness (SMI).* The 2018 RFI sought input to help determine whether and how to modify the Privacy Rule to address the opioid crisis and SMI, and promote family involvement in the care of loved ones experiencing these health situations. The RFI also sought comment on how the Department could amend the Privacy Rule to increase the disclosure of information by providers to family members experiencing difficulties obtaining health information about parents, spouses, minor and adult children, and other loved ones when needed to coordinate their care or otherwise be involved in their treatment (or the payment for such treatment).
- *Notice of Privacy Practices (NPP).* The 2018 RFI sought input on whether the Department should eliminate or modify the Notice of Privacy Practices signature

and recordkeeping requirements associated with distribution of the Notice of Privacy Practices. The Privacy Rule, at 45 CFR 164.520(c)(2)(ii), currently requires a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain a written acknowledgment of receipt of the provider's NPP; if unable to obtain the written acknowledgment, the covered health care provider must document its good faith effort to do so and the reason for not obtaining an individual's acknowledgment, and maintain the documentation for six years.[69] The 2018 RFI sought public comment on whether changing the requirements related to the acknowledgment of receipt could reduce administrative burden on covered health care providers and address confusion about the purpose and effect of the requirements. The 2018 RFI also asked whether and how other aspects of the Notice of Privacy Practices provisions (*e.g.*, content requirements) could be changed to ensure that individuals are informed about their rights and covered entities' privacy practices.

In addition to the three major topics described above, the RFI sought information about implementing a requirement of the HITECH Act to include disclosures by a covered entity for treatment, payment, and health care operations through an EHR in an accounting of disclosures.[70] Based on the comments received in response to the 2018 RFI, and the history of previous rulemaking on this topic, the Department intends to address this requirement in future rulemaking.

The Department received over 1,300 comments in response to the 2018 RFI, from many types of individuals and entities, including covered entities, patients, family caregivers, professional associations, privacy advocates, mental health professionals and advocates, business associates, researchers, and government organizations. The

---

[69] *See* 45 CFR 164.520(e) and 45 CFR 164.530(j)(2).
[70] *See* 42 U.S.C. 17935(c).

Department provides a more complete description of the 2018 RFI topics and responsive comments below.[71]

A. Individual Right of Access[72] (45 CFR 164.524)

General Policy Considerations

The ability of individuals to access and direct disclosures of their own health information is key to the coordination of their care. Patients are at the center of each health care encounter. As such, 45 CFR 164.524 of the Privacy Rule generally requires HIPAA covered entities (health plans and most health care providers)[73] to provide individuals, upon request, with access to their PHI in one or more designated record sets maintained by or for the covered entity. As finalized in 2013, this right includes the right to inspect or obtain a copy, or both, of the PHI, and to access the PHI in the form and format requested if readily producible. Individuals have a right to access this PHI for as long as the information is maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained on paper or in an electronic system onsite, remotely, or archived; or where the PHI originated (*e.g.*, from the covered entity, another health care provider, the patient, etc.). The individual right to inspect PHI held in a designated record set, either in addition to obtaining copies or in lieu thereof, requires covered entities to arrange with the individual for a convenient time and place to inspect the PHI. The right of access also

---

[71] Throughout this preamble, the phrases "majority of commenters" or "general consensus" are used to mean a majority of commenters that have commented on the particular issue or consensus among commenters who have commented on the issue being discussed. These statements should not be interpreted to mean all commenters who have commented on the 2018 RFI, but only those who commented on the particular issue being discussed.

[72] Throughout this NPRM, references to the individual right of access and individual access requests include access requests by the personal representative of an individual.

[73] The third type of covered entity, a health care clearinghouse, is not subject to the same individual access requirements as covered health care providers and health plans. *See* 45 CFR 164.500(b)(1) for a list of Privacy Rule provisions that apply to a health care clearinghouse in its role as a business associate of another covered entity.

includes the right to direct the covered entity to transmit an electronic copy of PHI in an EHR to a designated person or entity of the individual's choice.[74]

While OCR has issued extensive guidance and performed outreach to the public and regulated entities regarding the individual right of access, OCR continues to hear—through complaints, comments on the 2018 RFI, reports,[75] and anecdotal accounts—that individuals frequently face barriers to obtaining timely access to their PHI, in the form and format requested, and at a reasonable, cost-based fee. Associated delays or lack of patient access to their PHI may inhibit care coordination and contribute to worse health outcomes for individuals,[76] and contribute to burden on individuals and systems.

The 2018 RFI also requested information about current barriers or delays that health care providers face when attempting to obtain PHI from covered entities for treatment purposes. Specifically, the RFI asked whether the Privacy Rule could be modified to improve care coordination and case management by requiring covered entities and business associates to disclose PHI when requested by another covered entity for treatment purposes, for payment and health care operations purposes generally, or, alternatively, only for specific payment or health care operations purposes. The RFI further requested input on the effects of various potential requirements, including the creation of unintended burdens for covered entities or individuals, how much it would cost covered entities to comply, and whether any limitations should be placed on such disclosure requirements.

---

[74] In accordance with the court order in *Ciox v. Azar*, the Department is not enforcing a right to direct to a third party non-electronic copies of PHI or copies of PHI that are not in an EHR. These types of disclosures to third parties continue to be permitted with a valid authorization.

[75] Lye CT, Forman HP, Gao R, et al. "Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records." JAMA Network Open. Published online October 05, 2018(6):e183014. doi:10.1001/jamanetworkopen.2018.3014.

[76] *See e.g.*, The Joint Commission, "Transitions of Care: The need for collaboration across entire care continuum," https://www.jointcommission.org/assets/1/6/TOC_Hot_Topics.pdf (listing transfer of health information as foundational to safe transitions of care); Hesselink, G., Schoonhoven, L., Barach, P., Spijker, A., Gademan, P., Kalkman, C., Liefers, J., Vernooij-Dassen, M., & Wollersheim, H. (2012). "Improving patient handovers from hospital to primary care: a systematic review." ANNALS OF INTERNAL MEDICINE, 157(6), 417428.

After careful review of the responses to the 2018 RFI and the Department's analysis of the current Privacy Rule, the Department proposes to amend the Privacy Rule to strengthen the individual right of access and to remove barriers that may limit or discourage coordinated care or case management among covered entities and individuals, or otherwise impose regulatory burdens. Additionally, consistent with the court's decision in *Ciox v. Azar,*[77] the Department proposes to modify aspects of the individual's right under the Privacy Rule to direct a covered entity to transmit a copy of PHI to a third party.

Summary of Proposals to Modify the Individual Right of Access

The Department proposes to amend the individual right of access by incorporating definitions into the Privacy Rule that are necessary to implement key privacy provisions of the HITECH Act. The Department's proposed definitions for electronic health record and personal health application in 45 CFR 164.501 build on language from the HITECH Act definitions of electronic health record[78] and personal health record.[79] The Department also proposes to strengthen the individual right of access by strengthening the right to inspect and obtain copies of PHI and by shortening the time limits for covered entities to respond to access requests. The Department addresses requirements regarding the form and format in which covered entities must respond to individuals' requests for access, by clarifying that "readily producible" copies of PHI include copies of ePHI requested through secure, standards-based APIs using applications chosen by individuals, and that they also include

---

[77] No. 18-cv-0040-APM (D.D.C. January 23, 2020).

[78] 42 U.S.C. 17921(5): "The term "electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

[79] *Id.* at 17921(11): "The term "personal health record" means an electronic record of PHR identifiable health information (as defined in section 13407(f)(2) [of the HITECH Act]) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." Sec. 13407(f)(2) of the HITECH Act defines "PHR identifiable health information" as individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information (A) that is provided by or on behalf of the individual; and (B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. 42 U.S.C. 17937(f)(2).

copies in any form and format required by applicable state and other laws. The Department proposes that the individual right to direct a copy of PHI to a third party be limited to a right to direct an electronic copy of PHI in an EHR to a third party. To clearly distinguish between the scope and requirements of the individual right to inspect and obtain copies of PHI and the right to direct the transmission of electronic copies of PHI in an EHR to a third party, the Department proposes to list these distinct rights of access in separate paragraphs in the regulatory text:

- The individual right to inspect and obtain copies of PHI within the current rule requires covered entities to provide the requested information (with some exceptions) within a specific time limit and for a limited fee. This NPRM proposes to retain this individual right to inspect and obtain copies of PHI at 45 CFR 164.524(c).
- The right of an individual to direct the transmission of electronic copies of PHI in an EHR to a third party is established by the HITECH Act and interpreted by the *Ciox v. Azar* decision to apply only to PHI in an EHR. The proposed rule would codify the *Ciox v. Azar* limits into regulatory text at 45 CFR 164.524(d).
- The Department also proposes to create a pathway for individuals to direct the sharing of an electronic copy of PHI in an EHR among covered health care providers and health plans. The NPRM proposes to require a covered health care provider or health plan (the "Requestor-Recipient"), at the individual's direction, to submit the individual's access request regarding his or her own ePHI to another covered health care provider (the "Discloser"), requesting that the Discloser transmit the ePHI maintained by or on behalf of the Discloser in its EHR to the Requestor-Recipient. This new right would be inserted within the right to direct an electronic copy of PHI in an EHR to a third party, at proposed 45 CFR 164.524(d)(7).

Finally, with respect to fees charged by covered entities to individuals exercising the right of access, the Department proposes to adjust and clarify the fees that covered entities may charge for copies of PHI, and require covered entities to provide advance notice of approximate fees for copies of PHI requested under the access right or with an individual's valid authorization. The Department also proposes technical clarifications to the Privacy Rule provision requiring business associates to disclose PHI as needed for the covered entity to fulfill its obligations under the right of access.

1. Adding Definitions for Electronic Health Record or EHR and Personal Health Application" (45 CFR 164.501)

The Privacy Rule currently does not define the term "electronic health record." However, the HITECH Act codifies a definition of EHR that applies to that Act's privacy and security provisions for covered entities and business associates.[80] As part of this NPRM's proposal to modify the scope of the access right regarding PHI in an EHR, the Department proposes to add a definition of EHR in 45 CFR 164.501 that expands on the HITECH Act definition to clarify some of its terms:

> *Electronic health record* means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. Such clinicians shall include, but are not limited to, health care providers that have a direct treatment relationship with individuals, as defined at §164.501, such as physicians, nurses, pharmacists, and other allied health professionals. For purposes of this paragraph, "health-related information on an individual" covers the same scope

[80] *See* 42 U.S.C. 17921(5) for the HITECH Act definition: "The term "electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

of information as the term "individually identifiable health information" as defined at §160.103.

The Privacy Rule does not define the term "clinician" and the Department has not identified a uniform statutory or regulatory definition. For example, the term "clinician" is not included among the several definitions of "Health care provider" in the Social Security Act, which includes a long list of health care professionals as well as "any other person furnishing health care services or supplies."[81] Section 13101 of the HITECH Act, adding Title XXX – Health Information Technology and Quality to the PHSA, includes a definition for "health care provider" that appears to distinguish the term "clinicians" from other types of practitioners, but does not specify a basis for the distinction: ". . . and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary."[82] CMS offers a definition of "clinician" within its guidance materials discussing quality measures: "The term *clinician* refers to a healthcare professional qualified in the clinical practice of medicine. Clinicians are those who provide principal care for a patient where there is no planned endpoint of the relationship; expertise needed for the ongoing management of a chronic disease or condition; care during a defined period and circumstance, such as hospitalization; or care as ordered by another clinician. Clinicians may be physicians, nurses, pharmacists, or other allied health professionals."[83]

Consistent with the breadth of these various definitions, the Department proposes to interpret "authorized health care clinicians and staff" to at least include covered health care providers who are able to access, modify, transmit, or otherwise use or disclose PHI

---

[81] *See e.g.,* Social Security Act section 1171(3) (42 U.S.C. 1320d (3)) (defining "Health care provider" to include a provider of services (cross-referencing the definition with that in 42 U.S.C. 1861(u)), and any other person furnishing health care services or supplies.
[82] 42 U.S.C. 300jj (3), definition of "Health care provider".
[83] Available at https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/MMS/QMY-Clinicians.

in an EHR, and who have direct treatment relationships with individuals; and their workforce members (as workforce is defined at 45 CFR 160.103)[84] who support the provision of such treatment by virtue of their qualifications or job role. Accordingly, an EHR would include electronic records consulted by any covered health care provider, or a workforce member of such a covered health care provider, so long as the provider has a direct treatment relationship with individuals. The Department does not propose to include covered health care providers who have indirect treatment relationships with individuals. By definition, providers with indirect treatment relationships deliver health care based on the orders of another health care provider, and they typically provide services, products, or reports to another health care provider (*e.g.,* a provider with a direct treatment relationship with the individual).[85] Accordingly, the direct treatment provider that receives such services, products, or reports would be the entity documenting information in the EHR.

For example, an EHR would include electronic lab test reports created by workforce members of a large health system who are licensed clinical laboratory personnel, and who perform clinical lab tests for patients treated by the health system. Likewise, electronic billing records created, gathered, managed, and consulted by workforce members of a covered health care provider that has a direct treatment relationship with an individual (*e.g.*, a hospital) would be included in the term EHR because health care billing information is health-related information. The Department recognized as early as 2013 that many direct treatment providers use electronic practice systems that integrate functions such as scheduling and billing with providers' EHRs.[86] Additionally, the American Academy of Family Physicians, in presenting definitions for

---

[84] This NPRM uses the terms "workforce member" and "staff" interchangeably.
[85] *See* 45 CFR 164.501 (definition of "Direct treatment relationship").
[86] *See* Assistant Secretary for Planning and Evaluation (ASPE) report, "The Feasibility of Using Electronic Health Data for Research on Small Populations, Information Available in an Electronic Health Record" (September 1, 2013), available at https://aspe.hhs.gov/report/feasibility-using-electronic-health-data-research-small-populations.

both "electronic health record" and "electronic medical record," has noted that "electronic health record" refers to "computer software that physicians use to track all aspects of patient care. Typically this broader term also encompasses the practice management functions of billing, scheduling, etc."[87]

In contrast, the term EHR would not include health-related electronic records of covered health care providers that only supply durable medical equipment to other providers, who then provide the equipment to individuals, and thus do not have direct treatment relationships with individuals.

With respect to the types of information in an EHR, the Department proposes to equate "health-related information on an individual" in regulatory text with the scope of the familiar, defined term, individually identifiable health information or IIHI.[88] While the HITECH Act does not define "health-related information," section 13101 of the HITECH Act defines "health information" by reference to section 1171(4) of the Social Security Act, [89] which is consistent with the definition of the term contained in the Privacy Rule. Therefore, the Department believes it is reasonable to interpret the term "health-related information" to be at least as broad as "Health information," as defined in the Privacy Rule at 45 CFR 164.501.[90] The Department notes that "Health information" includes not

---

[87] *See* American Academy of Family Physicians (AAFP), "Introduction to Electronic Health Records (EHRs)" available at https://www.aafp.org/practice-management/health-it/product/intro.html.

[88] 45 CFR 160.103 provides in part that IIHI is "a subset of health information, including demographic information . . . created or received by a health care provider, health plan, employer or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual." *See* 45 CFR 160.103 for the full definition.

[89] *See* 42 U.S.C. 300jj (4) (adding section 3000(4) to the PHSA, definition of Health care provider).

[90] *Health information* means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. 45 CFR 164.501.

only clinical, but billing and other data. Therefore, the broader term "health-related information" could be expected to include such data and not be limited to clinical data.

Further, the Department interprets "on an individual," for HIPAA purposes to refer to information that is "individually identifiable." Health information that is not individually identifiable (*e.g.*, that is de-identified) is not protected by HIPAA. Thus, a definition of "health-related information on an individual" that encompasses information outside the scope of IIHI would not create an administrable standard under the HIPAA Rules. The Department seeks comment on the scope of this proposed definition for EHR, including billing records for health care.[91]

The Department also believes it is necessary to define a new term in the Privacy Rule, "Personal health application" (or "personal health app"), by drawing on the definition of a personal health record in the HITECH Act.[92] This term would be added to 45 CFR 164.501. More and more, individuals use personal health applications to access and manage their personal health information, and in this proposed rule, the Department proposes to revise the right of access to clarify that it includes the right of an individual to access electronic copies of the individual's PHI, and that one of the mechanisms by which a request for access can be fulfilled is by transmitting an electronic copy of an individual's PHI to a personal health application used by the individual. To support the Department's proposal to address the use of personal health applications in the right of access, the Department proposes to define personal health application in the HIPAA Rules as "an

---

[91] Note that the HITECH Act definition of "Electronic health record," 42 U.S.C. 17921(5), applies only to HIPAA covered entities and business associates. ONC's regulations at 45 CFR Subchapter D—Health Information Technology, do not define an EHR, but do include definitions for a *2015 Edition Base EHR* and a *Qualified EHR*. CMS has also proposed a definition of EHR in its proposed rule; *Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations.* S*ee* 84 FR 55766 (October 19, 2019), https://www.federalregister.gov/d/2019-22028/p-535.

[92] *See* 42 USC § 17921(11). "The term "personal health record" means an electronic record of PHR identifiable health information (as defined in section 17937(f)(2) of this title) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer."[93] Put another way, a personal health application is a service offered directly to consumers. The covered entity does not manage, share, or control the information, nor does the application developer manage the information on behalf of or at the direction of a health care provider or health plan (*e.g.,* through a patient "portal" that the entity uses to manage individuals' access to the PHI it maintains), or another party that collects or manages PHI for its own purposes (*e.g.,* a research organization). Instead, individuals (or their personal representatives) use a personal health application for the individuals' own purposes, such as to monitor their own health status and access their own PHI using the application. For example, individuals might request weight, vital signs, and other health information from their health care providers to either store it in the personal health application or to direct transmission to other persons. The Department notes that a personal health application is not acting on behalf of, or at the direction of a covered entity, and therefore would not be subject to the privacy and security obligations of the HIPAA Rules. However, the Department supports providing individuals with information that will assist them in making the best choices for themselves when selecting a personal health application or other applications that are not being provided on behalf of or at the direction of a covered entity.[94]

---

[93] This proposed definition of personal health application would not apply to or otherwise affect the requirements of the ONC Cures Act Final Rule or the CMS Interoperability and Patient Access Rule.

[94] *See* 85 FR 25642, 25814 (May 1, 2020) for an extensive discussion of how a covered entity may provide individuals with such information, in the ONC Cures Act Final Rule preamble regarding *Interference Versus Education When an Individual Chooses Technology to Facilitate Access.*

The Department requests comment on the proposed definition of personal health application, including the types of activities encompassed in the terms "managed," "shared," and "controlled," and on the Department's assumptions about the use of such applications by individuals. The proposed definition of personal health application is meant to be consistent with the HITECH Act definition of personal health record (PHR),[95] but specifically addresses certain health applications, which may or may not be PHRs.[96]

Taken together, the proposed definitions for EHR and personal health application would help clarify the proposed modifications to the right of access, including the scope of the modified right of individuals to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a designated third party.

---

[95] "[A]n electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." 42 U.S.C. 17921(11).

[96] The same software could be a personal health application under the proposed Privacy Rule definition and also be a personal health record under the HITECH Act for other purposes, to the extent it meets both definitions.

2. Strengthening the Access Right to Inspect and Obtain Copies of PHI

The individual right of access under the Privacy Rule includes a right to "inspect and obtain a copy of" PHI in a designated record set at 45 CFR 164.524(a)(1).[97] The Department proposes to strengthen the access right to inspect and obtain copies of PHI by incorporating a portion of the 2016 Access Guidance, discussed below, into a new provision of the Privacy Rule. To do so, the Department proposes to retain the substance of the current right at 45 CFR 164.524(a)(1), but redesignate current 45 CFR 164.524(a)(1)(i) and (ii) as 45 CFR 164.524(a)(1)(i)(A) and (B). The Department also proposes to add a new right at 45 CFR 164.524(a)(1)(ii) that generally would enable an individual to take notes, videos, and photographs, and use other personal resources to view and capture PHI in a designated record set as part of the right to inspect PHI in person. The Department does not propose to impose a requirement on covered entities that would result in the taking of an intellectual property right, and does not believe that an individual recording their own PHI in a designated record set through video, still camera photos, or audio recordings would be inconsistent with federal and state recording laws or intellectual property rights protections. However, the Department requests comment on this point and examples of possible unintended consequences of the proposal. Additionally, the Department invites comments on whether covered entities should be permitted to provide copies of PHI in lieu of in-person inspection of PHI when necessary to protect the health or safety of the individual or others, such as during a pandemic; and if so, whether the Department should establish additional rights for individuals in such circumstances, such as the right to receive such copies for free. The Privacy Rule currently does not provide covered entities with the opportunity to deny or delay (beyond 30 days plus one 30-day extension) the right to inspect PHI in person to prevent the spread of an infectious disease, or address the ability to provide a reasonable alternative based on the

[97] *See* 45 CFR 164.524(a).

need to protect the health or safety of the individual or others due to a pandemic or other public health emergency.

Under this proposal, covered entities generally would be required to allow individuals to take notes, videos, and photographs using personal resources after arranging a mutually convenient time and place for the individual to inspect their PHI in a designated record set, such as in a medical records office. This would be accomplished by redesignating the first paragraph of 45 CFR 164.524(a)(1) as subsection (i) and creating a new subsection (ii). Covered entities would be required to provide such access without imposing a fee under proposed 45 CFR 164.524(c)(4(ii). Additionally, the Department proposes to extend the right to inspect to situations where mutually convenient times and places include points of care where PHI in a designated record set is readily available for inspection by the patient, for example, by viewing x-rays, ultrasounds, or lab results in conjunction with a health care appointment with a treating provider. The Department anticipates that the time and place where an individual obtains health care treatment generally would be considered a convenient time and place for the individual to inspect the PHI that is immediately available in the treatment area. This provision would be added to 45 CFR 164.524(c)(3) as part of the implementation specifications regarding the time and manner of access, as follows: "When protected health information is readily available at the point of care in conjunction with a health care appointment, a covered health care provider is not permitted to delay the right to inspect."

In these circumstances, a covered health care provider would not be permitted to delay the right to inspect. The Department believes that it is common for individuals to take notes during a visit where health care treatment is provided and that individuals could benefit from taking photographs or recordings of PHI, contained in a designated record set, during such visits. This provision would not extend the right beyond the records

maintained by or for a covered entity as described in the definition of designated record set in the Privacy Rule.[98]

The Department seeks comment on whether to require covered health care providers to allow individuals to record PHI in this manner as part of the Privacy Rule access right; whether conditions or limitations should apply to ensure that a covered health care provider does not experience unreasonable workflow disruptions (*e.g.*, limitations on time spent recording PHI in conjunction with a health care appointment); any potential unintended consequences of a new requirement to allow inspection of PHI that is readily available at the point of care in conjunction with a health care appointment; and how to determine when PHI is "readily available."

Under proposed section 164.524(a)(1)(ii), the Department would not require a covered entity to allow the individual to connect a personal device, such as a thumb drive, to the covered entity's information systems. The Department does not expect a covered entity to tolerate unacceptable security risks (which would violate the HIPAA Security Rule) in order to accomplish a non-secure mode of data transfer to the requestor.[99]

The Department believes that the proposed changes would eliminate persistent barriers that individuals face when seeking to inspect or obtain copies of their PHI, as described above in Section III.A. At the same time, a provision at the end of the new subsection (ii) of 45 CFR 164.524(a)(1) would provide, "[A] covered entity is not required to allow an individual to connect a personal device to the covered entity's information systems and may impose requirements to ensure that an individual records only protected health information to which the individual has a right of access." Consistent with this provision, a covered entity could establish reasonable policies and safeguards to ensure,

---

[98] 45 CFR 164.501.

[99] *See* discussion of security considerations in the 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. *See also* 45 CFR 164.308(a)(1).

for example, that an individual's use of personal resources minimizes disruptions to the covered entity's operations, and is used in a way that enables the individual to copy or otherwise memorialize only the PHI in the individual's designated record set to which the individual is entitled pursuant to the right of access. However, a covered entity would not be permitted to establish such policies and safeguards that impose unjustified or unreasonable barriers to individual access. See proposed 45 CFR 164.524(b)(1)(ii).

3. Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access

a. Current Provisions and Issues to Address

Section 164.524(b)(1) of title 45 CFR requires a covered entity to permit an individual to inspect or to obtain a copy of PHI about the individual that is maintained in a designated record set, and to require individuals to make such a request in writing, provided the covered entity informs the individual of the writing requirement. Although the Department did not solicit commit in the 2018 RFI about this section of the Privacy Rule, the Department believes it is appropriate to solicit comment on a proposal to expressly prohibit a covered entity from imposing unreasonable measures that would impede an individual's right of access. The Department believes such a proposal would support the goal of improving coordination of care for individuals, as further discussed below.

Section 164.524(b)(2) of title 45 CFR requires a covered entity to act on an individual's request to exercise their right of access no later than 30 days after receipt of the request, with an option to extend the time to take action by an additional 30 days after providing written explanation and the date by which the entity will complete its action on the request. To assess whether the time limit could be shortened to better serve individuals seeking to exercise their right to access their records, in the 2018 RFI, the Department solicited public comments on this timeframe, the feasibility of covered entities meeting a

shorter time limit, recommended time limits, and whether access to PHI maintained by covered entities in electronic format should be subject to different timeliness requirements than non-electronic records (*e.g.*, paper).

Many commenters on the 2018 RFI preferred a uniform standard for providing access to PHI regardless of the record format (*e.g.*, electronic or non-electronic). Simplicity, consistency, and uniformity of requirements were cited as priorities above other considerations, such as differing technical capabilities with respect to different formats. Commenters cited numerous factors other than whether the information is in electronic or non-electronic form that affect a covered entity's ability to timely fulfill access requests, such as the nature of the requested information, whether the records are stored off-site, the need for professional or legal review based on state law or 42 CFR Part 2 requirements to segregate information that cannot be released at all or without authorization, and the size and complexity of the covered entity. Covered health care provider comments further described a number of factors that can affect access times for the production of electronic records, including PHI residing in multiple IT systems in varying formats and requests covering long periods of time, or covering a high volume of records related to complex and intensive medical treatment that must be collated and put into the requested electronic format or medium.

Citing these factors, health care providers who commented on this topic generally did not believe that requiring access to electronic records more quickly than non-electronic records would improve the overall speed of providing access to all of an individual's requested PHI, and some commenters expressed concern that doing so may negatively affect timely access to non-electronic records. To support this point, many described how fulfilling a single access request may encompass the production of both electronic and non-electronic records (sometimes referred to as a "hybrid" request or record). Commenters also reported that applying different time requirements for different parts of

an individual's record would add complexity, potentially creating additional administrative burdens and barriers to compliance.

Of the commenters who offered specific timeframes concerning current practices, about half reported providing records within 15 days and half stated that they take up to 30 days. Health care entities subject to shorter response times required under state law (including requirements in California and Texas)[100] commented that they are able to meet those shorter time limits. Also, among commenters providing a specific recommendation for shorter access time limits, the most suggested timeframe was 14 to 15 days, consistent with the deadlines in those states. Some commenters recommended prioritizing certain types of requests based on their purpose: two-thirds of organizational commenters who responded to this question stated that requests for continuity of care purposes or urgent medical needs should be prioritized.

Individual commenters described delays in obtaining access, including inconsistent or incomplete uploading of electronic records to health information exchanges, entities that routinely respond to access requests on day 29 with a demand for additional clarifying information in writing in order to process the requests, and entities that only respond when threatened with legal action. They also described the harmful effects on health when the process to access records is too complicated or when the provision of records is delayed or denied.

Examples from consumers included needing to repeat tests and procedures because medical history information was not available, which is both expensive and leads to delays in needed treatment; delayed referrals and inaccurate diagnoses based on incomplete information; and lack of timely information needed for self-care. Sometimes health decisions have to be made quickly, and individuals need access to information in a timely

---

[100] *See* Cal. Health & Safety Code 12110, Tex. Health & Safety Code 241.154 (hospitals), Tex. Occupations Code 159.006 (physicians), and Tex. Health & Safety Code 181.102 (other providers with an EHR).

manner to fully participate in their care or obtain an urgent second opinion from another medical professional.

Among commenters that opposed shorter timelines, many stated that covered entities would be burdened if they had to provide access within a shorter period. Several commenters stated that they would have to increase expenditures on staff, diverting resources from treating patients, and at least one mentioned the need to increase investment in information technology. Some commenters expressed particular concern that shorter access time limits would place an undue burden on smaller entities.

b. Proposals

To address the barriers to timely access described above, the Department proposes to modify the Privacy Rule as follows.

i. **Requests for Access**

Section 164.524(b) of title 45 CFR currently requires covered entities to permit individuals exercising their right of access to inspect or to obtain a copy of their PHI that is contained in a designated record set, and permits covered entities to require access requests in writing, provided that the covered entity informs the individual of that requirement. The Department proposes to modify the Privacy Rule to expressly prohibit a covered entity from imposing unreasonable measures on an individual exercising the right of access that create a barrier to or unreasonably delay the individual from obtaining access.[101] Specifically, in proposed new section 164.524(b)(1)(ii),[102] the Department proposes to clarify that, while an entity may require individuals to make requests for access in writing (as currently provided in the second sentence of section 164.524(b)(1)), it would not be permitted to do so in a way that impedes access.

---

[101]OCR previously addressed such unreasonable measures in guidance. *See* 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

[102] The Department would redesignate section 164.524(b)(1) as section 164.524(b)(1)(i) and move the second sentence of such provision, as redesignated, to section 164.524(b)(1)(ii).

To help define "unreasonable measures" for covered entities, the Department proposes to include and compare, in regulatory text, non-exhaustive specific examples of reasonable and unreasonable measures that some covered entities have imposed (as described in public comments or individuals' complaints submitted to the Department), or may be likely to impose. For example, proposed section 164.524(b)(1)(ii) compares a standard form containing the minimum information that is needed to process a request for access against a form requiring extensive information from the individual that is not necessary to fulfill the request; requiring the use of the form containing unnecessary information is an unreasonable measure. Other examples of unreasonable measures in the proposed regulatory text include requiring the individual to obtain notarization of the individual's signature, or accepting individuals' written requests only in paper form, only in person at the covered entity's facility, or only through the covered entity's online portal. Similarly, the Department proposes below to amend the Privacy Rule by adding section 164.514(h)(2)(v) to prohibit a covered entity from imposing an unreasonable identity verification requirement on an individual attempting to exercise the right of access, and includes examples of such measures.

The Department assumes a prohibition against "unreasonable measures" for requesting access would not result in adverse unintended consequences for individuals, but acknowledges that covered entities may have concerns about potential implementation burdens associated with this proposal. The Department solicits comment on its assumptions, and seeks examples of unreasonable measures that individuals and covered entities believe could reduce an individual's ability to participate in the coordination of his or her own healthcare. The Department also requests comment on burdens that covered entities believe may result from this proposed change.

ii. Timeliness

As noted above, the Privacy Rule generally requires covered entities to respond to requests by individuals to exercise their right of access no later than 30 days after receipt by either providing access or a written denial that meets certain requirements.[103] If the covered entity is unable to provide access or a written denial within 30 days, it may extend the allowable time by no more than an additional 30 days if the entity provides to the individual, within the initial 30-day time limit, a written statement of the reason for the delay and the expected completion date.[104]

The Department believes that entities can provide individuals access to their information within a time limit shorter than 30 days. Therefore, to strengthen the individual's right of access to their PHI in a designated record set, the Department proposes to modify section 164.524(b)(2)(i) and (ii) of the Privacy Rule to require that access be provided "as soon as practicable," but in no case later than 15 calendar days after receipt of the request, with the possibility of one 15 calendar-day extension. Where another federal or state law (*i.e.*, statute or regulation) requires a covered entity to provide an individual with access to the PHI requested in less than 15 calendar days, that shorter time limit would be deemed practicable within the meaning of the Privacy Rule under proposed new section 164.524(b)(2)(iii). The Department proposes, in new section 164.524(b)(2)(ii)(C), to also require covered entities to establish written policies for prioritizing urgent or other high priority access requests (especially those related to health and safety) so as to limit the need to use 15 calendar-day extensions for such requests.

At least eight states have statutory requirements to provide patients with copies of their health records in less time than the Privacy Rule's current 30-day limits, and at least

---

[103] 45 CFR 164.524(b)(2(i).
[104] *See* 45 CFR 164.524(b)(2)(ii)(A) and (B).

five states require the opportunity to view or inspect the record in fewer than 30 days.[105] These access laws primarily apply to health care providers, including hospitals and other health facilities, but not to health plans. Among these states, the requirements to provide copies range from 10 to 15 days.

The Department is strongly persuaded by these examples and by comments from entities operating in states with 10 to 15-day access provisions that, when mandated, covered entities are able to adapt to shorter access time limits. A majority of states do not impose time limits on health care entities that are as short as 15 days, so access to PHI in those states will be markedly improved. Additionally, these shorter timelines would better support the Department's initiatives to improve health care price transparency to empower and assist consumers with making more informed health care decisions. In support of these goals, the Administration has proposed and finalized other rules to require health insurance issuers and plans, as well as hospitals, to make health care prices more readily available to consumers in real-time. For example, in November 2019, CMS, along with the Internal Revenue Service, Department of the Treasury; and the Employee Benefits Security Administration, Department of Labor, proposed rules regarding transparency in coverage to give consumers real-time, personalized access to cost-sharing information. The proposed rules include a proposal for non-grandfathered health insurance plans and issuers in the individual and group markets to provide an estimate of participants', beneficiaries', and enrollees' cost-sharing liability for all covered health care items and services through an online self-service tool, or in paper form, upon request. The rule also

---

[105] *See e.g.,* California, Cal. Health & Safety Code 123110 (5 days to inspect; 15 days to receive a copy); Colorado, 6 Colo. Regs. 1011:1:II-5.2 (24 hours to inspect; 10 days to receive a copy); Hawaii, HRS 622.57 (10 days to receive a copy); Louisiana, LSA-R.S. 40:1165.1 (15 days to receive a copy); Montana, MCA 50-16-541(10 days, copy and inspect); Tennessee, TCA 63-2-101 (10 days to receive a copy); Texas, Tex. Health & Safety Code 241.154 (hosp.) (15 days, copy and inspect), Tex. Occupations Code 159.006 (physicians) (15 days to receive a copy), Tex. Health & Safety Code 181.102 (15 days to receive electronic copies), Tex. Admin. Code 165.2 (physicians) (15 days to receive a copy); and Washington, Wash. Rev. Code 70.02.080 (15 days, copy and inspect).

would require issuers and plans to disclose in-network provider negotiated rates and historical out-of-network allowed amounts through two machine-readable files posted on an internet website, thereby allowing the public, including personal health application developers (and other application developers that are not providing the application on behalf of or at the direction of a covered entity), to have access to health insurance coverage information.[106] In addition, CMS finalized a rule containing price transparency requirements for hospitals.[107] This rule provides that hospitals must publish on the web standard charges for certain items and services that could be delivered by the hospital to a patient, as well as display the price for bundled "shoppable" services that patients would likely schedule in advance, thereby informing the patient's selection of a hospital for scheduled procedures. [108] While many health plans have already provided pricing calculators as an online tool where individuals may access individualized estimates of out-of-pocket costs, not all individuals have equal access to or the ability to utilize internet resources. The proposed Privacy Rule modification would help address this gap in access by applying time limits to providing both electronic and non-electronic PHI the individual may need, such as health conditions and recommended treatment options, to conduct meaningful searches for pricing information. This proposed rule would extend and support the goals of these price transparency initiatives.

Therefore, the Department proposes to amend the individual access right provisions to require covered entities to provide copies of PHI as soon as practicable, but no later than 15 calendar days (with the possibility of one 15 calendar-day extension) or where another federal or state law requires a covered entity to provide an individual with

---

[106] *See* 84 FR 65464 (November 27, 2019).
[107] Medicare and Medicaid Programs: CY 2020 Hospital Outpatient PPS Policy Changes and Payment Rates and Ambulatory Surgical Center Payment System Policy Changes and Payment Rates; Price Transparency Requirements for Hospitals to Make Standard Charges Public, 84 FR 65524 (November 27, 2019).
[108] *Ibid*.

access to the PHI requested in less than 15 calendar days, that shorter time period will be deemed practicable under the Privacy Rule. The same timeliness requirements would be applied when an individual requests direct access under proposed 45 CFR 164.524(b)(2) and when an individual requests that an electronic copy of PHI in an EHR be directed to a third party under proposed 45 CFR 164.524(d)(5).

To limit compliance complexity, the Department proposes to uniformly apply this timeliness requirement, regardless of the form or format of the PHI (e.g., paper or electronic). The Department proposes to explicitly refer to calendar days as the units of time. The Department believes that the current 30-day limit is already understood to be calendar days, and the 2016 Access Guidance also uses the term "calendar days."[109] Thus, the proposed addition of the reference to calendar days would not be a material change, but a clarification.

The Department also proposes to add a requirement that a covered entity may use one 15-day extension of time for providing access to requested PHI if it has established a policy to address urgent or high-priority requests. This proposal is not intended to limit the use of extensions to urgent or high-priority requests, but to provide flexibility for entities that have this type of policy. The Department does not propose to define what constitutes an urgent or high priority request, and does not intend with this proposal to encourage covered entities to require individuals to reveal the purposes for their requests for access. However, examples of urgent or high priority requests could include when an individual voluntarily reveals that the PHI is needed in preparation for urgent medical treatment, or that the individual needs documentation of a diagnosis of severe asthma to be allowed to bring medication to school.

---

[109] *See* 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

Finally, the Department also proposes at 45 CFR 164.524(c)(3) to expressly provide that, while a covered entity may discuss aspects of the individual's access request with the individual before fulfilling the individual's request, such clarification of the request would not extend the time limit for providing access. This modification would put into regulatory language the Department's interpretation of the access deadlines in the 2016 Access Guidance[110] and help address situations described in public comments in which covered entities contact individuals for the first time near the end of the initial compliance deadline to discuss the request or obtain additional information, and then take unnecessary additional time beyond that initial deadline to fulfill the request.

Shortening and clarifying the Privacy Rule time limits for access requests would strengthen individuals' rights with respect to their health information, advance the aims of patient-directed health care, and enhance care coordination.

4. Addressing the Form of Access

The Privacy Rule requires a covered entity to provide the individual with access to the PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form, or other form and format as agreed to by the covered entity and individual.[111] If the individual requests electronic access to PHI that the covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format, if it is readily producible in that form and format, or if not, in an agreed upon alternative, readable electronic format.[112] The Department intends for the phrase "readily producible in that form and format" to

---

[110] "These timelines apply regardless of whether…[t]he covered entity negotiates with the individual on the format of the response. Covered entities that spend significant time before reaching agreement with individuals on format are depleting the 30 days allotted for the response by that amount of time." Available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

[111] *See* 45 CFR 164.524(c)(2)(i).

[112] *See* 45 CFR 164.524(c)(2)(ii).

refer to how the PHI is produced to the individual or to a third party designated by the individual to receive a copy of PHI *and* the form (*e.g.*, on paper or electronically) and format (*e.g.*, the type of electronic file, etc.) of the PHI that is transmitted. As new forms of information and communications technologies emerge, the "form and format" and the "manner" of producing or transmitting a copy of electronic PHI may become indistinguishable. For example, if a covered entity or its EHR developer business associate has chosen to implement a secure, standards-based API—such as one consistent with ONC's Cures Act certification criteria,[113] and the covered entity's Security Rule obligations—that is capable of providing access to ePHI in the form and format used by an individual's personal health application, that ePHI is considered to be *readily producible* in that form and format, and that is also the manner by which the ePHI is transmitted. Where ePHI is readily producible in the electronic form and format requested by the individual, the covered health care provider must provide that access, including when the individual requests access to the ePHI through a secure, standards-based API via the individual's personal health application.[114]

The Department is examining how best to address individuals' privacy and security interests when they use a personal health application that receives PHI from a covered entity and has outlined several approaches in the request for comment at the end of this section. The Department requests information about the costs and benefits of options for educating individuals in a manner that does not delay or create a barrier to

---

[113] ONC has finalized significant updates to its certification criteria at 45 CFR Parts 170 and 171. *See* 85 FR 25642 (May 1, 2020).

[114] *See* proposed 45 CFR 164.501 definition of personal health application: *Personal health application* means an electronic application used to access health information on an individual, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity. The Privacy Rule does not require a covered entity to implement an API for electronic transmission of an electronic copy of PHI to an individual. Covered entities that transmit ePHI electronically, through an API or by other means, are subject to the Security Rule requirements to ensure the confidentiality, integrity and availability of the ePHI they transmit. *See* 45 CFR 164.306, Security standards: General rules. *See* 45 CFR Subparts A and C for the complete Security Rule.

access. The options presented are consistent with the intent expressed in the ONC Cures Act Final Rule: although "an actor may not prevent an individual from deciding to provide its EHI to a technology developer or application despite any risks noted regarding the application itself or the third party developer," ONC "strongly encourage[s] actors to educate patients and individuals about the risks of providing other entities or parties access to their EHI."[115]

In addition, the Department proposes, at 45 CFR 164.524(c)(2)(iii), to provide that if other federal or state law (*e.g.,* a statute or regulation) requires an entity (which may include a business associate acting on behalf of a covered entity) to implement a technology or policy that would have the effect of providing an individual with access to his or her PHI in a particular electronic form and format (*e.g.*, if a federal law required the provision of access via secure, standards-based API), such form and format would be deemed "readily producible" for purposes of compliance in fulfilling requests for such PHI under 45 CFR 164.524(c)(2)(i) and (ii). This would mean, for example, that if a covered health care provider refused to provide an electronic copy of PHI in response to an individual's request for access via a secure API despite the provider's having implemented a secure API established within the provider's EHR for this purpose, the provider would be in violation of the requirement to provide the requested PHI in the form and format requested if readily producible.[116] In contrast, if the same covered health care provider required all applications to register before providing access via its secure API, imposing this requirement would not constitute a denial of access in the form and format requested, provided that the registration process did not exclude or prevent a personal

---

[115] 85 FR 25642, 25815 (May 1, 2020).

[116] Note that unlike the HIPAA Rules, the ONC Cures Act Final Rule defines access for the purposes of the information blocking provision as "the ability or means necessary to make EHI available for exchange, use, or both." *See* 45 CFR 171.102.

health application that was capable of securely connecting to the secure API from so connecting.[117]

The Department seeks comments on related situations: Whether to require a health care provider that has EHR technology that incorporates a secure, standards-based API without extra cost, to implement the API; whether to require a health care provider that could implement such an API at little cost to do so; and how to measure the level of cost that would be considered a reasonable justification for not implementing an API.

Section 164.524(c)(2)(iii) of the current Privacy Rule, which would be redesignated as sections 164.524(c)(2)(iv) and 164.524(d)(4), allows a covered entity to provide a summary in lieu of providing access to the requested PHI, or an explanation of the PHI to which access has been provided, if the individual agrees. To ensure that individuals are able to fully exercise their right of access, the Department proposes to add new sections 164.524(c)(2)(iv)(B) and 164.524(d)(4)(ii) to require that, when a covered entity offers a summary in lieu of access, it must inform the individual that the individual retains the right to obtain a copy of the requested PHI (or direct an electronic copy of PHI in an EHR to a third party) if they do not agree to receive the summary. The proposed requirement would not apply when the covered entity offers a summary because it is denying the request for a copy on unreviewable or reviewable grounds, in which case the covered entity must implement the required procedures for such denial. For example, if a covered physician offered to provide a summary in lieu of an entire medical record requested by an individual (or in lieu of "all PHI about the individual in a designated record set," if that is the request), the physician would be required to inform the individual

---

[117] HIPAA does not convey authority to impose security standards on a personal health application that is not a covered entity or a business associate. However, the ONC Cures Act Final Rule at 45 CFR 171.203 provides an exception to what is considered information blocking when the actor's practice that is likely to interfere with the access, exchange, or use of electronic health information is done in order to protect the security of electronic health information. An actor whose practices met this security exception would not be subject to civil money penalties for information blocking under 45 CFR 1003.1400 of the HHS OIG proposed rule. *See* 85 FR 22979 (April 24, 2020).

of the right to obtain all of the PHI requested. In contrast, if a covered psychologist offered to provide a summary in lieu of requested psychotherapy notes, the psychologist would be required to follow the implementation specifications for denial of access, including providing a written denial and making other information accessible, such as mental health records that are not psychotherapy notes, as defined in the Privacy Rule.

5. Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

a. Current Provisions and Issues to Address

The Privacy Rule right of access requires covered entities to transmit a copy of PHI directly to another person designated by the individual when directed by the individual.[118] Under the current regulatory provision, the request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI. The designated recipient (the "third party") may be a family member or caregiver, a health care provider, a researcher, or any other person or entity the individual (or their personal representative) chooses.

The access right to direct a copy of PHI to a third party is distinct from the provision that permits a covered entity to disclose PHI to a third party with an individual's valid authorization in at least four key respects:[119] (1) the mandatory versus permissive nature of the disclosure; (2) the manner in which the request is made (*e.g.,* with or without a form containing required elements); (3) the form and format of the information provided; and (4) the fees that may be charged. Under the right of access, the individual requests the desired PHI in a designated record set, for whatever purpose he or she wishes, and the covered entity that maintains the PHI is required to respond within a certain period

---

[118] *See* 45 CFR 164.524(c)(3)(ii). As discussed above, the Department is not enforcing the elements of this regulatory provision that apply to directing non-electronic copies of PHI or copies of PHI that are not in an EHR.

[119] *See* 45 CFR 164.508.

of time and to comply with certain form and format requirements in 45 CFR 164.524, and is subject to access fee limits. In contrast, the Privacy Rule specifically designed the authorization requirements to ensure that individuals agree to the specific uses or disclosures, including the purposes for the uses or disclosures, and that they understand and know how to exercise their rights. Therefore, an authorization states the purpose for the request, describes the PHI requested in a specific and meaningful fashion, and includes a statement explaining the individual's right to revoke the authorization (among other information). The covered entity that receives the individual's valid authorization is permitted, but not required, to disclose the PHI as requested, and may charge the individual for costs beyond those that may be included in a fee for providing copies of PHI pursuant to the right of access.

The right of access does not specifically address provider-to-provider exchanges of PHI because the Privacy Rule permits such disclosures without the individual's authorization for treatment, payment, and health care operations, among other specified purposes. The Privacy Rule also does not address fees for those disclosures. However, the Department believes that some patients have been using the right to direct PHI to a third party as a means of having one covered health care provider send records to another provider. The proposed changes to the right to direct copies of PHI to third parties, such as limiting the right to electronic copies in an EHR and allowing fees for copying ePHI onto electronic media may affect those exchanges of PHI, if health care providers choose to charge fees when sending copies of PHI to other providers when previously they did not.

b. Proposals

The Department proposes to create a separate set of provisions for the right to direct copies of PHI to a third party at subsection (d) of 45 CFR 164.524. Proposed subsection (d) will better align the Privacy Rule with the HITECH Act right to direct to a

third party only electronic copies of PHI in an EHR,[120] expand an individual's ability to submit an oral, electronic, or written request for a covered health care provider to transmit an electronic copy of PHI in an EHR to a designated third party in proposed 45 CFR 164.524(d)(1), and expand the access right to empower individual-directed sharing of electronic copies of PHI in an EHR (as the Department proposes to define electronic health record in 45 CFR 164.501) among covered health care providers and health plans as proposed in 45 CFR 164.524(d)(7). The Department believes that only covered health care providers would be responsible for fulfilling an individual's access request under these proposals because the Department believes other covered entities do not have an EHR as that term is defined in the HITECH Act (*i.e.,* an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff). The Department seeks comment on this assumption.

Under the first part of this proposal, at 45 CFR 164.524(d)(1), requests to direct copies of PHI to a third party will be limited to only electronic copies of PHI in an EHR. Therefore, if an individual directs a covered health care provider to transmit an electronic copy of PHI contained in an EHR (as defined in proposed 45 CFR 164.501) to a third party, the covered health care provider must provide a copy of the requested PHI to the person designated by the individual.

The *Ciox v. Azar* decision noted that the HITECH Act "says nothing about a right to transmit PHI contained in any format other than an EHR."[121] The Department believes that the *Ciox v. Azar* decision precludes a proposal to require covered health care providers to provide electronic copies of PHI to third parties designated by the individual in the form and format requested by the individual. However, the Department encourages

---

[120] *See* 42 U.S.C. 17935(e).
[121] See *Ciox v. Azar*, No. 18-cv-0040-APM, memorandum op. at 46.

covered health care providers, when feasible, to provide copies to third parties in the electronic format requested by the individual. There are many formats in which ePHI can be saved and transmitted that are accessible, readable, and usable by a third party designated by an individual to receive the individual's PHI. For example, the portable document format (PDF) was created specifically to present readable electronic documents independent of hardware, software, and operating systems. Other electronic formats are accessible, usable, and readable because of the popularity of the format (*e.g.*, files saved in .doc and .docx format). The 2013 Omnibus Rule preamble referred to these formats as examples of electronic formats that covered entities could use when providing ePHI in response to a right of access request to ensure patients could read and use the PHI they request.[122] In addition, ONC and CMS are promoting the use of the Fast Healthcare Interoperability Resources (FHIR) standard, which covered health care providers can adopt as an electronic format, to achieve interoperability and easy exchange of health information.[123]

However, in some cases, ePHI might be exported from legacy health IT systems in a proprietary format that would be unreadable for the average person. Further, many data systems offer the capability to export data in multiple formats for portability, and not all of the formats are equally accessible, usable, and readable. For example, a comma-separated value (CSV) file is a common format for sharing data between databases and spreadsheets. However, if a designated third party received PHI in a CSV file from a covered health care

---

[122] "The Department considers machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the protected health information in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats." *See* 78 FR 5566, 5631.

[123] *See* 45 CFR 170.215, Application Programming Interface Standards, adopted by ONC at 85 FR 25642, 25941 and ONC's Fact Sheet, "The ONC Cures Act Final Rule" available at https://www.healthit.gov/cures/sites/default/files/cures/2020-03/TheONCCuresActFinalRule.pdf; *See also* 85 FR 25510, 25521, explaining that CMS-regulated entities must adopt 45 CFR 170.215 to implement and maintain a standard-based Patient Access API to support data exchange and empower patients through use of technology ("apps").

provider, the third party may lack the necessary context to read and use such information. Because the right to direct PHI to a third party is a part of the individual right of access, the Department encourages covered health care providers to respond to such requests in a manner that does not frustrate individuals' efforts to exercise those rights in a meaningful way or potentially require the individual to make a second request to obtain a copy of the requested information directly.

As discussed above in reference to individual access, as new forms of information and communications technologies emerge, the "form and format" and the "manner" of producing or transmitting a copy of electronic PHI may become indistinguishable. For example, if a covered entity has implemented a secure, standards-based API that is capable of providing access to ePHI in the form and format used by an individual's personal health application, that ePHI is considered to be *readily producible* in that form and format, and that is also the manner by which the ePHI may be directed to a third party.

Under the second part of this proposal, in proposed 45 CFR 164.524(d)(1), a covered health care provider would be required to respond to an individual's request to direct an electronic copy of PHI in an EHR to a third party designated by the individual when the request is "clear, conspicuous, and specific" -- which may be orally or in writing (including electronically executed requests).[124] The proposed requirement would replace the current requirement that a request to direct an electronic copy of PHI in an EHR be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.[125]

Under these proposals, a written access request such as that contemplated in the current rule would be one means of exercising this right of access, but an oral request

---

[124] The exceptions to this right are parallel to the existing exceptions to the individual right of access in 45 CFR 164.524 (a)(1) for psychotherapy notes and information compiled in anticipation of, or for use in, legal proceedings or unreviewable or reviewable grounds of denial.
[125] *See* 45 CFR 164.524(c)(3)(ii).

could also be actionable if it is clear, conspicuous, and specific. For example, an oral request that identifies the designated recipient and where to send the PHI could meet this standard. Additionally, this provision would allow an individual to use an internet-based method,[126] such as a personal health application, to submit an access request to their health care provider to direct an electronic copy of their PHI in an EHR to a third party, so long as it is "clear, conspicuous, and specific."

The third part of this proposal, at 45 CFR 164.524(d)(7), would create a requirement within the right of access for a covered health care provider or health plan to facilitate an individual's request to direct an electronic copy of PHI in an EHR to a third party designated by the individual, which in this case would be the covered entity facilitating the request. If an individual makes a clear, conspicuous, and specific request that his or her covered health care provider or health plan ("Requester-Recipient") obtain an electronic copy of PHI in an EHR from one or more covered health care providers ("Discloser"), Requester-Recipient would be required to submit the individual's request to Discloser, as identified by the individual.[127] This requirement would apply when an individual is an existing or prospective new patient or a current member (or dependent) of Requester-Recipient, and is limited to directing electronic copies of PHI in an EHR back to Requester-Recipient. (The proposed rule would not require Requester-Recipient to determine whether the potential Discloser is a covered health care provider before submitting the individual's request.) Under this proposal, the individual may make the request orally if the request is clear, conspicuous, and specific. Requester-Recipient may document and submit the oral request in writing or electronically, or, if Discloser accepts

[126] This NPRM uses "internet-based method" to include online patient portals, mobile "apps," and successor technologies.

[127] Discloser is an entity that maintains or previously maintained an individual's PHI, so they will have had a relationship with the patient, unless the request is made in error.

oral requests for records from other health care providers or from health plans, Discloser could use its established procedures for accepting and verifying such requests.

The HITECH Act right of an individual to direct an electronic copy of their PHI in an EHR to a third party does not limit the type of entity that may be designated as a third party recipient. As such, covered entities already are potential third party recipients under the right of access, if designated as such by an individual. Under this proposal, a Requester-Recipient would be required to assist an individual in submitting their request for Discloser to direct PHI in an EHR maintained by or on behalf of the Discloser to Requester-Recipient; however, the Department does not propose to change any obligations of the Requester-Recipient once it receives the PHI. For example, the Privacy Rule does not require that a covered health care provider retain PHI it receives about individuals, and the Department does not propose to change this. While Requester-Recipient might be subject to a records retention requirement under state law, its obligations with respect to PHI it receives as a designated third party would be no different under this proposal than its existing obligations when it receives ePHI from other health care providers, *e.g.,* for treatment, payment, or health care operations (TPO) purposes. The Department believes this conclusion holds true whether the disclosure of PHI is pursuant to a valid authorization, or to a third party designated by an individual pursuant to an access request. The Department welcomes examples and comment on this assumption.

In summary, the proposed requirement offers a second mechanism (in addition to the permitted disclosure for TPO) for a covered health care provider or health plan to obtain an electronic copy of PHI in an EHR from another covered health care provider through a required disclosure initiated by an individual's exercise of the right of access. This requirement differs from the scenario in which, for example, one provider queries a health information system or health information exchange (HIE) for records from another

provider pursuant to an applicable disclosure permission, such as for treatment or health care operations purposes.

The Department's proposal would require that Requester-Recipient submit such access requests to Discloser on behalf of the individual as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and any information the Requester-Recipient needs to submit the access request to Discloser. For example, Discloser may need the name and birthdate of the individual, as well as the name of the Requester-Recipient, a link to a secure electronic document exchange portal, or a physical address where the Discloser may deliver electronic media. The time limit for Requester-Recipient to submit an individual's access request to Discloser would be distinct from covered entities' obligations to provide copies in response to an individual's access request, and a 15 calendar day extension would not be available to Requester-Recipient when submitting the request. Pursuant to the access right to direct an electronic copy of PHI in an EHR to a third party, Discloser would be required to provide the requested electronic copy to Requester-Recipient according to the shorter time proposed for all access requests when the individual directs the information to a third party under 45 CFR 164.524(d)(5) ("as soon as practicable, but not later than 15 calendar days after receiving the request"), provided that the request is clear, conspicuous, and specific. The proposal would permit one 15 calendar day extension under the same conditions described above with respect to the Discloser fulfilling other access requests. Thus, Requester-Recipient would be required to submit an individual's clear, conspicuous, and specific request to Discloser within 15 calendar days of receipt of the request from the individual, and Discloser would then be required to respond by providing the electronic copy to Requester-Recipient, in accordance with proposed 45 CFR 164.524(d)(7). As explained above with respect to requests to direct electronic copies of PHI in an EHR to a third party, individuals may choose to use an internet-based method, such as a personal health

application, to ask Requester-Recipient to submit a request to Discloser to transmit an electronic copy of the individual's PHI in an EHR to Requester-Recipient, so long as it is "clear, conspicuous, and specific." The Department welcomes comments on whether a Requester-Recipient should be permitted to refuse to submit a request for an individual in some circumstances (*e.g.*, if it already has the requested information), and whether the Department should specify in regulatory text that if a Requestor-Recipient discusses the request with the individual (*e.g.,* to clarify the request or explain how the request could be changed to be more useful in meeting the individual's health needs), such discussion does not extend the time limit for submitting the request.

The Department also seeks comments on approaches it may take to clarify that the Privacy Rule permits covered entities to use HIEs to make "broadcast" queries on behalf of an individual to determine which covered entities have PHI about the individual and request copies of that PHI. Section 164.506(c)(1) permits a covered entity to disclose PHI for its own health care operations purposes, including customer service activities, which could include forwarding an access request to other providers using a trusted exchange network. The Department is considering approaches to clarifying this permission to enhance the right of access and seeks comment on how to do so effectively.

The Department's proposal regarding individual-directed disclosures of PHI in an EHR among certain covered entities would strengthen and clarify the individual's ability to direct the sharing of such PHI. The proposed changes are not intended to replace or frustrate prompt transfers of PHI and ePHI that covered health care providers and health plans already make voluntarily for purposes of treatment, payment, and health care operations. Instead, as was urged by commenters on the 2018 RFI, the proposed changes would require covered entities to submit certain requests for PHI and require covered health care providers to make certain disclosures, pursuant to the exercise of the individual's right to access. This mechanism creates a new required disclosure to covered

entities, but in a manner that respects individual preferences and control over the disclosure of PHI through his or her exercise of the right of access.

Finally, parallel to the proposal with respect to the individual right to obtain copies of PHI (and discussed in III.a.4), the Department proposes to require covered entities to inform individuals about their right to direct the requested electronic copies of PHI in an EHR to designated third parties when a covered entity offers to provide a summary in lieu of the requested copies of PHI in 45 CFR 164.524(d)(4)(ii). Consistent with the earlier proposal, the new requirement would not apply when the covered entity offers a summary because it is denying the request for a copy on unreviewable or reviewable grounds, in which case the covered entity must implement the required procedures for such denial.

6. Adjusting Permitted Fees for Access to PHI and ePHI

a. Current Provisions and Issues to Address

The Privacy Rule allows covered entities to charge a reasonable, cost-based fee to fulfill access requests from individuals for copies of their PHI. Section 45 CFR 164.524(c)(4) limits the allowable fees to the costs of (i) labor for copying (whether the PHI is in paper or electronic form), (ii) supplies for creating the paper copy or electronic media if requested, (iii) postage, and (iv) preparing any agreed-upon summary or explanation of the requested PHI. Section 13405(e) of the HITECH Act expands the individual right of access to include the right to direct an electronic copy of PHI in an EHR to a third party. Because the HITECH Act expressly placed the new right within 45 CFR 164.524, the long established right of access, the Department interpreted the 2013 Omnibus Rule as applying the component parts of the existing access right to the new type of access right. This interpretation applied the limitation on fees that covered entities may charge individuals exercising the access right. However, the Department first explained its interpretation in the 2016 Access Guidance, not the 2013 Omnibus Rule. As a result, the

Ciox v. Azar court found that the Department had improperly imposed the fee limitations in the access right to direct a copy of PHI to a third party without notice and comment rulemaking. This NPRM proposes to place modified fee limitations in regulatory text and requests public comment on all aspects of the proposal.

b. Proposal

The Department proposes to modify the access fee provisions to establish a fee structure with two elements based on the type of access request. The first element describes categories of access for which covered entities cannot charge a fee. The second element describes the allowable costs that may be included when an access fee is permitted. The modified fee provisions will be separately located within the enumerated sections for the individual right to inspect and obtain copies of PHI and for the right to direct electronic copies of PHI in an EHR to third parties, as summarized below.

For the individual right to inspect PHI and to obtain copies of PHI about the individual, fees would be:

(1) Always free of charge (*i.e.,* no fee permitted) in proposed 45 CFR 164.524(c)(4)(ii), when:

(a) an individual inspects PHI about the individual in person, which may include recording or copying PHI in a designated record set with the individual's own device(s) or resource(s).

(b) an individual uses an internet-based method to view or obtain a copy of electronic PHI maintained by or on behalf of the covered entity. This includes, for example, access obtained by an individual through the covered entity's certified health IT (*e.g.,* the "view, download, and transmit" criterion at 45 CFR 170.315), or by a personal health application connecting to secure

standards-based APIs,[128] consistent with applicable federal or state law. The Department intends that such access would be provided without charging a fee to the individual or the personal health application developer.

(2) A reasonable, cost-based fee, in proposed 45 CFR 164.524(c)(4)(i), provided that the fee includes only the cost of:

(a) Labor for copying the PHI requested by the individual in electronic or non-electronic (*e.g.,* paper, film) form;

(b) Supplies for making non-electronic copies;

(c) Actual postage and shipping for mailing non-electronic copies; and

(d) Preparing an explanation or summary of electronic or non-electronic PHI, if agreed to by the individual as provided in paragraph (c)(2)(iii) when an individual requests an electronic or non-electronic copy of PHI about the individual through a means other than an internet-based method.

For the right to direct an electronic copy of PHI in an EHR to a third party, the fees would be:

Under proposed 45 CFR 164.524(d)(6), a reasonable, cost-based fee for an access request to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party through other than an internet-based method, provided that the fee includes only the cost of:

(a) Labor for copying the PHI requested by the individual in electronic form; and

(b) Preparing an explanation or summary of the electronic PHI, if agreed to by the individual as provided in paragraph (d)(4).

---

[128] *See e.g.,* 85 FR 25642, 25645 (May 1, 2020), discussing ONC adoption of API certification criteria at 45 CFR 170.213 and 215.

This category would apply to requests for a copy of PHI that cannot be fulfilled through an automated process. For example, requests to copy PHI in an EHR onto electronic media and mail it to a physical address would fall within this category.

A summary of how different types of access and recipients of the PHI would affect the proposed allowable access fees is outlined in the chart below.

Type of Access	Recipient of PHI	Allowable Fees
In-person inspection – including viewing and self-recording or -copying	Individual (or personal representative)	Free
Internet-based method of requesting and obtaining copies of PHI (*e.g.*, using View-Download-Transmit functionality (VDT), or a personal health application connection via a certified-API technology)	Individual	Free
Receiving a non-electronic copy of PHI in response to an access request	Individual	Reasonable cost-based fee, limited to labor for making copies, supplies for copying, actual postage & shipping, and costs of preparing a summary or explanation as agreed to by the individual
Receiving an electronic copy of PHI through a non-internet-based method in response to an access request (*e.g.*, by sending PHI copied onto electronic media through the U.S. Mail or via certified export functionality)[129]	Individual	Reasonable cost-based fee, limited to labor for making copies and costs of preparing a summary or explanation as agreed to by the individual
Electronic copies of PHI in an EHR received in response to an access request to direct such copies to a third party.	Third party as directed by the individual through the right of access	Reasonable cost-based fee, limited to labor for making copies and for preparing a summary or explanation agreed to by the individual.

[129] *See e.g.* 45 CFR 170.315(b)(10) Data export functionality, as added by ONC Final Rule,85 FR 25642 (May 1, 2020).

The proposed approach, described in further detail below, also would allow covered entities to recoup their costs for handling certain requests to send copies of PHI to third parties, while ensuring that covered entities do not profit from disclosures of PHI made at the individual's request.

(1)(a) No fees permitted when an individual inspects PHI in person, including taking notes, photographs, or using other personal resources to view or capture the information.

As noted above, the current Privacy Rule permits a covered entity to impose a reasonable, cost-based fee for providing copies of PHI that may include only the cost of labor for copying the PHI requested; supplies for creating the copy (*e.g.*, paper, electronic media); postage for mailing the copy to the individual, where applicable; and, if agreed to by the individual, preparation of an explanation or summary of the PHI. The Rule contains no provision permitting fees to be charged for inspection of PHI by the individual who is the subject of the PHI. The Department believes that a covered entity does not incur labor costs for copying, and is unlikely to incur costs for supplies, when providing the individual the opportunity to inspect PHI in person and use his or her own personal resources to capture the information. Therefore, the Department proposes to expressly provide that the covered entity may not charge a fee to an individual who exercises the right to inspect their PHI in person.

Based on its beliefs regarding likely costs, the Department proposes to expressly require that covered entities allow an individual to exercise the access right to inspect their PHI in person without charging a fee.[130] Inspecting PHI may include viewing the information on a patient portal, which could be made available in person for the individual at the point of care in conjunction with a health care appointment or at a medical records office.

---

[130] This proposal is consistent with the Department's interpretation of this issue in guidance. *See also* FAQ #2035, available at https://www.hhs.gov/hipaa/for-professionals/faq/2035/can-an-individual-be-charged-a-fee-if-the-individual/index.html.

The Department requests comment on any new costs that covered entities would likely incur when providing individuals with opportunities to inspect their PHI in this manner in person at the covered entity's facility.

(1)(b) No fees permitted when an individual uses an internet-based method to view and capture or obtain an electronic copy of PHI maintained by or on behalf of the covered entity.

The Department believes that access through an internet-based method likely occurs without involvement of covered entity workforce members, and thus believes that the covered entity likely incurs no allowable labor costs or expenses. The Department requests comment on its view of the costs of providing access through an internet-based method, including any internet-based methods described in the ONC Cures Act Final Rule.

Based on its views regarding costs, and to further the policy goal of removing unnecessary barriers to individuals' exercise of the right of access, the Department proposes to prohibit covered entities from charging a fee to provide access through an internet-based method, as described below. While covered entities currently use patient portals and APIs to provide individuals and/or their designated third party recipients with electronic access, the Department proposes that the term "internet-based method" would apply to portals and APIs, as well as similar successor technologies. The Department does not intend free access to apply to situations where the individual is simply using an online portal to submit a request for copies of PHI to be sent to him or her in a manner that would require the covered entity to incur allowable costs for supplies, postage, or labor for copying.

(2)(a) Access requests by an individual for a non-electronic copy of PHI through other than an internet-based method would remain subject to the individual access fee limitations.

When providing copies of PHI to an individual, covered entities would remain subject to the current access fee limits.[131] This would include only labor for copying PHI in non-electronic form, supplies for creating the non-electronic copy, actual postage for mailed copies, and the costs of preparing a requested summary or explanation of the PHI.

(2)(b) Access requests by an individual for an electronic copy of PHI through other than an internet-based method would be a reasonable, cost-based fee that is limited to the costs of: (i) labor for making electronic copies of the PHI, and (ii) preparing a summary or explanation as agreed to by the individual.

The Department understands that such methods may require special effort on the part of the covered entity, which may include, for example, copying PHI onto electronic media and mailing it to the individual or, under some circumstances, using the export functionality of certified EHR technology to transmit ePHI.[132] The costs of electronic media and postage would not be allowed for providing electronic copies of PHI by any method. Pursuant to section 13405(e) of the HITECH Act, "any fee that the covered entity may impose for providing [an] individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation)."[133] Therefore, the Department is proposing to limit the fees covered entities are permitted to charge for electronic copies of PHI in an EHR based on a plain reading of this statutory requirement.

For the right to direct the transmission of an electronic copy of PHI in an EHR to a third party:

A reasonable, cost-based fee that is limited to the costs of: (i) labor for making electronic copies of the PHI, and (ii) preparing a summary or explanation as agreed to by the individual.

---

[131] *See* 45 CFR 164.524(c)(4).

[132] *See e.g.,* 45 CFR 170.315(b)(10) and 85 FR 25642, 25691 (May 1, 2020). The ONC Cures Act Final Rule added this requirement but did not specify an export format such as an internet-based method of access. Therefore, at times special effort by covered entity workforce member may be required to copy the exported EHI.

[133] *See* 42 U.S.C. 17935(e)(2),

In response to the *Ciox v. Azar*[134] decision and comments received in response to the 2018 RFI, the Department proposes in 45 CFR 164.524(c)(3)(ii) to limit the right of an individual to direct copies of PHI to a third party to only electronic copies of PHI in an EHR (as defined in proposed 45 CFR 164.501). The Department also proposes to limit the allowable fees for such copies to the costs of labor for making such electronic copies.

Section 13405(e) of the HITECH Act created a new way for an individual to exercise the right of access by choosing to send a copy of PHI to a third party, and thus changed the assumptions previously expressed in the 2000 Privacy Rule that disclosures at the individual's initiation are made only to the individual, while disclosures to third parties are always initiated by others. For example, the 2000 Privacy Rule preamble contrasted the limited fees to provide PHI "for individuals" based on the individual's request with fees allowed for "the exchange of records not requested by the individual"[135] (*i.e.,* requests made by other persons). The HITECH Act expanded the types of records exchanges that could be requested by the individual pursuant to the right of access, with the result that the identity of the recipient of PHI no longer signifies whether the PHI was provided "for" the individual (*i.e.,* at the individual's request through their exercise of the right of access). In addition, the same policy rationales expressed in the 2000 Privacy Rule for limiting fees for individual requests for access, to ensure that the right of access "is within reach of all individuals,"[136] apply when the individual requests to direct a copy of PHI to a third party: in both cases, the individual is choosing where to send their own PHI and often, if not always, will be responsible for paying the fee themselves. Finally, by placing the right to direct an electronic copy of PHI in an EHR within the right of access, which had included access fee limitations since the 2000 Privacy Rule, the Department believes the HITECH

---

[134] No. 18-cv-0040-APM (D.D.C. January 23, 2020).
[135] *See* 65 FR 82462, 82754 (December 28, 2000).
[136] *See Id* at 82577.

Act contemplated that access fee limitations would apply, along with other aspects of the existing access right.

Under this proposal, the allowable fees would include, for example, the labor involved in transferring electronic copies of PHI from an EHR onto electronic media when requested by the individual, but would exclude the costs of the electronic media, the labor involved in shipping or mailing the media, and the costs of shipping or postage. Additionally, as under the current rule, a covered entity would be permitted to charge for the costs of preparing a summary or explanation of the requested PHI to be directed to a third party as agreed to by the individual in advance. With these proposed changes, individuals would rely on a valid authorization to send non-electronic copies of PHI in an EHR, or electronic copies of PHI that is not in an EHR, to third parties. Covered entities responding to requests based on an authorization would not be subject to the access fee limitations; however, the fees would remain limited by the Privacy Rule's provisions on the sale of PHI[137] and by applicable state law. Under the Privacy Rule's provisions on the sale of PHI at 45 CFR 164.502(a)(5)(ii)(B)(*2*)(*viii*) and 45 CFR 164.502(a)(5)(ii)(A), covered entities generally must limit fees for disclosures pursuant to an authorization to a "reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law" or must state in the authorization that the disclosure will result in remuneration to the covered entity as provided in 45 CFR 164.508(a)(4).

Although covered entities would be restricted from recouping some costs that are allowed under the current rule, the effect of limiting the right to direct PHI to a third party to only electronic copies of PHI in an EHR would significantly reduce covered entities'

---

[137] By default, this change would treat disclosures based on requests to direct non-electronic and non-EHR copies of PHI to third parties the same as other requests for disclosures pursuant to a valid authorization. See discussion of the limitations on requests to direct certain copies of PHI to a third party and related requirements, *infra. See also* 45 CFR 164.502(a)(5)(ii)(A) and 164.508(a)(4).

burdens by increasing the number of requests based on an authorization. For example, many states have laws permitting health care entities to impose fees for providing copies of medical records that may be higher than the Privacy Rule allows. The states, for example, may permit covered entities to charge for costs other than supplies, labor for copying, and postage, or may establish a per page fee in excess of what the Privacy Rule allows. However, under the current Privacy Rule, when an individual exercises his or her access right, including when directing an electronic or non-electronic copy of PHI to any third party, covered entities are not permitted to impose higher fees for copies of PHI that may be permitted by state law.[138]

The Department anticipates that no fees would be charged when an individual uses an internet-based method to direct an electronic copy of PHI in an EHR to any third party, when an individual uses such a method to direct a covered health care provider or health plan to submit an access request to another covered health care provider, or when an individual submits a request through a health care provider or health plan to other providers and plans using such method**.** The rationale for this understanding is the same as discussed above in relation to the individual right to access or obtain copies of PHI available via an internet-based method—that there are no associated costs incurred by the covered entity for responding to the specific request. The Department requests comment on whether the assumption that no costs will be incurred to provide access using an internet-based method applies to each of the internet-based access scenarios described in this paragraph.

As a consequence of the proposed limits on the right to direct transmission of electronic copies of PHI in an EHR, covered entities would be permitted to charge less restricted fees when fulfilling requests to send non-electronic copies of PHI in an EHR, or electronic copies of PHI that is not in an EHR, to third parties, because these requests

---

[138] *See* 78 FR 5566, 5636 (January 25, 2013).

would no longer be within the right of access.[139] Instead, such disclosures to third parties (whether to an individual's family member, covered entity, researcher, or any other person) would be accomplished through an individual's valid authorization, with the only Privacy Rule limitation on the fees for such copies being the Privacy Rule's provisions on the sale of PHI.[140]

The Department does not propose to change how covered entities currently charge for disclosing records to health plans and providers. It is the Department's understanding that frequently there is no charge for permitted disclosures of PHI to another covered entities for core health care activities such as treatment, payment, or health care operations. This proposal is not intended to cause covered entities to begin charging fees for such disclosures, but to recognize individuals as the center of their own health care and empower individual-initiated transfers of electronic copies of PHI in an EHR.

7. Notice of Access and Authorization Fees[141]

To increase an individual's awareness of the cost of copies of PHI, and to make the access fee requirements more uniform, the Department proposes to add a new subsection 525 to 45 CFR 164 to require covered entities to provide advance notice of approximate fees for copies of PHI requested under the access right and with an individual's valid authorization. Readily available public information about access fees would also serve to promote compliance with the Privacy Rule because covered entities will want to avoid

---

[139] By default, this would change the status of requests to direct non-electronic and non-EHR copies of PHI to third parties by relegating such requests to disclosures under the authorization standards. See discussion of the limitations on requests to direct certain copies of PHI to a third party and related information requirements, *infra.*

[140] 45 CFR 164.501(a)(5)(ii)(A) and 164.508(a)(4).

[141] This NPRM uses "access and authorization fees" to mean fees for copies of PHI provided pursuant to the individual's right of access and for disclosures made pursuant to a valid authorization, respectively.

posting fee schedules that show noncompliance with fee limitations,[142] or that publicly misrepresent their business practices, and individuals will be empowered to insist on covered entities' compliance as well. Specifically, covered entities would be required to post a fee schedule online (if they have a website) and make the fee schedule available to individuals at the point of service, upon an individual's request. The notice must include: (i) all types of access available free of charge and (ii) fee schedule for: (A) copies provided to individuals under 45 CFR 164.524(a), with respect to all readily producible electronic and non-electronic forms and formats for such copies; (B) copies of PHI in an EHR and directed to third parties designated by the individual under 45 CFR 164.524(d), with respect to all readily producible electronic forms and formats for such copies; and (C) copies of PHI sent to third parties with the individual's valid authorization under 45 CFR 164.508, with respect to all available forms and formats for such copies.

With respect to fee schedule availability at the point of service, the Department would expect that a covered health care provider would make the fee schedule available upon request, in paper or electronic form, at the point of care or at an office that is responsible for releasing medical records, as well as orally (*e.g.,* over the phone), as applicable. For both covered health care providers and health plans, the point of service also could include a customer service call center that handles requests for records, or any location at which PHI is made available for individuals to inspect, as required under 45 CFR 164.524.

---

[142] In addition to the access fees limits contained in 45 CFR 164.524, the Privacy Rule limits the fees that may be charged for uses and disclosures of PHI based on an authorization. Under the Privacy Rule's provisions on the sale of PHI, covered entities generally must limit fees for disclosures pursuant to an authorization to a "reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law" or must state in the authorization that the disclosure will result in remuneration to the covered entity. *See* 45 CFR 164.502(a)(5)(ii)(B)(*2*)(*viii*); 45 CFR 164.502(a)(5)(ii)(A); 45 CFR 164.508(a)(4).

Additionally, the Department proposes to require that covered entities provide an individualized estimate to an individual of the approximate fees to be charged for the requested copies of PHI, upon request. The Department would expect that the covered entity would provide the individualized estimate upon request and within the initial time (or in many cases sooner) in which the covered entity has to fulfill the access request (prior to any extension of time that may be allowed for providing the copies) and prior to providing the requested PHI, to allow for a meaningful decision by the individual regarding the scope of the request or the form and format requested. If more time is needed to provide the requested copies after providing an individualized estimate, a covered entity may notify the individual of its need for a 15-day extension.

The Department also proposes in 45 CFR 164.525 to require covered entities to provide, upon an individual's request, an itemization of the charges for labor for copying, supplies, and postage, as applicable, which constitute the total fee charged to the individual for copies of PHI.

The Privacy Rule does not prohibit a covered entity from requiring individuals to pay a fee for copies of PHI "upfront" before receiving such copies. The Department does not propose to amend the Privacy Rule to require covered entities to fulfill the requests of individuals (by providing copies of PHI) before fees are paid. However, because the Department believes that providing individuals with access to their health information is an important component of delivering and paying for healthcare, the Department continues to encourage covered entities that charge fees for copies of PHI to waive fees or provide flexibility in payment (such as delaying charges or accepting payment in installments, without delaying the provision of copies) for individuals who are unable to pay upfront due to an emergency or a lack of resources.[143] The Department also

---

[143] *See* 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

encourages covered entities to waive access fees in cases where the individual cannot pay the fee due to a demonstrated financial hardship, including when the requesting individual is a Medicaid beneficiary, homeless, otherwise financially disadvantaged, or experiencing financial strain due to some other type of emergency situation.

Finally, an individual's request for a fee estimate under this proposal would not automatically extend the time permitted for covered entities to provide copies of PHI under the right of access; however, a covered entity would have the ability to inform the individual if one 15-day extension is needed.

8. Technical Change to General Rules for Required Business Associate Disclosures of PHI

The Department proposes to insert clarifying language in 45 CFR 164.502(a)(4)(ii), which currently requires business associates to provide copies of PHI to covered entities, individuals, or individuals' designees, to satisfy the covered entity's obligations under the right of access. To clarify when a business associate must disclose PHI and to whom, the proposal would specify that a business associate is required to disclose PHI to the covered entity so the covered entity can meet its access obligations. However, if the business associate agreement provides that the business associate will provide access to PHI in an EHR directly to the individual or the individual's designee, the business associate must then provide such direct access. This proposed clarification is consistent with the preamble discussion on this topic in the 2013 Omnibus Rule[144] and subsequent guidance,[145] and is not intended to be a substantive change.

9. Request for Comments

---

[144] *See* 78 FR 5566, 5598-5599 (January 25, 2013).
[145] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html?language=es.

The Department seeks comment on the foregoing proposals, including any benefits or unintended consequences, and the following considerations in particular:

a. Whether the Department's proposed definition of EHR is too broad, given the context of the HITECH Act, such that the definition should be limited to clinical and demographic information concerning the individual.

b. Whether an electronic record can only be an EHR if it is created or maintained by a health care provider, or whether there are circumstances in which a health plan would create or maintain an EHR.

c. Whether the Department should instead define EHRs to align with the scope of paragraphs (1)(i) and (2) of the definition of designated record set.[146]

d. Whether the proposed definition of EHR includes PHI outside of an electronic designated record set, whether it should, and examples of such PHI.

e. Whether the proposed interpretation of "health care clinicians and staff" as it relates to the proposed EHR definition is appropriate, too broad, or too narrow, and in what respects.

f. Should "health care clinicians and staff" be interpreted to mean all workforce members of a covered health care provider? What are the benefits or adverse consequences of such an interpretation? Does the same interpretation apply regardless of whether the provider has a direct treatment relationship with individuals, and why or why not?

g. Are there other health care industry participants that have access to or maintain EHRs that should be explicitly recognized in the definition of EHR or that OCR should consider when establishing such a definition?

h. Whether EHR should be defined more broadly to include all ePHI in a designated record set, and benefits or drawbacks of doing so.

---

[146] *See* 45 CFR 164.501, definition of "Designated record set."

i. Should the definition of EHR for Privacy Rule purposes be aligned with other Department authorities or programs related to electronic health information? If so, which ones and for what purposes?[147]

j. Any other effects, burdens, or unintended consequences of the proposed definition of EHR or of including a definition for EHR in the Privacy Rule.

k. What types of activities should be encompassed in the terms "managed," "shared," and "controlled" in the proposed definition of personal health application, and whether other terms would improve the clarity of the definition.

l. State laws or other known legal restrictions that might affect the ability of individuals to take photos of or otherwise capture copies of their PHI in a designated record set.

m. The frequency with which covered entities currently receive requests to inspect PHI in person, and estimated annual costs to covered health care providers and health plans of fulfilling such requests.

n. Whether a time limit shorter than 15 calendar days for a covered entity to submit, or respond to, an individual's access request would be appropriate. The Department seeks comment on time limits for covered entities to respond to access requests, requests to direct electronic copies of PHI in an EHR to a third party, and requests to submit a request to another provider on behalf of the individual. The Department welcomes data on the burdens and benefits such a time limit would impose.

o. Whether a covered health care provider should be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules. What are the benefits or burdens of different approaches? For example:

---

[147] *See, e.g.,* 84 FR 55766 (October 19, 2019). *Electronic health record* means a repository that includes electronic health information that—(1) Is transmitted by or maintained in electronic media; and (2) Relates to the past, present, or future health or condition of an individual or the provision of health care to an individual. https://www.federalregister.gov/d/2019-22028/p-535

accepting the individual's judgment without requiring covered entities to provide education, notice, or warning; requiring a covered entity to provide a warning verbally and/or electronically at the time the individual requests transmission of PHI to a personal health application; providing education about the application developer's privacy and security policies and practices through an automated attestation and warning process; or adding information about risks to PHI disclosed to a personal health application in the covered entity's NPP.

p. The Department also invites comment on whether to apply any potential education, notice, or warning requirement to only health care providers or also to health plans. Whether the Department should consider requiring a covered health care provider or health plan to provide any specific educational or advisory language to individuals who may choose to share their PHI with other individuals through applications that are not regulated by the Privacy Rule.

q. Whether the Department should specify in regulatory text that if a Requestor-Recipient discusses the request with the individual (*e.g.,* to clarify the request or explain how the request could be changed to be more useful in meeting the individual's health needs), such discussion does not extend the time limit for submitting the request, and the benefits or drawbacks of such a provision.

r. Whether any federal or state law time limit shorter than 15 calendar days that applies to disclosures of PHI to a third party (*e.g.*, public health agency) should be deemed a "practicable" time limit under the Privacy Rule right of access.

s. Whether and how a covered entity should be required to implement a policy for prioritizing urgent or otherwise high priority access requests, so as to minimize the use of the 15-calendar-day extension. Would there be unintended adverse consequences of such a requirement—*e.g.,* would covered entities begin to require individuals to state the purposes for their access requests even though the Privacy Rule does not make the

right of access contingent on the purpose for the request? If a covered entity did impose such a requirement, would this constitute an unreasonable measure that impedes the individual from obtaining access?

t. Any benefits or drawbacks of the proposal to require a covered entity to act on an oral access request to either direct an electronic copy of PHI in an EHR to a third party or direct a covered entity to submit such a request, provided the oral communication is clear, conspicuous, and specific.

u. Whether there would be unintended consequences for the covered entity that has received PHI as a result of a request that was made to another covered entity by an individual.

v. "Clear, conspicuous, and specific" is a statutory standard[148] that the Department proposes to use in place of the existing regulatory requirement that the request be signed and in writing and clearly identify the designated third party. The Department requests comment on how to interpret the phrase "clear, conspicuous, and specific," including when the request is verbal.

w. Whether the Department should specify any bases for a Requester-Recipient to deny an individual's request to submit an access request to a Discloser, for example, if the requested disclosure is prohibited by state or other law or if the Requester-Recipient already has the information.

x. Whether there are certain types of individual requests to submit an access request to a Discloser that would place an undue burden on the Requester-Recipient, such as submitting large numbers of requests to multiple Disclosers, or other factors affecting the potential burden on or benefit to a Requester-Recipient.

y. Whether a covered health care provider or health plan that uses an HIE to make a broadcast query to identify other HIE participants that have PHI about that individual,

---

[148] *See* 42 U.S.C. 17935(e).

and that requests the PHI on behalf of an individual, should be considered to be making a permissible disclosure of PHI for customer service or other administrative or management activities that are part of the covered health care provider or health plan's health care operations.[149] Are there unintended consequences for covered entities or individuals of such an interpretation of health care operations?

z. Information from individuals and covered entities about how covered entities currently respond to "imperfect" requests to send PHI to a third party (*e.g.,* requesting information that is not part of the access right; all the necessary elements of a right of access request are not included when an individual directs electronic PHI in an EHR to a designated third party; invalid authorizations, etc.) and the efforts made by covered entities to enhance individuals' abilities to efficiently obtain the requested information.

aa. Whether the term "internet-based method" or alternative terms adequately describe online patient portals, mobile applications, APIs, and other related technologies. If there are unintended consequences associated with using such broad terminology, are there ways in which any unintended adverse effects could be minimized?

bb. Should the Privacy Rule prohibit covered entities from charging fees for copies of PHI when requested by certain categories of individuals (*e.g.,* Medicaid beneficiaries or applicants for or recipients of Social Security Disability Insurance (SSDI)), or when the copies are directed to particular types of entities (*e.g*., entities conducting clinical research)?

cc. Whether the Privacy Rule should prohibit covered entities from denying requests to exercise the right of access to copies of PHI when the individual is unable to pay the access fee. If so, how should a covered entity determine when an individual is unable to pay?

---

[149] *See* 45 CFR 164.501 (definition of "Health care operations," paragraph (6)).

dd. The fees (if any) that covered entities currently charge when sending records to another provider or covered entity at the request of an individual.

ee. What fees, if any, are charged for disclosures among covered entities made at the request of the entities?

ff. How covered entities currently treat access requests that involve converting non-electronic PHI into an electronic format, the fees that are charged for such requests, and how that compares to fees charged for similar requests for copies of PHI made by a third party with an individual's valid authorization.

gg. How the proposals to narrow the access right to direct PHI to third parties to electronic copies of PHI in an EHR will affect fees for copies of PHI.

hh. How covered entities currently calculate reasonable, cost-based fees for copies of PHI under the right of access. For example, OCR's 2016 Access Guidance offered three illustrative methods for calculating allowable access fees: (1) actual labor costs for copying, plus supplies and postage; (2) average labor costs for copying, plus supplies and postage; and (3) a flat fee of $6.50 for electronic copies of ePHI, inclusive of labor, supplies, and any applicable postage. The Department requests comment on the extent to which entities use each of these methods. For entities using the average costs option (2), the Department requests comment on what data is being used to calculate the average. It also seeks comment on how covered entities calculate fees for "hybrid" access requests—that is, requests for copies of PHI that encompass both electronic and non-electronic PHI.

ii. Comment on whether the Department should specify one or more of the three methods listed above, or another method, in the regulatory text as the exclusive acceptable method of calculating access fees. This NPRM does not propose to require any particular method of calculation; however, the Department requests comment on the benefits and burdens of doing so. The Department also requests comment on the

reasonableness of the $6.50 flat fee for electronic copies of PHI maintained electronically, and whether another flat rate would be more appropriate. Finally, the Department requests comment on whether other methods of calculating fees should be required in regulation or offered as options in guidance.

jj. Whether the Department should establish in regulation a separate required timeframe for covered entities to respond to individuals' requests for access fee estimates or an itemized list of charges, and what timeframe(s) would be appropriate, and whether the time to respond to a request for access should be tolled pending an individual's confirmation that it desires the requested information given the fee estimate.

kk. Whether there should be a legal consequence to covered entities for the bad faith provision of an incorrect estimate of fees for access and authorization requests, and if so, what actions should be considered evidence of bad faith sufficient to subject a covered entity to potential penalties.

ll. More information from covered entities and individuals about their experiences with records requests (including when made at the direction of the individual or with an individual's valid authorization) and any unintended consequences that may result from the Department's proposals.

mm. What are commonly available electronic forms and formats that covered entities and business associates generally provide to individuals or third parties? How many requests per month for electronic copies of PHI on electronic media do covered entities and business associates receive from individuals? How many requests per month are received for electronic copies provided through internet-based methods? How long does it take to fulfill each type of request?

nn. Do individuals or third parties ever receive requested PHI in unreadable electronic forms and formats? What are those forms and formats, and do covered entities or

business associates provide another form and format if they are told the first copy of PHI they provided is unreadable or unusable?

B. Reducing Identity Verification Burden for Individuals Exercising the Right of Access (45 CFR 164.514(h))

1. Current Provision and Issues to Address

Section 45 CFR 164.514(h) of the Privacy Rule generally requires a covered entity to take reasonable steps to verify the identity of a person requesting PHI before disclosing the PHI to help ensure that unauthorized persons do not obtain an individual's PHI.[150]

As OCR has explained in guidance,[151] the Department's view is that the Privacy Rule does not mandate any particular form of verification (such as viewing an individual's driver's license at the point of service), but instead generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided the verification processes and measures do not create barriers to, or unreasonably delay, the individual from obtaining access to their PHI. Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the individual is requesting and/or receiving access, such as in person, by phone (if permitted by the covered entity), by faxing or e-mailing the request on the covered entity's supplied form, by secure internet portal, or by other means. For example, if the covered entity requires that access requests be made on its own supplied form, the form could ask for basic information about the individual that would enable the covered entity to verify that the person requesting access is the subject of the information requested or is the individual's personal representative. For covered entities providing individuals with access to their PHI through internet portals, the Department's view is that the portals

---

[150] *See* 45 CFR 164.514(h). Disclosures under 45 CFR 164.510 are excepted from this requirement. *See* 45 CFR 164.514(h)(1)(i).

[151] *See* 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

should be set up with appropriate authentication controls, as required by 45 CFR 164.312(d) of the HIPAA Security Rule, to ensure that the person seeking access is the individual who is the subject of the PHI (or their personal representative).

Despite OCR's guidance explaining the Department's interpretation of the verification and individual access provisions in 45 CFR 164.514(h) and 164.524,[152] the Department has received complaints and heard anecdotal accounts of covered entities imposing burdensome verification requirements on individuals seeking to obtain their PHI pursuant to the individual right of access. For example, some covered entities require individuals to receive their PHI in person, or even to go through the process (and potential added expense) of obtaining a notarization on a written request, to exercise their right of access.

2. Proposal

To address these ongoing challenges and barriers to an individual's access to their health information, the Department proposes to modify paragraph (2)(v) of 45 CFR 164.514(h) to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or his or her personal representative) exercising a right under the Privacy Rule. In addition, the Department proposes to clarify within the regulatory text that unreasonable verification measures are those that require an individual to expend unnecessary effort or expense when a less burdensome verification measure is practicable for the particular covered entity. Unreasonable measures would include requiring individuals to obtain notarization of requests to exercise their Privacy Rule rights and requiring individuals to provide proof of identity in person when a more convenient method for remote verification is practicable for the covered entity. The Department would consider the application of the practicability standard for verification measures to encompass considerations related to an entity's fulfillment of its Security

---

[152] *Id.*

Rule obligations including its size, complexity and capabilities; its technical infrastructure, hardware, and software security capabilities; the costs of security measures related to verification and implementing measures that may be more convenient for individuals; and the probability and criticality of potential risks to ePHI in the covered entity's systems.[153] This modification is not intended to prevent covered entities from taking reasonable measures to verify the identity and authority of the individual or entity making the request.

As explained above, the Department proposes to clarify that a covered entity that implements a requirement for individuals to submit a request for access in writing would not be permitted to do so in a way that imposes unreasonable burdens on individuals. The proposed change to prohibit a covered entity from implementing unreasonable identity verification requirements complements the first proposal to ensure that an individual is afforded as much flexibility as reasonable when accessing his or her own records. In contrast, a covered entity that is responding to an individual's request to direct an electronic copy of ePHI in the covered entity's EHR to a third party must do so if the oral or written request is clear, conspicuous, and specific. The Department assumes that a covered entity holding records of an individual in an EHR has necessarily established a treatment relationship with such individual, and therefore, imposing additional verification requirements is unnecessary. The Department seeks comments on this assumption.

Consistent with the verification provisions described above, unreasonable measures for submitting an access request in writing would be measures that impede the individual from obtaining access when a measure that is less burdensome for individuals is practicable for the particular covered entity. For example, requiring individuals to complete a form with only the limited information needed for the entity to provide access would be considered reasonable because it only requests information necessary for verification and does not require the individual to expend unnecessary effort. In contrast,

---

[153] *See* 45 CFR 164.306(b)(2).

requiring individuals to fill out a form with the extensive information contained in a HIPAA authorization form may impose an unreasonable burden to individuals. In addition, while covered entities are encouraged to provide individuals with the option to submit access requests through online portals, it generally would be unreasonable for a covered entity to require that requests for access be made only through the covered entity's online portal, depending on factors such as the covered entity's analysis of security risks to ePHI.[154] Unreasonable measures also would include applying onerous or infeasible registration requirements for personal health applications (or other applications that are not being provided on behalf of or at the direction of the covered entity) that would create a barrier to or unreasonably delay registration beyond what is necessary for compliance with the HIPAA Security Rule, such as requiring a third party that does not meet the definition of a business associate to enter into a business associate agreement with the covered entity. Another example would be preventing an individual's personal health application from registering with an endpoint (*e.g.*, API) that the covered entity makes public, absent an identified security risk to the ePHI in the covered entity's (or its business associate's) EHR systems.

The Department's view is that, under the Privacy Rule access requirements, covered entities generally must allow every application that wants to register with the API to provide access for an individual, the ability to do so, assuming that it is practicable for the covered entities and absent any Security Rule concerns.[155] Therefore, a covered entity or its business associate that makes available a secure, standards-based API but denies registration, and therefore individual access, to a designated personal health application, or other application that is not being provided on behalf of or at the direction of a covered

---

[154] See proposed 45 CFR 164.514(h)(v), which would require a covered entity to examine risks pursuant to 45 CFR 164.308(b)(2).

[155] The ONC Cures Act Final Rule provides exceptions aligned to the HIPAA Rules to information blocking requirements to prevent harm, for privacy and security. This discussion is consistent with those provisions. *See* 85 FR 25642 (May 1, 2020), 45 CFR 171 Subpart B.

entity, may be in violation of the Privacy Rule requirements for provision of access of individuals to PHI. For example, a health care provider may not deny an application from registering solely because the application does not have a business associate relationship and agreement with the covered entity or because the application offers another service to patients that competes with a service the health care provider offers.

The Department recognizes that due to the variety of circumstances of individuals and entities, a given measure to complete identity verification or request access, such as using an online portal, may be convenient for some individuals and burdensome for others, and practicable for some entities but not for others. Due to this variability, the Department does not propose to require that covered entities implement any particular measure, nor require covered entities to analyze and adopt the least burdensome measure possible for each individual. Further, the Department does not intend to impede the ability of covered entities to comply with any applicable federal or state law provisions that provide greater privacy or security protections related to verification of identity to access medical records, provided that the identity verification measures used and the manner in which they are implemented do not impose unreasonable burdens on an individual's exercise of the right of access.[156] Rather, the Department would expect covered entities to avoid imposing measures that would require unnecessary effort or expense by an individual and to provide individuals with some flexibility (*e.g.*, by accepting verification and access requests by more than one practicable measure).

---

[156] For example, Privacy Act guidelines for federal agencies state, "A requester need not state his [or her] reason for seeking access to records under the Privacy Act, but an agency should verify the identity of the requester in order to avoid violating subsection (b) [of that Act.] https://www.justice.gov/opcl/individuals-right-access. *See* OMB Guidelines, 40 FR 28948, 28957-58 (July 9, 1975), available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf. *See also* 5 U.S.C. § 552a(i)(1) (imposing criminal penalties for disclosure of information to parties not entitled to receive it); 5 U.S.C. § 552a(i)(3) (imposing criminal penalties for obtaining records about an individual under false pretenses); *cf., e.g.,* 28 CFR 16.41(d) (DOJ regulation regarding the verification of identity). *See also* OMB guidance on Privacy Act implementation available at https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/.

3. Request for Comments

The Department requests comments on the above proposal, including:

a. Please describe any circumstances in which individuals have faced verification barriers to exercising their Privacy Rule rights, as well as examples of verification measures that should be encouraged as convenient and practicable, in comparison to those that should be prohibited as per se unreasonable. Please also describe any circumstances related to unreasonable verification measures imposed on third parties to whom an individual directs a copy of PHI.

b. What verification standard should apply when a covered health care provider or health plan submits an individual's access request to another covered health care provider or health plan? Specifically, should the covered entity that holds the requested PHI be required to verify the identity and authority of the covered entity that submitted the request, but be permitted to rely on the requesting entity's verification of the identity of the individual (or personal representative)?

c. How could or should covered entities consider the costs of implementation when evaluating whether a verification method is practicable?

d. Whether the proposal would support individuals' access rights by reducing the verification burdens on individuals, and any potential unintended adverse consequences.

e. Whether a different identity verification standard should apply when an individual requests access, as compared to when a personal representative requests access on the individual's behalf.

f. Examples of state law identity verification requirements that apply when a covered entity provides PHI to an individual or personal representative, or fulfills an individual's request to direct a copy of PHI to a third party. Please provide input on

whether any state law identity verification requirements create a barrier to or unreasonably delay an individual's exercise of the right of access in a manner that should be considered inconsistent with the Privacy Rule.

C. Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management (45 CFR 160.103)

1. Current Provision and Issues to Address

The Privacy Rule expressly permits certain uses and disclosures of PHI, without an individual's valid authorization, for treatment and certain health care operations, among other important purposes.[157] The definitions of both treatment and health care operations include some care coordination and case management activities. For example, the Privacy Rule definition defines treatment to include "the provision, coordination, or management of health care."[158] The definition of health care operations includes, among other activities, "… population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination . . . and related functions that do not include treatment."[159]

The preamble to the 2000 Final Privacy Rule states that certain activities "may be considered either health care operations or treatment, depending on whether population-wide or patient-specific activities occur, and if patient-specific, whether the individualized communication with a patient occurs on behalf of a health care provider or a health plan. For example, a telephone call by a nurse in a doctor's office to a patient to discuss follow-up care is a treatment activity. The same activity performed by a nurse working for a

---

[157] *See* 45 CFR 164.506. 45 CFR 160.103 defines "Disclosure" as "release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information"; The term "Use" is defined as "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information with an entity that maintains such information."

[158] *See* 45 CFR 164.501, definition of "Treatment."

[159] *See* 45 CFR 164.501, definition of "Health care operations."

health plan would be a health care operation."[160] Therefore, the Privacy Rule contemplates that health plans would—as part of health care operations—conduct the types of activities described in this NPRM as care coordination and case management not only at the population level across multiple enrolled individuals but also at the individual level for unique patients including providing for their care across different settings.[161]

Despite this guidance published in the preamble to the 2000 Privacy Rule,[162] some covered entities appear to interpret the existing definition of health care operations to include only *population-based* care coordination and case management, which would have the effect of excluding individual-focused care coordination and case management by health plans. Since health plans do not perform treatment functions as defined by HIPAA, such an interpretation could limit a health plan's ability to perform such individual-level care coordination or case management activities.

While the 2018 RFI did not specifically request comment on the definitions of treatment or health care operations, both of which include care coordination activities, some covered entities expressed uncertainty regarding whether the use or disclosure of PHI for a particular care coordination or case management activity is permitted as part of treatment, health care operations, both, or neither. Some covered entities reported that, due to uncertainty about which provisions apply in certain circumstances, they do not request or disclose PHI even when doing so would support coordinated care and the transformation of the health care system to value based care.

2. Proposal

---

[160] 65 FR 82462, 82627 (December 28, 2000).
[161] This NPRM describes such activities as "population-based" and "individual-level" care coordination and case management, respectively.
[162] 65 FR 82462, 82627 (December 28, 2000).

The Department proposes to clarify the definition of health care operations in 45 CFR 164.501 to encompass all care coordination and case management by health plans, whether individual-level or population-based. The proposal would provide clarity to covered entities and individuals regarding which Privacy Rule standards apply to which care coordination and case management activities, and thereby facilitate those beneficial activities. The clarification also would complement and enhance the proposal in this NPRM to modify the minimum necessary standard to promote uses and disclosures for care coordination and case management for treatment or health care operations by covered health care providers and health plans. The Department believes that, as drafted, the placement of commas separating the list of activities following the term "population-based activities" permits the interpretation that the term "population-based activities" modifies (*i.e.*, places a condition on) all of the activities listed between the semi-colons, including case management and care coordination, although the Department has not placed that interpretation on the definition of health care operations. In order to clearly convey that the activities listed are each separate types of health care operations, the Department proposes to change the commas into semi-colons. The new definition proposed in paragraph (1) of the definition of "Health care operations" in 45 CFR 164.501 would read as follows:

> . . . population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

The Department believes this change in punctuation would clarify that health care operations encompasses all care coordination and case management activities by health plans and covered health care providers, whether population-based or focused on

particular individuals, and thus would increase the likelihood of these entities' using and disclosing PHI for such beneficial activities.

3. Request for Comments

The Department requests comments on the benefits and costs of clarifying the definition of health care operations, including information on how, if at all, this clarification would affect covered entities' decision-making regarding uses and disclosures of PHI for these purposes, and on any potential unintended adverse consequences.

D. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-level Care Coordination and Case Management (45 CFR 164.502(b)(2))

1. Current Provision and Issues to Address

The Privacy Rule generally requires that covered entities use, disclose, or request only the minimum PHI necessary to meet the purpose of the use, disclosure, or request.[163] This minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate use and disclosure of PHI.[164] While the standard is an important privacy protection that is consistent with foundational federal information privacy policy,[165] the Department believes that there is room for flexibility in the application of the standard without sacrificing key privacy protections.

---

[163] *See* 45 CFR 164.502(b)(1).

[164] "Use" in this context refers to internal utilization and sharing of PHI within a covered entity or business associate. *See* 45 CFR 160.103.

[165] *See* Advisory Committee on Automated Personal Data Systems, Report: "Records, Computers and the Rights of Citizens," ASPE (1973) available at https://aspe.hhs.gov/report/records-computers-and-rights-citizens. *See also*, "Guidelines for the Protections of Privacy and Transborder Flow of Personal Data*,"* Organization for Economic Cooperation & Development (1981, revised in 2013), available at http://www.oecd.org/sti/ieconomy/privacy.htm.

The Privacy Rule's minimum necessary requirements are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity and to avoid creating unnecessary barriers to information sharing for permitted purposes. Accordingly, the minimum necessary standard gives a covered entity that receives a request for PHI from another covered entity (and certain non-covered entities) the ability to rely on the requestor's assessment of what it needs, if such reliance is reasonable under the circumstances.[166] For example, a covered health care provider may determine that it is reasonable to rely on a health plan's representations that the plan is requesting the minimum necessary PHI to conduct a medical necessity determination for payment purposes. The disclosing provider is not required to make its own independent assessment of what is the minimum necessary PHI that can be disclosed to meet the request.[167] As another example, a health plan may rely on the representations of a public health authority, including a person or entity acting under a grant of authority from, or under a contract with, a public health authority, requesting PHI that the information requested is the minimum necessary for the stated purposes, such as preventing or controlling disease, provided that the authority is authorized by law to collect or receive information for the requested purposes.[168]

The minimum necessary standard also includes important exceptions to facilitate the provision of health care to individuals. Most importantly, the minimum necessary standard does not apply to disclosures to, or requests by, a health care provider for treatment purposes[169]—an exception intended to avoid creating barriers or delays in providing patient care. For example, a hospital that discloses PHI to an inpatient

---

[166] *See* 45 CFR 164.514(d)(3)(iii)(B).
[167] *See* 45 CFR 164.514(d)(3)(iii)(B) stating that a covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:… "(B) The information is requested by another covered entity".
[168] *See* 45 CFR 164.514(d)(3)(iii)(A) and 45 CFR 164.512(b)(1)(i). *See also* definition of "Public health authority", 45 CFR 164.501.
[169] *See* 45 CFR 164.502(b)(2)(i).

rehabilitation facility to coordinate patient care is making a disclosure to a health care provider for treatment that is not subject to the minimum necessary standard, regardless of whether the facility is covered by the HIPAA Rules. However, while disclosures of PHI to health care providers for treatment, including for case management and care coordination, are excluded from the minimum necessary standard, uses of PHI for treatment must adhere to the minimum necessary standard.[170] With respect to uses of PHI, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the PHI to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access.[171]

The Privacy Rule also permits certain uses and disclosures of PHI for care coordination and case management that are considered health care operations activities, and thus are subject to the minimum necessary standard.[172] For example, the Privacy Rule permits a covered health care provider or health plan to use or disclose only the minimum necessary PHI for population-based case management, such as to identify all patients or enrollees with diabetes and send them information about a recommended healthy diet to facilitate diabetes self-management.[173]

Finally, under the Privacy Rule, because health plans generally do not perform treatment functions, any care coordination or case management activity conducted by a health plan generally is a health care operation subject to the minimum necessary standard.[174] Thus, the current rule imposes greater restrictions on disclosures to and requests by health plans than on disclosures to and requests by covered health care

---

[170] *See* 45 CFR 160.103 definition of "Use" as "the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."
[171] *See* 45 CFR 164.514(d)(2)(i).
[172] *See* 45 CFR 164.501, definition of "Health care operations."
[173] *See* 45 CFR 164.502(b)(1)-(2), identifying when the minimum necessary standard applies and does not apply.
[174] *See* 45 CFR 164.501, definition of "Health care operations."

providers when conducting care coordination or case management activities related to an individual.

In the 2018 RFI, the Department requested public input on whether it should expand the exceptions to the minimum necessary standard to include uses and disclosures for additional activities related to care coordination and case management.[175] For example, the Department asked whether the exceptions to the minimum necessary standard should be expanded to include payment and health care operations activities such as population-based care coordination and case management activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development.[176] Comments varied widely, even within the general categories of commenters (*e.g.*, health care providers or consumers).

Many commenters supported expanding the exceptions to the minimum necessary standard for care coordination and case management. These commenters stated that such an expansion would allow providers to better coordinate and manage patient care across systems and delivery models. Some health care professionals who supported additional exceptions expressed concern that their interpretation of "necessary" might not be correct, and that they would be "punished" under the existing standard for an impermissible use or disclosure of PHI. Some commenters reported that this uncertainty about compliance requirements creates fears that may result in less information sharing, and therefore less efficient and effective care.

In contrast, over half of the responsive commenters opposed adding exceptions to the minimum necessary standard. Many commenters expressed strong concerns that a broader exception could undermine patient privacy or lead to unspecified harm to patients, some specifically noting that the minimum necessary standard is the only requirement for

---

[175] *See* 83 FR 64302 (December. 14, 2018).
[176] *Ibid*.

covered entities to consider what information is reasonably needed for their purpose before making a request, use, or disclosure. Others asserted that if health care operations activities were excepted from the standard, there would be no clear boundaries and covered entities likely would disclose entire patient records to each other, when convenient, without effective limit. In addition, some covered health care provider commenters expressed fear of an increase in requests for large volumes of data that would overwhelm their capacity.

2. Proposal

To consistently promote permissible disclosures of PHI for care coordination and case management, the Department proposes to add an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management.[177] The exception would apply only to those care coordination and case management activities that are at the individual level, in recognition of the concerns expressed by commenters that this proposal would weaken patient privacy by permitting additional PHI to flow for these purposes.

Health plans and covered health care providers would continue to be responsible for meeting the minimum necessary requirements that apply to: (1) disclosures of PHI for health care operations other than individual-level care coordination and case management; (2) disclosures of PHI for care coordination and case management to most entities other than health care providers and health plans, such as social services agencies or transitional supportive housing authorities; (3) uses of PHI for care coordination and case management, whether as part of treatment or health care operations; and (4) uses, requests, and disclosures of PHI for other purposes, including all population-based activities, when

[177] *See* proposed 45 CFR 164.502(b)(2)(vii).

applicable.[178] In addition, covered entities would continue to be able to agree to and honor an individual's request not to use or disclose information for these purposes, as provided in the Privacy Rule and the ONC Cures Act Final Rule information blocking exception for respecting an individual's request.[179]

This proposal would relieve covered entities from the requirement to make determinations about the minimum information necessary when the request is from, or the disclosure is made to, a covered health care provider or health plan to support individual-level care coordination and case management activities. The proposal would also remove the disincentive to disclose and request PHI to support care coordination and case management based on uncertainty about applicable permissions and fear of being subject to penalties for noncompliance resulting from such uncertainty. For example, when a health plan requests a disclosure for care coordination or case management to facilitate an individual's participation in the plan's new wellness program, a requesting health plan or covered health care provider would be relieved of the responsibility for determining the minimum necessary amount of PHI for the purpose and the disclosing health plan or covered health care provider would be relieved of the responsibility of assessing whether reliance on the health plan's determination of the minimum necessary PHI for its purpose is reasonable under the circumstances. As another example, when a covered health care provider contacts a health plan to coordinate potential mental health treatment referrals for a patient, the provider would not need to consider what information is the minimum necessary to disclose to the health plan for this purpose. In fact, the ONC Cures Act Final Rule would prohibit a health care provider from limiting a permissible disclosure to what the provider believes to be the minimum necessary information when the Privacy Rule specifically excepts the disclosure from the minimum necessary standard. However, the

---

[178] *See* 45 CFR 164.502(b); 164.514(d).
[179] *See* 45 CFR 164.522(a); 171.202(e).

provider still could honor an individual's request for restrictions on disclosures of PHI,[180] consistent with the ONC Cures Act Final Rule privacy sub-exception for respecting an individual's request not to share information.[181]

This proposed exception would enable health plans and covered health care providers to more easily and efficiently request and disclose PHI for care coordination and case management for individuals, and would complement the proposal in this NPRM to create an express permission for covered entities to disclose PHI for care coordination and case management, which is described below.

3. Request for Comments

The Department requests comments on the above proposal, and the following considerations in particular:

a. Would the proposed exceptions improve the ability of covered entities to conduct care coordination and case management activities? Why or why not? Please provide any cost or savings estimates that may apply both on the entity level and across the health care system.
b. Please provide examples of particular care coordination or case management activities that would be furthered or impeded by this proposal.
c. Please describe any unintended negative consequences of the proposed changes for the privacy of PHI or the health information rights and interests of individuals. Would there be any negative impact, in particular, on certain populations (*e.g.*, people with disabilities, older adults, rural dwellers, persons experiencing mental health conditions and/or substance use disorders or other illnesses, or others)?

---

[180] *See* 45 CFR 164.522.
[181] *See* 45 CFR 171.201(e).

d. Would the proposed changes have similar or different effects on the activities of health plans versus health care providers? Are there unintended consequences for other ancillary providers including social services agencies, community based organizations, and HCBS providers? Please describe.

e. What alternative regulatory modifications or clarifying guidance might achieve the same or greater improvements in care coordination or case management?

f. A health care provider that refused to disclose PHI would not be considered to be information blocking when a state or federal law requires one or more preconditions for providing access, exchange, or use of electronic health information and the precondition has not been satisfied.[182] This proposed modification would remove one of the minimum necessary policy "preconditions" for refusing to respond to a request for an individual's PHI without violating the information blocking prohibition. How would the information blocking provisions in the ONC rule interact with these modifications, and are there any adverse unintended consequences that might result, such as covered entities requesting and receiving far more than the minimum amount of PHI necessary for individual-level care coordination and case management and using PHI for other unrelated purposes?

g. Some disclosures for payment purposes with respect to an individual's health care are related to care coordination and case management (*e.g.,* review of health care services for appropriateness of care). Disclosures for payment purposes are subject to the minimum necessary standards. Should all or certain individual-level payment activities be included in the proposed exception?

---

[182] As noted elsewhere in this preamble, the ONC Cures Act Final Rule defines information blocking, in part, as a practice that, if "conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information. *See* 45 CFR 171.103 *Information blocking and* § 171.202 Privacy exception (b) *Sub-exception – precondition not satisfied.*

h. Please provide additional examples of circumstances in which it should be considered reasonable, or unreasonable, to rely on the representations of another entity that it is requesting the minimum necessary PHI.

E. Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management that Constitutes Treatment or Health Care Operations (45 CFR 164.506)

1. Current Provisions and Issues to Address

Section 45 CFR 164.506 sets forth the permissible uses and disclosures of PHI to carry out TPO. Section 45 CFR 164.506(b)(1) permits, but does not require, covered entities to obtain an individual's consent to use or disclose their PHI for TPO purposes,[183] while 45 CFR 164.506(c) describes the implementation specifications for TPO uses and disclosures, including 45 CFR 164.506(c)(1), which expressly permits a covered entity to use and disclose PHI for its own TPO. OCR guidance provides an example of how this Privacy Rule provision permits covered health care providers to disclose PHI to public or private-sector entities that provide health-related social and community based services as part of the disclosing provider's treatment activities:[184]

> A health care provider may disclose a patient's PHI for treatment purposes without having to obtain the authorization of the individual. Treatment includes the coordination or management of health care by a health care provider with a third party. Health care means care, services, or supplies related to the health of an individual. Thus, health care providers who believe that disclosures to certain social service entities are a necessary component of,

[183] A consent that a covered entity chooses to obtain consistent with 45 CFR 164.506(b) is different from an authorization obtained under 45 CFR 164.508, which is required for certain uses and disclosures of PHI.

[184] The disclosure of patient information for treatment and other purposes may be subject to other laws, including 42 CFR Part 2 for substance use disorder records.

> or may help further, the individual's health or mental health care may disclose the minimum necessary PHI to such entities without the individual's authorization. For example, a provider may disclose PHI about a patient needing mental health care supportive housing to a service agency that arranges such services for individuals. [185]

The guidance explains the circumstances in which the Privacy Rule permits a covered health care provider to disclose PHI about an individual to a third party when the third party is part of the broader health treatment plan, or participating in the coordination of care, for an individual.[186] Such a treatment disclosure generally is subject to the minimum necessary standard, where the disclosure is made to a third party entity that is not a health care provider, even though the entity is providing health-related services.[187]

Under the Privacy Rule, a covered health care provider is able to make a disclosure for treatment purposes of an elderly or disabled patient by disclosing PHI to a home and community based services (HCBS)[188] provider if it is for the coordination or management of treatment by the health care provider.[189] For example, a health care provider may disclose the minimum necessary PHI to a senior center or adult day care provider to help coordinate necessary health-related services for an individual, such as arranging for a home aide, to help the older adult or disabled person with their prescibed

---

[185] *See* HHS Office for Civil Rights, Frequently Asked Questions on Mental Health, Disclosures for Care Coordination (2018), available at https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html. A consent that a covered entity chooses to obtain consistent with 45 CFR 164.506(b) is different from an authorization obtained under 45 CFR 164.508, which is required for certain uses and disclosures of PHI.

[186] *Ibid*. However, the disclosure of patient information for treatment and other purposes may be subject to other laws, including 42 CFR Part 2 for substance use disorder records.

[187] *See* 45 CFR 164.502(b)(2)(i).

[188] Information about HCBS is available at https://www.medicaid.gov/medicaid/hcbs/index.html. Some HCBS providers also may be health care providers within the definition at 45 CFR 160.103, in which case the disclosing provider could disclose PHI for the receiving HCBS provider's treatment purposes. *See* 45 CFR 164.506(c)(2).

[189] *See* 45 CFR 164.506(c).

at-home or post-discharge treatment protocol. Likewise, a disclosure could also facilitate care coordination and case management as part of a covered health plan's health care operations, such as when a health plan discloses the PHI of a senior citizen to a senior wellness center as part of the plan's wellness program in which the senior citizen is enrolled.

Despite the guidance on this topic, OCR has heard that many covered entities make disclosures to third parties that are commonly referred to as social services agencies and community based organizations, and to HCBS providers, only after obtaining a valid authorization from the individual. Similarly, some covered entities never disclose PHI to these health-related service providers, even when a treating provider specifies the service as part of a treatment plan or when it would enable the covered health care provider's treatment of the individual across a care continuum (*e.g.*, from inpatient to home or HCBS setting). Some covered entities may not be aware that the Privacy Rule contemplates disclosures of PHI to third party organizations without authorization for care coordination and case management, including when required by law.[190] Other covered entities may be uncertain about the scope of the permission to disclose, and may fear that they will inadvertently violate the HIPAA Rules, as the current regulatory provisions permitting disclosures for treatment do not expressly list these types of entities as permissible recipients of PHI.

The 2018 RFI requested comments on whether the Department should modify the Privacy Rule to clarify the scope of and eliminate any confusion about a covered entitity's ability to disclose PHI to third parties, such as social services agencies, community based organizations, and HCBS providers,[191] as necessary for a disclosing health care provider to carry out a treatment plan, or for a disclosing health plan to conduct care coordination and

---

[190] *See* 45 CFR 164.506(c) and 164.512(a).

[191] The Department intends to include other types of organizations that are similar to these named examples.

case management as health care operations. Health care associations, information technology (IT) vendors, health plans, and health care providers commented on this topic.

Some supportive commenters urged the Department to clarify the permissions for covered entities by modifying the regulation text to reduce any confusion on the part of covered entities about their ability to disclose PHI to the types of entities that typically partner with providers and (in some cases) health plans to improve those covered entities' own treatment- or health care operations-based care coordination and case management for the individual. Most commenters also stated that such a regulatory change should include a definition of social services agencies with examples of the types of services contemplated. Several commenters recommended that the Department permit disclosures of PHI with these organizations only with an individual's consent.

Some health plan commenters stated that an express regulatory permission for covered entities to disclose PHI to social services agencies for care coordination and case management purposes would be helpful, but recommended placing some limits on the permission, such as only permitting disclosures with patient consent. Several health plans described the care coordination and case management activities they would like to provide to their plan members, including working closely with community based organizations and/or multi-disciplinary teams to address the social determinants of health, without first receiving the individual's valid authorization; and coordinating comprehensive wraparound services, including clinical and behavioral health care, social services, and patient advocates to support certain populations, such as people experiencing SMI or SUD. The Department finds the comments by health plans to be persuasive in demonstrating the need to propose an express permission to disclose PHI for individual-level care coordination and case management activities that constitute health care operations.

Not all commenters supported addressing disclosures to third parties including social services agencies, community based organizations, and HCBS providers through rulemaking. Some correctly stated that covered health care providers already are permitted to make such disclosures, and therefore the commenters did not believe a change in the regulation was needed. Others specifically opposed expanding disclosures to any law enforcement entity that may be part of a multi-disciplinary team, expressing concern that law enforcement intrusions into health records can deter patients from seeking needed care, especially if law enforcement has broad access to SUD treatment information.

2. Proposal

The Department proposes to modify 45 CFR 164.506(c) to add a new subsection 164.506(c)(6). This new subsection would expressly permit covered entities to disclose PHI to social services agencies, community based organizations, HCBS providers, and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered health care provider or as a health care operations activity of a covered health care provider or health plan. Under this provision a health plan or a covered health care provider could only disclose PHI without authorization to a third party that provides health-related services to individuals; however, the third party does not have to be a health care provider. Instead, the third party may be providing health-related social services or other supportive services--*e.g.*, food or sheltered housing needed to address health risks. Section 45 CFR 164.501 of the Privacy Rule defines treatment as "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to

another." Section 45 CFR 164.501 paragraph (1) of the current Privacy Rule definition of health care operations also refers to case management and care coordination.[192] This express permission would allow a covered entity to disclose PHI to these third party entities that provide or coordinate ancillary and other health-related services when the covered entity determines that the disclosure is needed to provide health-related services to specific individuals for individual-level care coordination and case management activities that constitute treatment or health care operations, as applicable.[193] For example, a covered entity could disclose the PHI of a senior individual experiencing chronic illness to a senior center attended by the individual to check on his or her health periodically, and to ask the senior center to give reminders about effective disease self-management.

The Department notes that there may be instances in which some disclosures for care coordination and case management, for treatment or health care operations, -will be made to business associates engaged by a covered entity, such as a health plan, to provide health-related services to an individual, or that relate to an individual's health care, on behalf of the plan. In such cases, the covered entity must have a HIPAA compliant business associate agreement in place prior to disclosing the PHI for this purpose. In other cases, the entity receiving the PHI will be providing health-related services on its own behalf, and not performing covered activities or functions for or on behalf of the disclosing covered entity. In the latter situation, a business associate agreement is not required, because the entity receiving the PHI does not meet the definition of a business associate.[194]

---

[192] This NPRM includes a proposal to change the punctuation in paragraph (1) of the definition of health care operations at 45 CFR 164.501 to make clear that care coordination and case management are not limited to "population-based activities." *See* proposed 45 CFR 164.501.
[193] *See* proposed 45 CFR 164.506(c)(6).
[194] *See* the definition of "Business associate" at 45 CFR 160.103. Whether the Privacy Rule permits a particular disclosure for health care operations is determined separately from whether a business associate agreement is required. These provisions of the rule operate independently, such that disclosures for health care operations may be made to an entity that is neither a covered entity nor a business associate of the covered entity. *See, e.g.,* 65 FR 82462, 82491 (December 28, 2000).

The express permission for disclosures to these third party entities is being proposed primarily to facilitate the treatment and health care operations of the disclosing covered entities in cases where a disclosure will serve the health care or health-related needs of individuals. The Department's understanding is that, in general, the third party entities receiving PHI under this proposed permission would not be covered entities and thus, the PHI disclosed to them would no longer be protected by the HIPAA Rules. However, because some of these third party recipients of PHI may be health care providers or covered health care providers under HIPAA,[195] which can perform care coordination and case management for their own treatment activities (and, with respect to covered health care providers, for health care operations), the Department does not propose to limit the regulatory text of the permission to disclosures made by a covered health care provider or health plan as part of *the discloser's own* treatment and health care operations. For example, under this proposal a covered health care provider could expressly disclose PHI for the case management and care coordination activities of another health care provider or health plan. Such disclosures are permitted under the current rule at 45 CFR 164.506(c)(2) and (c)(4); however, the Privacy Rule currently does not address the applicability of this permission to case management and care coordination. The Department requests comment on whether such limiting language would be appropriate.

Although the Department believes that such disclosures generally are permitted under the existing Privacy Rule for treatment or certain health care operations, this additional, express regulatory language would provide greater regulatory clarity, and help ensure that covered entities are able to disclose PHI to coordinate care for individuals with social services agencies, community based organizations, and HCBS providers or other similar third parties that are providing health-related services to those individuals. The

---

[195] *See* the definitions of "Health care provider" and "Covered entity" at 45 CFR 160.103.

Department acknowledges that some RFI commenters expressed concerns about expressly permitting such disclosures without individuals' authorization or consent. In response, the Department notes that, similar to its proposal to except certain care coordination and case management disclosures from the minimum necessary standard, it also proposes to limit the scope of this permission to disclosures by covered entities for care coordination and case management for individuals (whether as treatment or health care operations, depending on whether the covered entity is a health care provider or a health plan, respectively), rather than population-based activities. The Department believes that the limitation to individual-level activities will ensure that the disclosures made under this permission would be akin to disclosures for treatment, which individuals expect to occur without their needing to provide an authorization or consent. The existing Privacy Rule right to request restrictions on disclosures for treatment, payment, and health care operations purposes under 45 CFR 164.522(a) also remains available for individuals to request more limited disclosures.

The Department believes this change would facilitate and encourage greater wraparound support and more targeted care for individuals, particularly where it would be difficult to obtain an individual's authorization or consent in advance, because the individual cannot easily be contacted (*e.g.,* when an individual is homeless). This improved care coordination and case management could lead to better health outcomes while retaining existing limits on population-based disclosures. At this time, the Department proposes to place examples of the third party recipient entities in regulatory text but does not propose definitions of care coordination and case management that such third parties must conduct to be appropriate recipients of PHI for these purposes. The Department believes the robust description and discussion of stakeholder definitions for "care coordination and case management" affords the regulated community sufficient

information with which to determine whether a recipient is engaged in the contemplated activities.

3. Request for Comments

The Department requests comments on the above proposal, and the following considerations in particular:

a. Whether the proposal to create an express permission to disclose PHI to certain third parties for individual level treatment and health care operations would help improve care coordination and case management for individuals, and any potential unintended adverse consequences.

b. Whether the proposal poses any particular risks for individuals related to permitting disclosures without authorization for individual-level care coordination and case management activities that are health care operations (*i.e.,* those that are conducted by health plans) in addition to individual-level care coordination and case management activities that constitute treatment (*i.e.,* those that are conducted by health care providers).

c. Would the proposed change remove perceived barriers to disclosure of PHI, as appropriate, to social services agencies, community-based organizations, and HCBS providers to better enable care coordination and case management? Are there other entities the Department should identify in regulatory text as examples of appropriate recipients of PHI under the proposed permission?

d. Should the proposed change be limited to care coordination and case management for a particular individual as proposed, or should it also include population-based efforts?

e. Would this permission to disclose PHI for case management and care coordination to the entities described above interact with the ONC information blocking requirement

to create any unintended adverse consequences for individuals' privacy? Please explain.

f. Should the Department specify the types of organizational entities to be included as recipients of PHI in this express permission in regulation text, as well as limitations or exclusions, if any, that should be placed on the types of entities included? If yes, what types of organizational entities should be included or excluded?

g. Should the Department limit the proposed permission to disclose PHI to circumstances in which a particular service provided by a social services agency, community-based organization, or HCBS provider is specifically identified in an individual's care plan and/or for which a social need has been identified via a screening assessment? Should the Department require, as a condition of the disclosure, that the parties put in place an agreement that describes and/or limits the uses and further disclosures allowed by the third party recipients?

h. To what extent are social services agencies, community-based organizations, and HCBS providers covered health care providers under HIPAA? How many are non-covered health care providers? Are any such entities covered under HIPAA as health plans?

F. Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances (45 CFR 164.502 and 164.510-514)

Support from family members, friends, and caregivers is key to helping people experiencing substance use disorder (SUD) or serious mental illness (SMI).[196] However,

---

[196] *See* Substance Abuse and Mental Health Administration, *Mental Health and Substance Use Disorders,* which defines these terms as follows: Serious mental illness is defined by someone over 18 having (within the past year) a diagnosable mental, behavior, or emotional disorder that causes serious functional impairment that substantially interferes with or limits one or more major life activities. Substance use disorders occur when the recurrent use of alcohol and/or drugs causes

individuals' family members and caregivers cannot help if they are not informed. Therefore, to encourage covered entities to share information in individuals' best interests, without fear of HIPAA penalties, the Department proposes to amend five provisions of the Privacy Rule to replace "the exercise of professional judgment" standard with a standard permitting certain disclosures based on a "good faith belief" about an individual's best interests. Further, to better enable covered entities to prevent and lessen harm to individuals or the public, the Department proposes to replace the Privacy Rule provision that currently permits a covered entity to use or disclose an individual's PHI based on a "serious and imminent threat" with a "serious and reasonably foreseeable threat" standard. These provisions and the proposed amendments are discussed in detail below.

1. Current Provisions and Issues to Address

Disclosures to personal representatives

Under 45 CFR 164.502(g) of the Privacy Rule, a personal representative is a person with authority under applicable law (*e.g.*, state law) to act on behalf of an individual in making decisions related to health care.[197] In general, the Privacy Rule treats a personal representative in the same way it treats the individual; thus, for example, a personal representative is able to exercise the individual's right to obtain PHI about the

---

clinically significant impairment, including health problems, disability, and failure to meet major responsibilities at work, school, or home. For minors, the term "Serious Emotional Disturbance" refers to a diagnosable mental, behavioral, or emotional disorder in the past year, which resulted in functional impairment that substantially interferes with or limits the child's role or functioning in family, school, or community activities. Available at https://www.samhsa.gov/find-help/disorders.

[197] 45 CFR 164.502(g)(3)(i) lists exceptions to this general rule, specifying that such a person may not be a personal representative with respect to information pertaining to a health care service if: (A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or (C) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

individual.[198] In many circumstances, the parent or guardian of an unemancipated minor child is treated as the minor's personal representative under applicable law. In addition, to address circumstances in which state or other applicable law does not treat a parent as an unemancipated minor's personal representative, the provision at 45 CFR 164.502(g)(3)(ii)(C) permits, but does not require, covered entities to provide access under 45 CFR 164.524 to a parent, guardian or other person acting in *loco parentis* who is not a personal representative under applicable law, if the action is consistent with state or other applicable law, and the decision to disclose is based on the professional judgment of a licensed health care professional.

Uses and disclosures requiring an opportunity for the individual to agree or object

Under 45 CFR 164.510, covered entities, including health care providers, generally must provide an individual with the opportunity to agree or object before using or disclosing the individual's PHI for inclusion in a facility directory or disclosing PHI to family members, caregivers, or others involved in care or payment for care. However, individuals are not always able to agree or object to such uses or disclosures, particularly in emergency situations.

Accordingly, 45 CFR 164.510(a)(3) permits a covered health care provider to disclose facility directory information, including name, location within the provider's facility, general condition, and religious affiliation to clergy and others, such as family members, who ask for the individual by name, when the individual cannot agree or object due to incapacity or an emergency treatment circumstance, if: (A) consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and (B) the disclosure is in the individual's best interests, as determined by the covered health care provider, in the exercise of professional judgment.

---

[198] *See* 45 CFR 164.502(g)(1).

A similar rationale applies to 45 CFR 164.510(b), which recognizes that family members and other caregivers have a legitimate need to obtain the information that will permit them to continue to participate in the individual's care when it is in the individual's best interests, particularly in emergency circumstances. Currently, 45 CFR 164.510(b)(2)(iii) permits a covered entity to disclose relevant PHI about an individual who is present and has decision- making capacity, if the covered entity can reasonably infer, based on the exercise of professional judgment, that the individual does not object to the disclosure. Further, 45 CFR 164.510(b)(3) permits a covered entity to disclose relevant PHI about an individual who cannot agree or object due to incapacity or an emergency circumstance to family members and other caregivers involved in the individual's care or payment for care, if the covered entity, based on professional judgment, determines that the disclosure is in the best interests of the individual.

Identity Verification

Section 164.514(h)(2)(iv) of title 45 CFR generally requires covered entities to establish and use written policies and procedures reasonably designed to verify the identity and authority of the requestor of PHI.[199] However, certain circumstances surrounding the disclosure itself may accomplish the verification without having to collect additional documents or rely on a pre-established procedure.[200] Therefore, 45 CFR 164.514(h)(2)(iv) provides that a covered entity's obligation to verify a requestor's identify is met if the covered entity relies on an exercise of professional judgment pursuant to 45 CFR 164.510, or acts on a good faith belief in making a disclosure pursuant to 45 CFR 164.512(j) to prevent or lessen certain serious and imminent threats.

Uses and disclosures to avert a serious threat to health or safety

---

[199] *See* 65 FR 82462, 82546 (December 28, 2000).
[200] *Ibid.*

Section 164.512(j) of title 45 CFR permits covered entities, "consistent with applicable law and standards of ethical conduct," to rely on a good faith belief to use or disclose PHI when necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[201] The permission is intended to accommodate, and be consistent with, a "duty to warn" third parties of a threat as established in case law (and, in some states, statutory requirements).[202] Certain conditions apply, including that the recipient of the PHI must be reasonably able to prevent or lessen the threat, or the use or disclosure must be necessary for law enforcement to identify or apprehend the subject individual.[203] In the case of a disclosure to law enforcement, additional conditions include that the individual made a statement admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, or that circumstances demonstrate that the subject individual escaped from a correctional institute or lawful custody, as defined in the Privacy Rule.[204]

Relevant guidance encouraging disclosures of PHI to help individuals experiencing opioid use disorder or mental illness

On October 27, 2017, in response to the nation's opioid crisis, OCR issued guidance titled *How HIPAA Allows Doctors to Respond to the Opioid Crisis*.[205] The guidance addresses the HIPAA permission for covered health care providers to share PHI with an individual's friends, family, and others involved in the individual's care or the

---

[201] *See* 45 CFR 164.512(j)(1)(i)(A). To "lessen" a threat could mean, for example, to reduce the severity of the threat, or the likelihood of the anticipated harm occurring.
[202] *See* 65 FR 82462, 82538 (December 28, 2000). *See also* state law requirements compiled at http://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx. To the extent that state or other law requires a disclosure (*e.g.*, as part of a statutory duty to warn), the Privacy Rule would permit the disclosure under its permission for uses and disclosures of PHI required by law. *See* 45 CFR 164.512(a). However, not all states have enacted such requirements, and those that do apply a variety of different standards. In contrast, HIPAA's disclosure permission applies a uniform permissive standard to covered entities nationwide.
[203] *See* 45 CFR 164.512(j)(1)(ii).
[204] *Ibid. See also* 164.501, definition of "Correctional institution," including description of "lawful custody."
[205] Guidance on Responding to an Opioid Overdose, HHS Office for Civil Rights (October 27, 2017), available at https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf?language=es.

payment for that care when the individual has overdosed and is unable to agree or object to uses and disclosures of PHI. The guidance clarifies that "a provider may use professional judgment to talk to the parents of someone incapacitated by an opioid overdose about the overdose and related medical information, but generally could not share medical information unrelated to the overdose without permission."[206]

The guidance further clarifies when a covered health care provider may rely on another permission, 45 CFR 164.512(j), in an overdose situation:

> For example, a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if the doctor informs family, friends, or caregivers of the opioid abuse after determining, based on the facts and circumstances, that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge.[207]

Although the guidance focuses primarily on overdose situations, the HIPAA provisions apply equally to the disclosure of PHI during other health emergencies or dangerous situations. The full text of the guidance is available at https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf?language=es.

In addition to guidance addressing the opioid epidemic, OCR has issued guidance to assist individuals experiencing SMI, their families, and other caregivers as required by the Cures Act.[208] Section 11001 of the Cures Act includes a "sense of Congress" that clarification was needed regarding the Privacy Rule's existing permitted uses and disclosures of PHI by health care professionals to communicate with caregivers of adults with SMI to facilitate treatment. Section 11003 directed the Secretary, acting through the Director of OCR, to issue clarifying guidance explaining the circumstances under the

---

[206] *Ibid.*
[207] *Ibid.*
[208] Available at https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf.

Privacy Rule in which a health care provider or other covered entity may disclose PHI, such as in the exercise of professional judgment regarding the best interests of a patient when the patient is incapacitated or in an emergency situation, and the circumstances in which HIPAA permits disclosures of PHI to a patient's family and other caregivers. In response to the requirements in the Cures Act, OCR created new webpages for health care professionals and consumers containing all of its guidance and materials related to mental and behavioral health information.[209]

Despite issuing extensive guidance, OCR continues to hear that some covered entities are reluctant to disclose information to persons involved in the care of individuals experiencing these health issues, even when the Privacy Rule permits such disclosures. For example, since the guidance was published and as recently as July 11, 2018, a patient advocate testified before the Federal Commission for School Safety (FCSS) that, despite OCR's efforts to disseminate guidance, providers continue to "stonewall" families when asked to disclose PHI and routinely withhold medical information from family members, out of concerns of potentially violating HIPAA.[210]

The Department has similarly heard anecdotal accounts that some health care providers are reluctant to disclose needed health information about an incapacitated patient to even their closest friends and family, due to concerns about potential penalties under HIPAA. OCR understands that this reluctance to disclose, even when the Privacy Rule permits disclosure, creates particular difficulties, and potential risks for patients and others, when a patient is unable to agree or object to the disclosure due to incapacity related to SMI, SUD, or another cause.

---

[209] "Information Related to Mental and Behavioral Health, including Opioid Overdose," HHS Office for Civil Rights (2017), available at https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html and https://www.hhs.gov/hipaa/for-individuals/mental-health/index.html.

[210] "Final Report on the Federal Commission on School Safety," Department of Education (December 18, 2018), p. 136, available at https://www2.ed.gov/documents/school-safety/school-safety-report.pdf.

In addition, in the wake of the incidents of mass violence in recent years, such as shootings and acts of terrorism, the Department has heard anecdotes claiming that HIPAA impedes health care providers from disclosing PHI, even when such disclosure could prevent or lessen a serious and imminent threat of harm or violence. According to these accounts, the reluctance to disclose persists even though the HIPAA Rules permit disclosure in such circumstances.

In the 2018 RFI, the Department solicited public input to determine whether and how to modify the Privacy Rule to help combat the opioid crisis, treat SMI, and promote family involvement in the care of individuals experiencing these health situations. It also sought comment on how the Department could amend the Privacy Rule to increase disclosures of PHI by covered health care providers with family members and other caregivers experiencing difficulties obtaining health information about their minor and adult children or parents, spouses, and other individuals when needed to coordinate their care or otherwise be involved in their treatment. Noting anecdotal information suggesting that some covered entities are reluctant to involve the caregivers of individuals facing health crises for fear of violating the Privacy Rule, the Department asked for examples of circumstances in which the Privacy Rule has presented real or perceived barriers to family members attempting to access information.

Many commenters asked the Department to align the Privacy Rule with 42 CFR Part 2 (Part 2), which requires certain federally funded SUD treatment programs (called "Part 2 programs") and downstream recipients (called "lawful holders") of their patient-identifying information to maintain the confidentiality of records related to the diagnosis and treatment of SUD.[211] Part 2 modifications are outside the scope of this rulemaking,

[211] The Part 2 regulations are authorized by section 290dd-2 of Title 42 US Code, which provides that "Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance use disorder education, prevention, training, treatment, rehabilitation, or research, which is

and nothing in this Privacy Rule NPRM would change the Part 2 compliance obligations of covered entities who are subject to Part 2. Further, this NPRM does not affect covered entities' obligations to comply with applicable state laws that restrict the disclosure of sensitive information, including SUD or other sensitive health issues.

On March 27, 2020, Congress enacted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) which requires greater alignment of the Part 2 regulations with the HIPAA Rules.[212] On July 15, 2020, the Department, through the Substance Abuse and Mental Health Services Administration (SAMHSA), published a final rule revising the Part 2 regulations to facilitate such activities as quality improvement and claims management in a manner that more closely aligns Part 2 with some of the disclosure permissions of the Privacy Rule.[213] The Department will implement the CARES Act requirements concerning the Part 2 regulations in a future rulemaking.

Nearly all commenters who identified as family members of patients agreed that in many cases more information related to an individual's SMI or SUD should be disclosed to family caregivers, and shared personal stories about the devastating consequences – such as suicide, missed appointments, homelessness, and lack of continuity in treatment and medication – that occurred because of a lack of information disclosure. A few commenters suggested that HIPAA should preempt all state laws that restrict disclosures of mental and behavioral health information to family members or coordinating health and social services agencies. A few other commenters expressed concern that the inability to disclose PHI related to mental health to social services agencies largely impacts poor individuals and minorities.

---

conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e), be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b)."

[212] *See* Pub.L. 116-136, 134 Stat. 286 (March 27, 2020). Section 3221 of Pub.L. 116-136 amended 42 U.S.C. 290dd-2.

[213] *See* 85 FR 42986 (July 15, 2020).

Commenters who identified as patients or privacy advocacy groups almost universally opposed modifying the Privacy Rule to expand permitted disclosures of information related to SMI and opioid use disorder or other SUDs. Many commenters expressed fear of family members and employers having access to this information, citing potentially adverse consequences, including fear of discrimination, abuse, and retaliation. Many health care providers expressed concern about the chilling effect that increased disclosures would have on individuals seeking treatment for opioid use disorders and stated that the Privacy Rule is already flexible enough to permit the amount of disclosure needed to address the opioid epidemic. Many suggested issuing clarifying guidance on existing regulatory permissions as a preferred approach to increasing disclosures of PHI. A few pointed to the need to leverage technology, such as consent management and data segmentation, pursuant to the health information certification standards[214] published by ONC, as a means to help providers protect sensitive records while accessing information necessary for care.

As the Department noted in the 2018 RFI, the Privacy Rule generally defers to state law with respect to the circumstances in which a parent or guardian is treated as the personal representative of an unemancipated minor child, and under which information may not be disclosed to parents. Many commenters recognized state law, not the Privacy Rule, as the source of the more restrictive provisions (*e.g.*, state laws that restrict access to an unemancipated adolescent's mental health information). Nevertheless, some commenters suggested that HIPAA presented a barrier, especially in cases where a teenager or school-aged child experienced mental illness. Accordingly, some covered entities, professional organizations, advocacy organizations, and parents supported increasing parental access to minors' PHI. Some commenters were particularly supportive of increasing disclosures of PHI involving SUD, SMI, and other behavioral health

[214] *See* 45 CFR Parts 170 and 171.

concerns. However, some commenters raised concerns about abusive parents or guardians gaining access to a minor child's PHI, and some appreciated that the Privacy Rule currently permits a covered entity to deny access to a personal representative suspected of abuse or neglect. In addition, some commenters expressed concern that increasing parental access would inhibit a child from seeking the health care he or she needs, especially with respect to sensitive health conditions.

The Department received a few comments related to adult children being able to access the records of their parents. For example, one commenter suggested that the Department create a "relative caregiver" category with a right to access the medical records of elderly parents; another commenter provided a similar suggestion to address the care of individuals experiencing dementia. In contrast, several commenters raised concerns about impinging on the individual autonomy of their adult parents or other adults, and stressed the importance of protecting privacy for older adults.

2. Proposals

The Department believes more can be done to encourage health care providers to disclose PHI when families and other caregivers of individuals are attempting to assist with health related emergencies, SUD (including opioid disorder) or SMI, and other circumstances in which individuals are incapacitated or otherwise unable to express their privacy preference. To address these concerns, the Department proposes several modifications to the Privacy Rule to encourage covered entities to use and disclose PHI more broadly in scenarios that involve SUD, SMI, and emergency situations, provided that certain conditions are met. In particular, the Department proposes to amend five provisions of the Privacy Rule to replace "exercise of professional judgment" with "good faith belief" as the standard pursuant to which covered entities would be permitted to make certain uses and disclosures in the best interests of individuals. The professional

judgment standard presupposes that a decision is made by a health care professional, such as a licensed practitioner, whereas good faith may be exercised by other workforce members who are trained on the covered entity's HIPAA policies and procedures and who are acting within the scope of their authority. The Department also proposes a presumption that a covered entity has complied with the good faith requirement, absent evidence that the covered entity acted in bad faith. Together, these proposed modifications would improve the ability and willingness of covered entities to make certain uses and disclosures of PHI as described below.

The Department acknowledges prior comments expressing concern that a good faith standard offers individuals less privacy protection. However, covered entities still must take into account the facts and circumstances surrounding the disclosures, such as an individual's prior expressed privacy preferences and knowledge of any abusive relationship between the person to whom the covered entity would disclose PHI and the individual. Similarly, the Department would treat disclosures for any improper purpose as "bad faith" disclosures. Examples of bad faith could include knowledge that information will be used to harm the individual or will be used for crime, fraud (including defrauding the individual), or personal enrichment. As another example, a provider who is sued for malpractice and demands a signed statement of satisfactory care from an incapacitated individual's family member in exchange for disclosing the individual's PHI to the family member has likely acted in bad faith. Finally, the Department encourages covered entities to ascertain the privacy preferences of individuals who are at known risk of experiencing episodes of incapacity before such individuals become incapacitated, where possible.

Replacing professional judgment with good faith in sections 45 CFR 164.502(g)(3)(ii)(C), 164.510(a)(3), 164.510(b)(2)(iii), 164.510(b)(3), 164.514(h)(2)(iv)

The Department's proposal to replace "professional judgment" with a standard based on the good faith belief of the covered entity in the five provisions listed above

should improve care coordination by expanding the ability of covered entities to disclose PHI to family members and other caregivers when they believe it is in the best interests of the individual, without fear of violating HIPAA. The requirement under the current rule to exercise "professional judgment" could be interpreted as limiting the permission to persons who are licensed or who rely on professional training to determine whether a use or disclosure of PHI is in an individual's best interests. While professional training and experience naturally inform a health care provider's good faith belief about an individual's best interests, a good faith belief does not always require a covered entity or its workforce member to possess specialized education or professional experience. Rather, a good faith belief may be based on, for example, knowledge of the facts of the situation (including any prior expressed privacy preferences of the individual, such as those in an advance directive), or the representations of a person or persons who reasonably can be expected to have knowledge of relevant facts.

At the same time, as illustrated by the following scenarios, a standard of "good faith" anticipates that a covered entity or workforce member would exercise a degree of discretion appropriate for its role when deciding to use or disclose PHI, and to comply with any other conditions contained in the applicable permissions. For example, "good faith" would permit a licensed health care professional to draw on experience to make a good faith determination that it is in the best interests of a young adult patient, who has overdosed on opioids, to disclose information to a parent who is involved in the patient's treatment and who the young adult would expect, based on their relationship, to participate in or be involved with the patient's recovery from the overdose. In this circumstance, the professional's good faith belief should be informed by professional judgment, but the professional would be assured that the Department would not second-guess the decision made for the patient's best interests by, for example, requiring the professional to prove that the decision was consistent with his or her professional training.

Likewise, front desk staff at a physician's office who have regularly seen a family member or other caregiver accompany an adult patient to appointments could disclose information about upcoming appointments when the patient is not present, based on the staff's knowledge of the person's involvement and a "good faith" belief about the patient's best interests. The extent of the disclosure of PHI would be limited to the level of involvement of the family member or caregiver of which the staff is aware, consistent with the covered health care provider's policies and procedures for disclosures of PHI by workforce members. In contrast, front desk staff would not be permitted to decide whether to provide access to records under the individual right of access at 45 CFR 164.524 to a parent who is not their minor child's personal representative, because the applicable permission at 45 CFR 164.502(g)(3)(2)(C) requires that the decision be made by a licensed health care professional.

The Department understands that these proposals may raise concerns about unintended consequences where a covered health care provider is asked to disclose sensitive information to family members or other caregivers about individuals at risk of, or experiencing, abuse by the requesting family members or caregivers. The Department assumes that health care providers would incorporate relevant concerns about an individual's risk of abuse as a key factor in whether a disclosure of PHI is in an individual's best interest. Disclosures to suspected abusers are not in the best interests of individuals and health care providers' workforce members should feel confident that this proposal would not negate their ability to consider all relevant factors when making decisions about disclosing PHI to an individual's family and other caregivers related to their involvement in the individual's care or payment for care.

The following examples illustrate the operation of a good faith standard in each provision this proposal would modify:

- *Parent or guardian who is not the individual's personal representative.* The Department proposes to amend 45 CFR 164.502(g)(3)(ii)(C) to permit a covered entity to disclose the PHI of an unemancipated minor to a parent or guardian who is not the personal representative of the individual under HIPAA if consistent with state or other applicable law and a licensed health care professional has a good faith belief that disclosing PHI is in the best interests of the individual. For example, the proposed change would permit a covered health care provider to disclose PHI of an un-emancipated minor experiencing SUD in a state or jurisdiction where applicable law does not treat the minor's parent as a personal representative, when the provider believes that disclosing information to the parent could improve the care and treatment of the minor. This proposed good faith standard would remove an impediment to disclosures of PHI to a parent or guardian of a minor experiencing SUD or SMI where the parent or guardian is not recognized as the personal representative of the minor under state law. At the same time, this proposal would not preempt state laws that prohibit the disclosure of sensitive information because this proposal would permit, but not require, the disclosure under HIPAA. As such, a covered entity could comply with both HIPAA and a more restrictive state law by limiting disclosures in accordance with the state law.
- *Facility Directories.* The Department proposes to amend 45 CFR 164.510(a)(3)(i)(B) to permit a covered entity to include an individual's name in a facility directory and to disclose, for directory purposes, the individual's location and general condition, when the individual is unable to agree or object and the covered entity has a good faith belief that the disclosure is in the best interests of the individual. For example, this change would facilitate a hospital's disclosure of directory information about an individual who is incapacitated and unable to

identify family members or other caregivers involved in his or her care who are trying to locate the individual. The Department does not propose to change 45 CFR 164.510(a)(3)(i)(A), which requires that a disclosure under 45 CFR 164.510(a)(3) be consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider.

- *Emergency contacts*. The Department proposes to amend 45 CFR 164.510(b)(2)(iii) to permit covered entities to disclose relevant information to a person involved in the individual's care or payment for care when the covered entity reasonably infers, based on a good faith belief, that the individual does not object. For example, under this proposal an acute care facility that lacks a written designation of an emergency contact but possesses knowledge of an incapacitated patient's designated emergency contact could disclose PHI to that contact, based on a good faith belief that the patient does not object to the disclosure. In contrast, a disclosure of PHI by a covered entity with knowledge of an individual's advance directive that documents an objection to disclosure to a particular person would be inconsistent with a good faith belief that the individual does not object.
- *Emergencies and incapacity*. The Department proposes to amend 45 CFR 164.510(b)(3) to permit covered entities to disclose relevant information about the individual to family members and other caregivers who are involved with the individual's care or payment for care, or who require notification related to the individual, when the individual cannot agree to the disclosure because of absence, incapacity, or emergency circumstances, and the covered entity has a good faith belief that the disclosure is in the best interests of the individual. This change would, for example, facilitate a health care provider's disclosure of PHI to a caregiver of a patient who is incapacitated by an overdose, mental health crisis, or other health emergency. The Privacy Rule does not define incapacity, but the

Department has provided examples and explained that a formal determination is not necessary.[215]

- *Verifying requestor's identity.* The Department proposes to amend 45 CFR 164.514(h)(2)(iv) to provide that a covered entity would satisfy its obligations to verify a requestor's identity if the covered entity acts on a good faith belief in making a disclosure of relevant PHI under 45 CFR 164.510, 164.512(j), and 164.514(h)(2)(iv). These disclosures are already limited in scope to the information relevant to assisting the individual with his or her health care or payment for care (45 CFR 164.510) or to the minimum amount of information necessary for the purpose (45 CFR 164.512(j)). This proposal would, for example, improve the ability of a covered hospital to disclose PHI of an individual experiencing an emergency to a person who represents that he or she is a family member or caregiver of the individual, without requiring the family member or caregiver to present documentation of the relationship with the individual, if the hospital has a good faith basis for believing the requestor and the requestor's identity. As stated in the preamble to the 2000 Privacy Rule:

> "Requiring written proof of identity in many of these situations, such as when a family member is seeking to locate a relative in an emergency or disaster situation, would create enormous burden without a corresponding enhancement of privacy, and could cause unnecessary delays in these situations. The Department therefore believes that reliance on professional judgment provides a better framework for balancing the need for privacy with the need to locate and identify individuals…. As with many of the requirements of this final rule, health care providers are given latitude and

[215] *See* e.g., https://www.hhs.gov/hipaa/for-professionals/faq/2090/when-does-mental-illness-or-another-mental-condition-constitute-incapacity-under-privacy-rule.html.

expected to make decisions regarding disclosures, based on their professional judgment and experience with common practice, in the best interest of the individual."[216]

A hospital may not have a good faith basis for believing the requestor's representations about the requestor's identity and relationship with the individual if, for example, a workforce member receives a request from an unfamiliar and unverified email address or the requestor is unknown and not named as a contact in an individual's record. Additionally, this proposal would not remove a covered entity's obligation(s) under other applicable laws, such as laws requiring providers to obtain documentation of a relationship before disclosing information, including laws governing requests for access to medical records by a person who claims to be an individual's personal representative.

The Department also proposes to amend the Privacy Rule at 45 CFR 164.502 by adding a new paragraph (k), which would apply a presumption of compliance with the "good faith" requirement when covered entities make a disclosure based upon a belief that the disclosure is in the best interests of the individual with regard to those five provisions.

Changing "serious and imminent" to "serious and reasonably foreseeable"

As noted above, 45 CFR 164.512(j)(1)(i)(A) permits covered entities to use or disclose PHI, consistent with applicable law and standards of ethical conduct, if the covered entity has a good faith belief that the use or disclosure is necessary to prevent or lessen a "serious and imminent threat" to the health or safety of a person (including the individual) or the public.[217] The recipient of the PHI must be reasonably able to prevent

---

[216] 65 FR 82462, 82719 (December 28, 2000).

[217] 45 CFR 164.512(j)(1)(i)(A). 45 CFR 164.512(j), unlike the provisions above that currently permit uses and disclosures based on professional judgment, already permits a covered entity to disclose PHI based on a good faith belief.

harm or lessen the threat, or the use or disclosure must be necessary for law enforcement to identify or apprehend an individual.[218]

To clarify that the Privacy Rule permits covered entities to address threats of harm, the Department proposes to amend the Privacy Rule at 45 CFR 164.512(j)(1)(i)(A) to replace the "serious and imminent threat" standard with a "serious and reasonably foreseeable threat" standard. The Department seeks to prevent situations in which covered entities decline to make uses and disclosures they believe are needed to prevent harm or lessen threats of harm due to concerns that their inability to determine precisely how imminent the threat of a harm is may make them subject to HIPAA penalties for an impermissible use or disclosure. The proposed modification would permit covered entities to use or disclose PHI without having to determine whether the threatened harm is imminent (which may not be possible in some cases); instead, they may determine whether it is reasonably foreseeable that the threatened harm might occur. The Department further proposes to add a new paragraph (5) to define "reasonably foreseeable" using a reasonable person standard.[219] This standard involves consideration of whether a similarly situated covered entity could believe that a serious harm is reasonably likely to occur, and does not require a determination that a majority of covered entities could have such a belief. However, the "reasonably foreseeable" standard would not permit the application

---

[218] *See* 45 CFR 164.512(j)(1)(ii)(A-)(B). This condition additionally requires the individual who is the subject of the PHI to have admitted participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim of the crime, or the individual who is the subject of the PHI has escaped from a correctional institute or lawful custody.

[219] *See, e.g.,* Rest. 2d Torts, section 283. In describing the standard of the "reasonable man" in the context of negligence in tort law, the authors note benefits of the standard that also apply to the proposal in this NPRM: "The chief advantage of this standard of the reasonable man is that it enables the triers of fact who are to decide whether the actor's conduct is such as to subject him to liability for negligence, to look to a community standard rather than an individual one, and at the same time to express their judgment of what that standard is in terms of the conduct of a human being. The standard provides sufficient flexibility, and leeway, to permit due allowance to be made for such differences between individuals as the law permits to be taken into account, and for all of the particular circumstances of the case which may reasonably affect the conduct required, and at the same time affords a formula by which, so far as possible, a uniform standard may be maintained."

of assumptions unwarranted by the individual's diagnosis and specific circumstances. For example, the assumption that a person with a diagnosis of depression or anxiety is a threat to themselves or others merely by virtue of that diagnosis is unfounded. Likewise, assuming that an individual on the autism spectrum who displays certain behaviors frequently associated with mental illness has co-occurring mental illness without any such diagnosis is unfounded.

The Department recognizes that some covered health care providers, such as licensed mental and behavioral health professionals, have specialized training, expertise, or experience in assessing an individual's risk to health or safety (*e.g.*, through a violence or suicide risk assessment). Therefore, the reasonably foreseeable standard would include an express presumption that such a covered health care provider has met the reasonably foreseeable standard when it makes a disclosure related to facts and circumstances about which the covered health care provider (or member of the provider's workforce) has specialized training, expertise, or experience.

Threats to public health or safety would include, for example, mass shootings, the use of explosive devices to attack a crowd, or other acts of terrorism. These examples are intended to highlight for covered health care providers their ability to use or disclose PHI to lessen the threat of, or prevent harm due to, potential mass violence and are not intended to limit the scope or type of serious and reasonably foreseeable threats covered by this provision. That is, a covered entity (or a member of a covered entity's workforce) need not have such specialized training, expertise, or experience in order to meet the reasonably foreseeable standard.

The Department does not propose to change the existing "presumption of good faith belief" at 45 CFR 164.512(j)(4), which explains the circumstances in which a covered entity is presumed to have acted in good faith with regard to a belief that a use or

disclosure is necessary to prevent harm or lessen a threat.[220] Therefore, with the proposed modification, a covered entity that reports a threat to health or safety could potentially benefit from two presumptions under the Privacy Rule: (1) a presumption that the serious harm the covered entity identified was reasonably foreseeable, and (2) a presumption that the covered entity believed the use or disclosure was necessary to prevent harm or lessen the threat.

The Department expects that the proposed modification would improve the timeliness of disclosures that would have occurred, but for the covered entity's uncertainty regarding whether a threatened harm is "imminent." As such, this proposed change would improve covered entities' ability to disclose PHI to persons who are reasonably able to lessen the threat and to prevent harm to the individual, other persons, or the public – with sufficient time for such persons to act.

Thus, for example, adopting a "serious and reasonably foreseeable threat" standard could further enable a health care provider to timely notify a family member that an individual is at risk of suicide, even if the provider cannot predict that a suicide attempt is likely to occur "imminently." For an individual who poses a threat to public safety, a "serious and reasonably foreseeable threat" standard may afford a health care provider sufficient time to notify a person, such as a law enforcement official, who is in a position to avert a serious harm that may occur and ensure the safety of the individual and others.

By referencing mental and behavioral health professionals in the proposed definition of reasonably foreseeable, the Department does not mean to imply that individuals with mental or behavioral health conditions are more likely than other individuals to commit acts of violence. As the Department has stated previously,[221] mental

---

[220] *See* 45 CFR 164.512(j)(4). The provision states the presumption of good faith belief applies "if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority."

[221] *See* HIPAA Privacy Rule and the National Instant Criminal Background Check System Proposed Rule, 79 FR 784 (January 7, 2014), and Final Rule, 81 FR 382 (January 6, 2016).

illness is not proven to be an effective predictor of gun violence, and individuals who are experiencing mental illness are more likely to be the victims of violent crime than perpetrators.[222] The Department does not intend with this proposal to perpetuate false and harmful stereotypes about individuals with SMI or SUD, but rather to ensure that HIPAA is not a barrier in instances when entities believe a disclosure of PHI is necessary to prevent harm to the individual or to others.[223] Further, the Department believes that licensed mental and behavioral health professionals are among the health care providers that are most likely to have specialized training, expertise, or experience for which it is reasonable to establish a higher level of deference to their belief that a threat exists and that serious harm is reasonably foreseeable. The Department requests comment on this proposal.

The Department also proposes non-substantive revisions to 45 CFR 164.512(j) to refer to preventing a harm or lessening a threat, rather than preventing or lessening a threat. These proposed revisions are intended to clarify the standard, not change it; however, the Department requests comment on whether any unintended adverse consequences may result from the revisions.

Finally, the Privacy Rule does not preempt other law that is more protective of the individual's privacy.[224] As such, this proposal would not relieve covered entities of stricter restrictions on disclosure under state law or other Federal laws. However, the proposal would help ensure that HIPAA is not a barrier to disclosures needed to prevent harm.

3. Request for Comments

The Department requests comments on the above proposal, and the following considerations in particular:

---

[222] *See* 79 FR 784, 788 (January 7, 2014) and 81 FR 382, 386 (January 6, 2016).
[223] *Ibid., Id.* at 387.
[224] *See* 45 CFR 160.203.

a. Would the proposed change in standard from "professional judgment" to "good faith belief" discourage individuals from seeking care?

b. Should the Department apply the good faith standard to any or all of the other nine provisions in the Privacy Rule that call for the exercise of professional judgment? Are there circumstances in which it would be inappropriate to apply a presumption of compliance across the other nine provisions?

c. Should 45 CFR 164.510(b)(3) be revised to permit a covered entity to disclose the PHI of an individual who has decision making capacity to the individual's family member, friend, or other person involved in care, in a manner inconsistent with the individual's known privacy preferences (including oral and written expressions), based on the covered entity's good faith belief that the use or disclosure is in the individual's best interests, in any situations outside of an emergency circumstance? Put another way, are there examples in which the totality of the facts and circumstances should or would outweigh an individual's preferences, but do not rise to the level of posing a serious and reasonably foreseeable threat under 45 CFR 164.512(j)? Are there examples related to individuals who have regained capacity after having been formerly incapacitated, such as where an individual recovering from an opioid overdose leaves the hospital against medical advice or leaves a residential treatment program?

d. When should overriding an individual's prior expressed preferences constitute bad faith on the part of the covered entity, which would rebut the presumption of compliance? Are there instances in which overriding an individual's prior expressed preferences would not constitute bad faith on the part of the covered entity?

e. Would the proposed "serious and reasonably foreseeable threat" standard discourage individuals from seeking care?

f. Would the proposed standard improve a covered entity's ability to prevent potential harm, such that the benefits of the change would outweigh potential risks? Please provide examples.

g. How often do mental and behavioral health professionals perceive that HIPAA constrains their ability to report such threats? Please provide specific examples, when available, including relevant state law.

h. Are there potential unintended consequences related to granting extra deference to a covered health care provider based on specialized risk assessment training, expertise, or experience when determining that a serious threat exists or that serious harm is reasonably foreseeable? Are there unintended consequences related to specifying mental and behavioral health professionals as examples of such providers?

i. As an alternative to the existing proposal, should the Department establish a specific permission for mental and behavioral health professionals to disclose PHI when in the view of the professional, the disclosure could prevent serious and reasonably foreseeable harm or lessen a serious and reasonably foreseeable threat to the health or safety of a person or the public? What would be potential unintended consequences of such an alternative?

G. Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgment of Receipt, Establishing an Individual Right to Discuss the NPP with a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element (45 CFR 164.520)

1. Current Provision and Issues to Address

The Privacy Rule, at 45 CFR 164.520, requires a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain a written acknowledgment of receipt of the provider's NPP. If the provider is unable to obtain the written acknowledgment, the provider must document its good faith efforts and

the reason(s) for not obtaining an individual's acknowledgment, and maintain such documentation for six years.[225]

The Department has heard anecdotally and in public comments on the 2018 RFI that the acknowledgment requirements impose paperwork burdens that are perceived as unnecessary and that create confusion for individuals (who may erroneously believe they are signing an authorization or waiver of some kind), as well as front office staff (who may erroneously believe that individuals must sign the acknowledgment to obtain care).

In the 2018 RFI, the Department asked whether it should eliminate the signature and recordkeeping requirements in 45 CFR 164.520 to reduce administrative burden on covered health care providers and free up time and resources for providers to spend on treatment, including care coordination. In addition, the 2018 RFI asked providers to suggest alternative ways to document that they provided an NPP to an individual if the written acknowledgment were no longer required. The Department also asked whether and how to modify other NPP requirements to alleviate covered entity burdens without compromising transparency about providers' privacy practices or an individual's awareness of his or her rights. In particular, the Department requested feedback on how to improve the NPP content and dissemination requirements.

Most commenters stated that the acknowledgment requirement was unduly burdensome, but did not provide cost estimates. Many covered entities and associations that commented reported experiencing a large administrative burden to document the good faith effort to obtain the acknowledgment in cases where the patient is unconscious or otherwise incapacitated or cannot sign the acknowledgment due to communication barriers.

Covered entities and large associations agreed with the Department's concern in the 2018 RFI that some individuals may mistakenly believe that their signature or written

---

[225] *See* 45 CFR 164.520(e); 45 CFR 164.530(j)(2).

acknowledgment of the NPP is required to receive treatment. Commenters of all types reported their observations of individuals not reading the NPP when presented with it. Commenters also noted that physician offices frequently provide the NPP form to patients as part of a large bundle of paperwork at the time of the visit. Some commenters perceived the bundling of the NPP and acknowledgment with other paperwork as diminishing the likelihood that individuals pay attention to NPP content.

Associations and health systems/hospitals supported eliminating the requirement of a written acknowledgment of receipt of the NPP and believed the expected benefits would outweigh any adverse consequences. Professional associations, hospitals, and physicians commented that the signed NPP acknowledgment or the documentation of good faith efforts to obtain the written acknowledgment was of little or no use, and was an unnecessary burden.

In contrast, a number of commenters opposed removing the requirement relating to the written acknowledgment of receipt of the NPP, asserting that the acknowledgment helps to ensure that individuals are aware of their HIPAA rights. These commenters expressed concern that eliminating the written acknowledgment requirement would make it difficult or even impossible to track whether an individual was actually given the NPP and made aware of his or her rights under HIPAA.

Some commenters suggested alternative policy solutions or other actions that the Department could take to improve consumer awareness of the NPP, such as requiring providers to post the NPP electronically and increasing consumer education about the contents of the NPP.

Regarding NPP content, ONC, in collaboration with OCR, developed several model NPPs, which are publicly available on the OCR website.[226] These models use plain

---

[226] *See* "Model Notices of Privacy Practices," HHS Office for Civil Rights (2013), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-

language and approachable designs that were tested with consumer focus groups. The 2018 RFI sought comment on whether covered entities use the model NPPs, whether the model NPPs should contain more specific information, and whether an entity that uses a model NPP should be deemed compliant with the NPP content requirements.

Some commenters stated that they use the model NPP as a reference when creating their own forms, or modify a model to conform to state law and other organizational requirements. Some professional associations supported creating a safe harbor for entities using a model NPP, but several commenters pointed out potential challenges that such a safe harbor could create. For example, some commenters stated that a safe harbor would lead to greater confusion, with some entities having to incorporate provisions from state or local law into model NPP language. Others stated that utilizing the model NPP form would lead to longer and harder-to-understand notices. Most commenters urged that, rather than creating a safe harbor, the Department instead focus on developing consumer-focused educational materials.

Additional issues to address in connection with the NPP would arise from the NPRM's proposal to limit the individual right to direct PHI to a third party only to an electronic copy of ePHI in an EHR. Covered entities may receive requests from individuals to direct to third parties copies of PHI that are not ePHI in an EHR and therefore are outside the scope of the access right to direct a copy of PHI to a third party. The current NPP content does not address these limitations. For example, an individual submits a request to her health plan to direct ePHI in a designated record set to a third party, but that ePHI is not in an EHR. As another example, an individual requests that a paper copy, rather than an electronic copy, of PHI in an EHR be sent to a third party. Neither of these requests would be included in the individuals' right of access to direct an

---

practices/index.html and https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/npp_fullpage_hc_provider.pdf.

electronic copy of their PHI in an EHR to a third party. In addition, the Department is aware that many requests to send PHI to a third party may be for a "complete medical record" that exists in multiple forms and formats (electronic and in paper),) which are hybrid in nature. The current NPP content requirements do not help the individual understand how to obtain such records.

2. Proposal

To alleviate paperwork burdens and reduce confusion for individuals and covered health care providers, the Department proposes to eliminate the requirements for a covered health care provider with a direct treatment relationship to an individual to obtain a written acknowledgment of receipt of the NPP and, if unable to obtain the written acknowledgment, to document their good faith efforts and the reason for not obtaining the acknowledgment.[227] The proposal also would remove the current requirement to retain copies of such documentation for six years.[228]

To ensure that individuals are able to understand and make decisions based on the information in the NPP, the Department proposes at 45 CFR 164.520(b)(1)(iv)(G) to replace the written acknowledgment requirements with an individual right to discuss the NPP with a person designated by the covered entity. In addition, the Department proposes at 45 CFR 164.520(b)(1)(i) to modify the content requirements of the NPP to help increase patients' understanding of an entity's privacy practices and their rights with respect to their PHI. First, the Department proposes to modify the required header of the NPP to specify to individuals that the notice provides information about (1) how to access their health information; (2) how to file a HIPAA complaint; and (3) individuals' right to receive a copy of the notice and to discuss its contents with a designated person.

---

[227] *See* 45 CFR 164.520(c)(2)(ii).
[228] *See* 45 CFR 164.520(e).

Second, the required header would specify whether the designated contact person is available onsite and must include a phone number and email address the individual can use to reach the designated person. This header content requirement would apply to all covered entities, and not just covered health care providers with direct treatment relationships with individuals, ensuring consistency in how NPP content is presented to individuals. Providing this information at the beginning of the NPP would improve patients' awareness of their Privacy Rule rights, what they can do if they suspect a violation of the Privacy Rule, and how to contact a designated person to ask questions.

Further, consistent with the proposed header language, and to ensure that individuals are fully informed of their access rights, the Department proposes at 45 CFR 164.520(b)(1)(iv)(C) to modify the required element of an NPP that addresses the access right, to describe how an individual can exercise the right of access to obtain a copy of their records at limited cost or, in some cases, free of charge, and the right to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party. Finally, the Department proposes to add an optional element to the NPP to include information to address instances in which individuals seek to direct their PHI to a third party, when their PHI is not in an electronic health record or is not in an electronic format. This optional element would help make individuals aware that they retain the right to obtain the PHI directly and give it to a third party or they can request to send a copy of PHI directly to a third party using a valid authorization. The Department believes these proposals to remove the acknowledgment of the NPP requirements would eliminate a significant documentation and storage burden for health care providers. The Department also believes the proposals would help individuals better understand how to exercise their rights, including what they can do if they suspect a violation of the Privacy Rule, and who to contact with specific questions.

Based on public comments on the 2018 RFI, the Department does not propose to create a safe harbor to deem those entities that use the model NPP compliant with the NPP content requirements. Instead, the Department requests comment on ways the model NPP could be changed to improve consumer understanding. For example, the Privacy Rule requires that the NPP contain a description, including at least one example, of the types of uses and disclosures the covered entity is permitted to make for health care operations (as well as for treatment and payment), and the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required.[229] The model NPP explains that the health care operations permission allows uses and disclosures of PHI to "run [the] organization," which is further described as disclosing an individual's health information to run the practice, improve care, and contact the individual. The model NPP also includes an example of health care operations as "us[ing] health information . . . to manage your treatment and services."[230]

Based on the Department's experience, many individuals are not aware of the scope of activities that constitute health care operations, and thus the description and example currently in the model NPP may not provide sufficient detail to inform the individual of how their health information may be used and disclosed for health care operations purposes. To that end, the Department requests recommendations for how best to impart to individuals how health information can be used and disclosed under the health care operations permission in the model NPP.

Finally, consistent with public feedback, the Department will continue to consider how to best educate and conduct outreach to inform individuals about their Privacy Rule rights and entities' privacy practices.

---

[229] *See* 45 CFR 164.520(b)(1)(ii)(A) and (D).

[230] *See* "Full Page Model Notice of Privacy Practices", HHS Office for Civil Rights (2013), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/npp_fullpage_hc_provider.pdf.

3. Request for Comments

The Department requests comments on the above proposal, and the following considerations in particular:

a. Would the proposed changes to the NPP requirements have any unintended adverse consequences for individuals or regulated entities?

b. Would the revised NPP content requirements improve individuals' understanding of, and ability to exercise, their rights under the Privacy Rule?

c. Are there ways that OCR can improve the model NPPs to be more informative and easier to understand?

d. Should the model NPP's description of health care operations be modified? If so, please provide suggested language for modifying the description in the model NPP to reflect how your organization uses PHI for health care operations purposes.

e. Are there specific examples that should be included in a model NPP to explain to individuals how PHI can be used or disclosed for health care operations?

f. Specific examples of amounts spent and any other costs incurred by a covered entity to comply with the requirements relating to the acknowledgement of receipt of the NPP, when the covered entity fulfills the requirements using paper-based or electronic forms, signatures, or document filing systems.

H. Permitting Disclosures for Telecommunications Relay Services for People who are Deaf, Hard of Hearing, or Deaf-Blind, or who have a Speech Disability (45 CFR 164.512)

1. Current Provisions and Issues to Address

Telecommunications Relay Service (TRS) facilitates telephone calls between individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability,

and others.[231] TRS is a federally mandated service that federally regulated common carriers (*e.g.*, operators of all landline and mobile telephone services) are required to provide individuals, in the general public, who are deaf, hard of hearing, or deaf-blind, or who have a speech disability.[232] The Federal Communications Commission (FCC), pursuant to the Americans with Disabilities Act (ADA)[233] certifies TRS programs, which are available in all 50 states, the District of Columbia, Puerto Rico, and U.S. territories. States and other government entities typically compensate telephone companies to provide TRS services.[234]

TRS facilitates such telephone communication by using a communications assistant[235] who transliterates conversations (or, in some cases, interprets using ASL). The communications assistant relays information, which may include PHI, between a person who uses text or video and another person, who may be communicating by voice or who may also use TRS.[236] Several forms of TRS are available.[237] All TRS providers must comply with standards for operators established by the FCC pursuant to Title IV of the ADA, including protecting the confidentiality of all relayed communications.[238]

OCR has a longstanding FAQ on the use of TRS by a covered entity to communicate with an individual who is deaf, hard of hearing, or deaf-blind, or who has a

---

[231] *See "*Consumer Guide, Telecommunications Relay Service," FCC (2017), available at https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.
[232] *See* 47 U.S.C. 225(b).
[233] Pub. L. 101-336, 104 Stat. 327 (July 26, 1990), and its amendments.
[234] *See* "Consumer Guide, Telecommunications Relay Service," https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.
[235] A communications assistant is "[a] person who transliterates or interprets conversation between two or more end users of TRS." 47 CFR 64.601(a)(12).
[236] *See generally*, FCC's 2017 "Consumer Guide, Telecommunications Relay Service," available at https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.
[237] TRS types include Text-to-Voice, Voice Carry Over, Hearing Carry Over, Speech-to-Speech Relay, Shared Non-English Language Relay, Captioned Telephone Service, IP Captioned Telephone Service, Internet Protocol Relay Service, and Video Relay Service. *Id.* at 2.
[238] Except in very limited circumstances specified in FCC regulations, TRS communications assistants are not permitted to keep notes of the contents of a call after a call, unless the caller requests that the communications assistant retain such information in order to facilitate the completion of subsequent calls. In no case may the communications assistant retain such information after the completion of the subsequent call(s). *See* 47 CFR 64.604(a)(2).

speech disability. The FAQ states that a covered entity is permitted to disclose an individual's PHI to a TRS communications assistant when communicating with the individual, without the need for a business associate agreement with the TRS provider.[239] The FAQ explains that the Privacy Rule permits disclosures to TRS communications assistants under 45 CFR 164.510(b) because individuals have an opportunity to agree or object to disclosures of PHI to a TRS communications assistant at the beginning of a call, and the individuals are identifying the communications assistant as involved in their care if they do not object. The FAQ also explains that the TRS provider is not acting for or on behalf of the covered entity when it provides such relay services, and therefore is not a business associate.

Since the FAQ was created, the Department has become aware that advances in technology now allow people who are deaf, hard of hearing, or deaf-blind, or who have a speech disability to communicate with the help of a TRS communications assistant in a seamless manner, with immediate connection and instantaneous transliteration of text or interpretation of ASL to voice and vice versa, such that the other party to the call may not know that a person is using a TRS communications assistant. In addition, TRS is used to not only connect patients and providers, but also to assist communications between workforce members of covered entities and business associates. For these reasons, the original assumption that individuals would always have the opportunity to agree or object to a use or disclosure of PHI to a communications assistant no longer holds when it is a workforce member of the covered entity or business associate, rather than an individual (*e.g.*, patient or beneficiary), who needs the TRS services to assist in making communications. Further, stakeholders have requested that the Department specifically address the use of TRS by members of the covered entity or business associate workforce

---

[239] *See* HHS Office for Civil Rights Frequently Asked Questions, available at https://www.hhs.gov/hipaa/for-professionals/faq/500/is-a-relay-service-a-business-associate-of-a-doctor/index.html.

to share PHI with other workforce members or outside parties as needed to perform their duties. These stakeholders have shared anecdotal accounts in which a covered entity or business associate refuses to allow a workforce member to use this essential service because of concerns about violating the Privacy Rule if they do not have a business associate agreement with the TRS provider.

2. Proposal

The Department proposes to expressly permit covered entities (and their business associates, acting on the covered entities' behalf) to disclose PHI to TRS communications assistants to conduct covered functions by adding a new paragraph (m) to 45 CFR 164.512.[240] This proposed permission would cover all disclosures to TRS communications assistants relating to any covered functions performed by, for, or on behalf of covered entities and clarify for covered entities that a business associate agreement is not needed with a TRS communications assistant.

The Department also proposes to add a new subsection (v) to paragraph (4) of the definition of business associate at 45 CFR 160.103 to expressly exclude TRS providers from the definition of business associate. The proposed exclusion would apply regardless of whether the workforce member is an employee, contractor, or business associate of the covered entity. This proposal would ensure that covered entities and business associates do not bear the burdens of analyzing whether they need business associate agreements with TRS providers and, potentially, establishing such agreements.

Together, these modifications would help ensure that workforce members and individuals who are deaf, hard of hearing, or deaf-blind, or who have a speech disability are able to communicate easily using TRS for care coordination and other purposes.

---

[240] The terms "Telecommunications Relay Service" and "Telecommunications Relay Service Communications Assistant" have the same meaning used in 47 CFR Part 64.

3. Request for Comments

The Department requests comments on this proposal, including the following questions:

a. Would the proposed change achieve the anticipated effects?

b. Are there any potential unintended, adverse consequences of the proposal?

c. Please share data related to the number of covered entity and business associate workforce members who are deaf, hard of hearing, or deaf-blind, or who have a speech disability and currently utilize TRS to perform their duties.

d. Please provide data on the amount of time and other resources covered entities and business associates have spent on determining whether they need a business associate agreement with a TRS provider, or actually entering into business associate agreements with TRS providers.

I. Expanding the Permission to Use and Disclose the PHI of Armed Forces Personnel to Cover all Uniformed Services Personnel (45 CFR 164.512(k))

1. Current Provision and Issues to Address

The original Privacy Rule[241] established an express permission for covered entities to use and disclose the PHI of Armed Services personnel, under certain conditions, to avoid the burden and obstacles of obtaining individuals' authorizations when the balance of privacy interests and social values weighed toward permitting the use or disclosure of PHI without authorization for specialized purposes. Currently, a covered entity may use and disclose the PHI of Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, provided the conditions at 45 CFR 164.512(k) are met. The appropriate military

[241] *See* 65 FR 82462, 82704, 82817 (December 28, 2000).

command authorities and the purposes for which the PHI may be used or disclosed must be identified through ***Federal Register*** notices.[242]

Like the Secretaries of the Armed Services, the Secretaries of HHS and the Department of Commerce are responsible for ensuring the medical readiness of the Uniformed Services personnel in the U.S. Public Health Service (USPHS) Commissioned Corps and the National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps, respectively. Pursuant to 42 U.S.C. 204a(a)(1), while on active duty, the ongoing medical standards require USPHS personnel to be medically fit to deploy in response to urgent and emergent public health crises, as well as for any necessary military mission, and for duty in various environments. These medical standards include physical, dental, and mental health requirements. The NOAA Commissioned Corps has a similar standard, requiring personnel to meet U.S. Coast Guard medical standards to maintain individual medical readiness for deployment on aircraft and shipboard missions. Further, when personnel in the Uniformed Services are no longer fit for duty, they are entitled to retirement pay and compensation, and once separated they are entitled to receive veterans' benefits. In order to confirm the medical fitness of personnel, the USPHS and NOAA Commissioned Corps must have access to personnel's medical records.

In addition, the USPHS Commissioned Corps and NOAA Commissioned Corps routinely align their policies and practices with those of the Armed Forces. Members of the USPHS and NOAA Commissioned Corps may be assigned to the Armed Services and must meet medical readiness standards consistent with the various military missions of the Armed Services. In times of war, the President may declare the USPHS and the NOAA Commissioned Corps to be a military service.

However, the members of the USPHS and NOAA Commissioned Corps are not members of the Armed Services, and thus covered entities currently are not permitted to

---

[242] *See* 45 CFR 164.512(k)(1)(i).

use and disclose the PHI of such Commissioned Corps personnel for the same purposes as for Armed Forces personnel unless the member is actively assigned to the Armed Services. The Department proposes to expand the existing permission at 45 CFR 164.512(k)(1) in recognition that ensuring the health and well-being of Uniformed Services personnel is essential, whether such personnel are serving in the continental United States or overseas or whether such service is combat-related. In all environments, operational or otherwise, the Uniformed Services must be assured that personnel are medically qualified to perform their responsibilities and medically ready for deployment at all times.

Although the issue was not raised in the 2018 RFI, the Department received a joint comment in response to the 2018 RFI from the Directors of the Commissioned Corps of NOAA and USPHS suggesting that the current permission for covered entities to use and disclose the PHI of Armed Forces personnel be broadened to also include non-armed Uniformed Services personnel. The Directors of the NOAA and USPHS Commissioned Corps stated that the existing rule limits the ability of the NOAA and USPHS Commissioned Corps to facilitate health care coordination and case management for Commissioned Corps personnel, which is important for ensuring that personnel meet medical readiness standards, and thus for fulfilling the Commissioned Corps' respective missions. The commenters also stated that the permission is important because personnel and the broader population are put at risk when personnel do not disclose medical conditions to Commissioned Corps leaders and are deployed on a Commissioned Corps mission.

2. Proposal

The Department agrees that expanding the Armed Forces permission may facilitate coordinated care and enhance USPHS and NOAA Commissioned Corps' readiness.

Therefore, to improve care coordination and case management for individuals serving in the Uniformed Services, the Department proposes in 45 CFR 164.512(k)(1) to expand to all Uniformed Services personnel the current Armed Forces permission for covered entities to use and disclose PHI for mission requirements and veteran eligibility.

3. Request for Comments

The Department requests comments on this proposal, including on whether the proposed change would achieve the anticipated effects and any potential unintended consequences.

IV. Public Participation

The Department seeks comment on all issues raised by the proposed regulation, including any unintended adverse consequences. Because of the large number of public comments normally received on ***Federal Register*** documents, the Department is not able to acknowledge or respond to them individually. In developing the final rule, the Department will consider all comments that are received by the date and time specified in the DATES section of the Preamble.

Because mailed comments may be subject to security delays due to security procedures, please allow sufficient time for mailed comments to be timely received in the event of delivery delays. Any attachments submitted with electronic comments on www.regulations.gov should be in Microsoft Word or Portable Document Format (PDF). Please note that comments submitted by fax or email and those submitted after the comment period will not be accepted.

V. Regulatory Impact Analysis

The Department has examined the impact of the proposed rule as required by Executive Order 12866 on Regulatory Planning and Review, 58 FR 51735 (October 4, 1993); Executive Order 13563 on Improving Regulation and Regulatory Review, 76 FR 3821 (January 21, 2011); Executive Order 13132 on Federalism, 64 FR 43255 (August 4, 1999); Executive Order 13175 on Consultation and Coordination with Indian Tribal Governments, 65 FR 67249 (November 6, 2000); Executive Order 13771 on Reducing Regulation and Controlling Costs, 82 FR 9339 (January 30, 2017); the Congressional Review Act, Pub. L. 104-121, sec. 251, 110 Stat. 847 (March 29, 1996); the Unfunded Mandates Reform Act of 1995, Pub. L. 104-4, 109 Stat.48 (March 22, 1995); the Regulatory Flexibility Act, Pub. L. 96-354, 94 Stat. 1164 (September 19, 1980); Executive Order 13272 on Proper Consideration of Small Entities in Agency Rulemaking, 67 FR 53461 (August 16, 2002); the Assessment of Federal Regulation and Policies on Families, Pub. L. 105-277, sec. 6545, 112 Stat. 2681 (October 21, 1998); and the Paperwork Reduction Act of 1995, Pub. L. 104-13, 109 Stat. 163 (May 22, 1995).

A. Executive Orders 12866 and 13563 and Related Executive Orders on Regulatory Review

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). Executive Order 13563 is supplemental to, and reaffirms the principles, structures, and definitions governing regulatory review as established in, Executive Order 12866.

This proposed rule is deregulatory. The Department has estimated that the effects of the proposed requirements for regulated entities would result in new costs of $996 million within 12 months of implementing the final rule. The Department estimates these first year costs would be partially offset by $880 million of first year cost savings,

followed by net savings of $825 million annually in years two through five, resulting in overall net cost savings of $3.2 billion over five years.

The Department estimates that the private sector would bear approximately 60 percent of the costs, with state and federal health plans bearing the remaining 40 percent of the costs. All of the costs savings experienced from the first year through subsequent years would benefit covered entities. As a result of the economic impact, the Office of Management and Budget (OMB) has determined that this proposed rule is an economically significant regulatory action within the meaning of section 3(f)(1) of EO 12866. Accordingly, OMB has reviewed this proposed rule.

The Department presents a detailed analysis below.

1. Summary of the Proposed Rule

This NPRM proposes to modify the Privacy Rule to improve individuals' access to their PHI, increase permissible disclosures of PHI, and improve care coordination and case management by:

- Adding definitions for electronic health records (EHRs) and personal health applications.
- Modifying the provisions on the individuals' right of access to protected health information (PHI) by: strengthening the individual's right to inspect their PHI, which includes allowing individuals to take notes or use other personal resources to view and capture copies of their PHI in a designated record set; shortening covered entities' response time to 15 calendar days (from the current 30 days); clarifying what constitutes a readily producible form and format when providing requested copies of PHI, which may be ePHI transmitted via a personal health application, while requiring covered entities to inform individuals about their right to obtain or direct copies of PHI to a third party when a summary or explanation is offered; requiring covered health

care providers and health plans to respond to certain record requests from other covered health care providers and health plans made at the direction of an individual; clarifying when ePHI must be provided to the individual free of charge; amending the fee structure for certain requests to direct ePHI to a third party; and requiring covered entities to post fee schedules on their websites (if they have a website) for common types of requests for copies of PHI, and, upon request, provide individualized estimates of fees for copies and an itemized list of actual costs for requests for copies.

- Reducing the identity verification burden on individuals exercising their access right.
- Amending the definition of health care operations to clarify the scope of care coordination and case management activities encompassed in the term.
- Creating an exception to the minimum necessary standard for disclosures to, or requests from, a health plan or covered health care provider for individual-level care coordination and case management activities.
- Clarifying the scope of covered entities' ability to disclose PHI to social services agencies, community-based organizations, home and community based service (HCBS) providers, and other similar third parties that provide health-related services, to facilitate individual-level care coordination and case management activities that constitute treatment- or health care operations.
- Replacing the privacy standard that permits covered entities to make decisions about certain uses and disclosures based on their "professional judgment" with a standard permitting covered entities to use or disclose PHI in some circumstances based on a good faith belief that the use or disclosure is in the best interests of the individual. The proposed standard would presume a

covered entity's compliance with the good faith requirement; the presumption could be overcome with evidence that a covered entity acted in bad faith.

- Expanding the ability of covered entities to use or disclose PHI to avert a serious threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current standard which requires a "serious and imminent" threat to health or safety.
- Eliminating the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices and modifying the content requirements of the Notice of Privacy Practices to clarify for individuals their rights with respect to their PHI and how to exercise those rights.
- Expressly permitting disclosures to Telecommunications Relay Services (TRS) communications assistants and modifying the definition of business associate to exclude TRS providers.
- Expanding the Armed Forces permission to use or disclose PHI to all Uniformed Services, which would include the U.S. Public Health Service (USPHS) Commissioned Corps and the National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps.

The proposed changes to the Privacy Rule offer some estimated costs, and numerous and substantial estimated cost savings and expected benefits which the Department is unable to quantify, but are described in depth below. These include improved care coordination and health outcomes; improved harm reduction; greater adherence to treatment for persons experiencing health emergencies, SUD, and SMI; improved understanding of individuals' rights and covered entities' privacy practices; improved access to care; quicker, more convenient access to PHI by individuals; improved access to PHI by health care providers and health plans; reduction in access fee disputes,

resulting in improved ability to collect of fees for copies of PHI; increased certainty about allowable fees; increased adoption and utilization of EHR technology; improved employment conditions and opportunities for workforce members of HIPAA covered entities and business associates who are deaf, hard of hearing, or deaf-blind, or who have a speech disability; and improved compliance with non-discrimination laws that require accessibility for individuals with disabilities.

The Department has identified three general categories of costs arising from these proposals which mostly relate to activities by HIPAA covered entities, particularly health care providers and health plans: (1) administrative activities (first-year and ongoing); (2) revising or creating policies and procedures, the NPP, and an access fee schedule; and (3) revising training programs for workforce members.

The Department estimates that the first-year costs will total $996 million. These costs are attributable to covered entities revising or developing new policies and procedures, at a cost of $696 million; revising training programs for workforce members, at a cost of $224 million; and additional administrative tasks, at a cost of $76 million. For years two through five, estimated annual costs of $55 million are attributable to ongoing administrative costs, primarily related to improvements to the right of access to PHI.

The Department estimates annual cost savings of $880 million per year, over five years, attributable to eliminating the NPP acknowledgment requirements (cost savings of $537 million) and clarifying the minimum necessary standard ($343 million).

The Department estimates net costs for covered entities totaling $116 million in the first year followed by net savings of $825 million annually in years two through five, resulting in overall cost savings of $3.2 billion over five years. Covered entities would

experience an average net savings of approximately $1,065 per entity in years two through five after expending costs of $150 per entity in the first year.[243]

Table 1. Estimated Five-Year Costs and Cost-Savings, Undiscounted, in Millions

Costs	**Amount**
Revise Training	$224
Revise Policies and Procedures	$696
Administrative Costs	$297
Capital Costs	$1
Total Costs	**$1,218**
Cost Savings	
Eliminate Notice of Privacy Practices Acknowledgment	$2,685
Clarify Minimum Necessary Standard	$1,715
Total Cost Savings	**$4,400**
Net Total (negative = savings)	**-$3,182**

The Department estimates that the proposed adjustments to costs that can be charged to individuals for copies of PHI in an EHR on electronic media would result in a transfer of those expenses from individuals to covered entities in a total estimated amount of $1.4 million. The Department also estimates that the proposed changes to the right to direct the transmission of copies of PHI to a third party and to allowable access fees would result in an annual transfer of $43 million in costs incurred by covered entities to individuals for directing copies of PHI to third parties. The net result of these proposals likely would be a transfer of an estimated $41.6 million in costs from covered entities to individuals and some third party recipients of PHI in the form of higher fees for copies of PHI.

2. Need for the Proposed Rule

[243] The Department recognizes that some of the proposed changes would affect certain covered entities more than others, resulting in significantly different costs and savings. The tables summarizing estimated costs and cost savings account for these differences (Cost-Benefit Analysis, subsections f - j and Tables 10 – 17).

The Privacy Rule balances protecting the privacy of individuals' PHI with facilitating the use and disclosure of PHI for important public interest purposes, such as facilitating efficient care coordination and case management. This proposed rule would improve on this balance with modifications to promote the transformation to value-based health care and reduce regulatory burdens by removing unhelpful or unnecessary requirements. Based on public comments on the 2018 RFI and OCR's experience administering and enforcing the Privacy Rule, the Department has identified areas where the Privacy Rule could be modified to improve the flow of PHI for such purposes in a manner that would continue to protect individuals' privacy. These include changes strengthening the individual's ability to gain access to his or her own PHI; enhancing the disclosure of PHI between covered entities; improving health care providers' ability to disclose needed PHI to patients' family members, friends, caregivers, and others in a position to prevent harm; supporting the rights of workforce members who need accommodations to communicate and share PHI; including all branches of the Uniformed Services in applicable disclosure permissions; and technical amendments for business associates to provide individuals with access to copies of PHI.

a. Individual Right of Access

Individual access to PHI is a core right established by the Privacy Rule. Delays or lack of access inhibit care coordination and may contribute to worse health outcomes for individuals. Individuals frequently face barriers to obtaining timely access to their PHI, in the form and format requested, and at a reasonable, cost-based, and transparent fee. A recent cross-sectional study of medical records request processes conducted in 83 top-ranked US hospitals found numerous indications of noncompliance with the access right.[244]

---

[244] Lye CT, Forman HP, Gao R, et al. "Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records." JAMA Network Open. October 5, 2018,

To address multiple barriers to individual access, the Department proposes to: add definitions of EHR and personal health application; expressly provide that the right to inspect PHI in person includes the right of an individual to take notes and photographs of, and use other personal resources to capture, PHI; clarify what constitutes a readily producible form and format for copies of PHI, while requiring covered entities to inform individuals about access rights when offering a summary in lieu of providing or directing copies; shorten the time limits for covered entities to respond to access requests; empower individuals to use the right of access to direct the disclosure of PHI among their health care providers and health plans; adjust and clarify the fees covered entities may impose; and require covered entities to provide individuals with notice of the fees charged for copies of PHI. Additionally, the Department proposes to limit the scope of the right to direct the transmission of copies of PHI to a third party to electronic copies of PHI in an EHR, consistent with the *Ciox v. Azar* decision.[245]

i. Defining Electronic Health Record and Personal Health Application

The Department proposes to add a definition of EHR for the purpose of clarifying the scope of the individual right to direct an electronic copy of PHI in an EHR to a third party. For purposes of harmonizing the proposed regulatory changes and the right of the individual to obtain an electronic copy, the Department interprets the EHR as health information "created, gathered, managed, and consulted by authorized health care clinicians and staff." The definition would be tied to clinicians with direct treatment relationships with individuals and consistent with the defined terms in the current rule. The proposed definition would improve understanding of whether certain aspects of a covered entity's electronic records are or are not part of an EHR to enable a covered entity

---

1(6):e183014, available at https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2705850.

[245] No. 18-cv-0040-APM (D.D.C. January 23, 2020).

to assess whether such electronic PHI is subject to the HITECH Act right of access requirements to respond to requests from an individual to direct electronic copies of PHI in an EHR to designated third parties. Although covered health care providers have substantial flexibility in determining the composition of an EHR, an EHR may vary across different health care providers. The definition is intended to provide a clear standard by which health care providers would be able to identify what PHI is subject to HITECH Act requirements for electronic PHI in an EHR. As noted earlier, the Department proposes that only covered health care providers would provide such access because only providers would maintain EHRs as defined in proposed 45 CFR 164.501, and that an EHR would also include billing records.

The Department also proposes to add a new definition for the term "Personal health application" that is similar to the HITECH Act definition of personal health record (PHR),[246] but is intended to specifically address health applications, which may or may not be PHRs.[247] Adding this definition would clarify the intended scope of proposed changes to the right of access, such as clarifying that an individual may use an internet-based method such as a personal health application to obtain access without charge.

ii. Strengthening the Right to Inspect and Obtain Copies of PHI

The individual right of access under the Privacy Rule includes a right to "inspect and obtain a copy of" PHI in a designated record set.[248] The Department proposes to strengthen the access right to inspect and obtain copies of PHI to generally enable an

---

[246] *See* the HITECH Act definition of personal health record, "[A]n electronic record of PHR identifiable health information (as defined in section 17937(f)(2) of this title) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." 42 U.S.C. 17921(11). *See also* proposed 45 CFR 164.501, definition of "Personal health application."

[247] The same software could be a personal health application under the proposed Privacy Rule definition and also be a personal health record under the HITECH Act for other purposes, to the extent it meets both definitions.

[248] *See* 45 CFR 164.524(a).

individual to take notes, videos, and photographs, and use other personal resources to capture PHI in a designated record set, as part of the right to inspect PHI in person.

iii. Timeliness

Timely access to an individual's own PHI can be a key component to patient-directed care (see discussion of harms due to lack of timeliness above in section III.A.3.a.). The Department proposes to modify the Privacy Rule to require that access be provided as soon as practicable, but no later than 15 calendar days after receipt of the request, with the possibility of one 15 calendar-day extension, provided certain conditions are met. Where another federal or state law (*i.e.*, statute or regulation) requires a covered entity to provide individuals with access to the PHI requested in less than 15 calendar days, that shorter time period would be deemed practicable under 45 CFR 164.524 (b)(2)(i) and (d)(5). The Department also proposes to add a new condition requiring a covered entity to establish a written policy to prioritize urgent or other high-priority access requests (especially those for health and safety and to support individual decisions about treatment options), to limit the need to use a 15 calendar-day extension for such requests. This would reduce by half the time within which entities must provide access to PHI, consistent with existing requirements in several large states, improvements in health IT, and consumers' needs and expectations. The proposal would also prohibit covered entities from delaying the right to inspect PHI that is readily available at the point of care in conjunction with a health care appointment.

The Department lacks sufficient data to correlate shorter required access times with health care costs. The Department examined state health expenditure data[249] and

[249] *See* "Kaiser Family Foundation, Health Care Expenditures, per Capita, by State of Residence," available at https://www.kff.org/other/state-indicator/health-spending-per-capita/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D (*citing CMS,* National Health Care Expenditure Data, available at https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsStateHealthAccountsResidence.html.

noted that of the eight states with shorter access time limits than the Privacy Rule,[250] six rank in the lowest third for health care expenditures; however, there is a lack of granularity to this data upon which to draw clear conclusions about the potential ongoing burden to covered entities. The Department has estimated that the proposed changes would increase costs on an ongoing basis and welcomes data about these estimates, as detailed in the cost-benefits analysis.

Finally, the Department also proposes to expressly provide that while a covered entity may discuss aspects of the individual's access request with the individual before fulfilling the individual's request, such discussions to clarify the scope of the request would not extend the time limit for providing access. This modification would help address the issue raised in individual complaints and comments on the 2018 RFI that covered entities may contact individuals for the first time nearly 30 days after receiving a request for access to discuss the request or obtain additional information, and then take additional time beyond the 30-day period to fulfill the request.

iv. Addressing the Form and Format of Access

The Department proposes to clarify that "readily producible" includes access through APIs and personal health applications and to add a set of parallel requirements related to the form of access that applies to both the individual right to obtain copies of PHI and the access right to direct the transmission of electronic copies of PHI in an EHR to a designated third party. As new forms of information and communications technologies emerge, the "form and format" and the "manner" of producing or transmitting a copy of electronic PHI may become indistinguishable. For example, if a covered entity or its EHR developer business associate has chosen to implement a secure, standards-based API—such as one consistent with ONC's Cures Act certification

[250] California, Colorado, Hawaii, Louisiana, Montana, Tennessee, Texas, and Wyoming (New York's shorter time limit is published as agency guidance).

criteria,[251] and the covered entity's Security Rule obligations—that is capable of providing access to ePHI in the form and format used by an individual's personal health application, that ePHI is considered to be *readily producible* in that form and format, and that is also the manner by which the ePHI is transmitted.

Additionally, when a covered entity offers a summary in lieu of providing or directing the requested copies of PHI, the Department would require the covered entity to inform the individual of the right to obtain or direct the requested copies if the individual does not agree to the offered summary. This requirement would not apply when the covered entity denies the access request for a copy on unreviewable or reviewable grounds, in which case the covered entity must implement the required procedures for such denial.

v. Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

The Department proposes to implement the *Ciox v. Azar* decision by codifying in regulation the HITECH Act right to direct the transmission to a third party of only electronic copies of PHI in an EHR in 45 CFR 164.524(d)(1). Under this proposal, if an individual directs a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party, the covered health care provider would be required to provide a copy of the requested PHI to the person designated by the individual. The Department believes this proposal is consistent with the plain meaning of section 13405(e) of the HITECH Act, which extended a right to a copy of PHI in an EHR "in an electronic format" as part of the Privacy Rule right of access. As a result, requests to direct to a third party non-electronic copies of PHI in a designated record set (whether from an EHR or other source) and electronic copies of PHI that is not in an EHR, would no longer fall within the right of access. Individuals would continue to have the right to directly obtain

[251] ONC has finalized significant updates to its certification criteria at 45 CFR Parts 170 and 171. *See* 85 FR 25642 (May 1, 2020).

the types of PHI that are outside of the scope of the access right to direct electronic copies of PHI in an EHR to a third party, and also could request that a copy of the PHI be sent to a third party by submitting a valid authorization. To address the potential impact on individual rights as a result of these changes the Department proposes an optional element for the Notice of Privacy Practices (NPP) as described in the NPP sections of the NPRM.

The Department proposes to extend the right to direct copies of PHI to a third party by adding an express right to request that covered health care providers and health plans submit an access request to covered health care providers for electronic copies of PHI in an EHR on behalf of the individual. Under this proposal, if an individual is a current or prospective new patient of a covered health care provider, or an enrolled member or dependent of a health plan, and the individual makes a clear, conspicuous, and specific request that their health care provider or health plan submit an access request for electronic copies of PHI in an EHR to another covered health care provider, the first health care provider or health plan ("Requester-Recipient") would be required to submit the request on behalf of the individual as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and any information needed to make the access request. The requirement would be limited to requests to send the electronic PHI back to the covered entity that submitted the request on behalf of the individual.

A covered health care provider that receives an individual's access request ("Discloser") for an electronic copy of PHI maintained in an EHR by or on behalf of the Discloser, from a health care provider or health plan Requester-Recipient that is clear, conspicuous, and specific (*e.g.*, clearly identifies the Requester-Recipient, the scope of the requested PHI and where to transmit it), would be required to transmit the requested electronic copy to the Requester-Recipient, consistent with obligations under the access right to direct a copy of PHI to a third party. The Department reconfirms the clarification provided in the preamble to the 2000 Privacy Rule and OCR's 2016 Access Guidance that

a covered entity may accept an electronic copy of a signed request by the individual or personal representative (*e.g.*, PDF), as well as an electronically executed request (*e.g.*, via a secure web portal or using secure, standards-based API technology) that includes an electronic signature of the individual or personal representative.[252]

These proposed changes would empower individuals' ability to direct the transmission of PHI in an EHR through a health care provider or health plan. The costs for implementing these changes generally would be one-time expenditures for updating policies and procedures to ensure compliance with the proposed requirement to submit requests for individuals to health care providers within 15 calendar days of receipt of the request from the individual as would be required under the proposed changes. The Department anticipates that some covered entities are already relying on the individual right to direct the transmission of copies to a third party[253] as a means of obtaining electronic copies of PHI in an EHR[254] and are facilitating individuals' access rights by transmitting requests within 15 calendar days in compliance with applicable state laws, so these changes would create certainty without significantly increasing burdens for these covered entities. Additionally, despite problems that are addressed by this proposal, many covered entities that receive requests from another covered entity for copies of PHI are fulfilling such requests, so no additional burden would be created for these disclosing entities when the electronic copy requested by the individual is submitted by and transmitted to their current health care provider or health plan.

---

[252] *See* 65 FR 82462, 82660 (December 28, 2000) ("We intend e-mail and electronic documents to qualify as written documents. Electronic signatures are sufficient, provided they meet standards to be adopted under HIPAA. In addition, we do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act."); *see also* OCR's 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs.

[253] See 45 CFR 164.524(c)(ii).

[254] 45 CFR 164.524(c)(3)(ii) requires the covered entity holding the PHI to disclose it to the person designated by the individual. Thus, a health care provider seeking an individual's PHI may find it expedient at times to rely on this provision and be designated as the third party recipient rather than use the treatment disclosure permission under 45 CFR 164.502 and 164.506, which do not require a covered entity to respond to a request.

vi. Adjusting Permitted Fees for Access to PHI and ePHI

Based on enforcement experience and comments received on the 2018 RFI, the Department is aware that individual access is at times expensive for individuals. At the same time, some large organizations have complained about the time and cost needed to respond to multiple, voluminous requests to provide PHI to third parties under the individual access right and reported struggling to meet the time limitations for such requests while also fulfilling requests for access received directly from individuals and provider-to-provider requests for PHI for continuity of care purposes. Additionally, commenters explained that requests to send medical records to a third party often ask for production of non-electronic copies, even when the PHI is in an EHR and could be provided electronically.

To address these multiple concerns and the *Ciox v. Azar* court ruling,[255] the Department proposes to modify the access fee provisions to create separate fee structures for individual requests for access and requests to direct electronic copies of PHI in an EHR to a third party. Each fee structure would contain two elements based on the type of access request: one element describing when access is to be provided without charge and another element describing the allowable costs for certain types of access, as follows.

For individual requests for access and copies of PHI:

(1) Under proposed 45 CFR 524(c)(4)(ii), always free of charge (*i.e.,* no fee permitted) when:

(a) An individual inspects PHI about the individual in person, including capturing images or video recordings of PHI in a designated record set with the individual's own device.

(b) An individual uses an internet-based method to view or obtain a copy of electronic PHI maintained by or on behalf of the covered entity.

[255] No. 18-cv-0040 (D.D.C. January 23, 2020).

(2) Under proposed 45 CFR 164.524(c)(4)(i), fee permitted, subject to the existing access right fee limits, when an individual requests electronic or non-electronic copies of PHI through a means other than an internet-based method.

For requests to direct an electronic copy of PHI in an EHR to a third party:

Under proposed 45 CFR 164.524(d)(6), a reasonable, cost-based fee for an access request to direct a covered health care provider to transmit an electronic copy of PHI in an EHR to a third party through other than an internet-based method, provided that the fee includes only the cost of:

> (a) Labor for copying the PHI requested by the individual in electronic form; and
>
> (b) Preparing an explanation or summary of the electronic PHI, if agreed to by the individual as provided in paragraph (d)(4).

The Department proposes the two types of no-charge access (for inspecting PHI in person or internet-based access, including directing electronic copies of EHRs to third parties) because there are no additional allowable labor costs or expenses for this type of access. The Department does not anticipate additional costs from adding this regulatory requirement because the current rule has no provision for fees for inspecting PHI and the proposal is based on the 2016 Access Guidance, which the Department understands many entities had been voluntarily following.

The proposal to limit the allowable costs for requests to direct PHI to third parties to only electronic copies of PHI in EHRs to the labor for making the electronic copies would increase covered entities' and business associates' costs for electronic media, labor for mailing and shipping, and actual postage and shipping. However, the concurrent proposal to narrow the right of individuals to direct only electronic copies of PHI in an EHR to third parties would allow covered entities and business associates to recoup

additional costs for handling many requests, while maintaining the Privacy Rule's prohibitions on the sale of PHI[256] and preserving individuals' privacy regarding the purpose of their requests. As discussed in more detail later in this regulatory impact analysis, the Department estimates that the increased costs that covered entities and business associates could include in fees for sending non-electronic copies of PHI or electronic copies of PHI not in an EHR to third parties will exceed the cost items for which they will no longer be allowed to include in fees for requests to direct electronic copies of PHI in an EHR to third parties. Under these proposed changes, a covered entity could charge for reviewing a request to send non-electronic copies of PHI and electronic copies of PHI in an EHR, searching and retrieving, and segregating or otherwise preparing the PHI that is responsive to the request at higher rates than the Privacy Rule currently allows for access requests, when requests for copies are made with a valid authorization. However, by narrowing the scope of access requests to direct PHI to third parties to only electronic copies in an EHR, the Department does not intend to allow covered entities to engage in what would otherwise be considered a sale of PHI.[257] Thus, the permitted fees under 45 CFR 164.502 and 164.508--a reasonable, cost-based fee for preparing and transmitting PHI or a fee otherwise expressly permitted by other law--would apply to many requests that previously would have been made under the right of access to direct copies to a third party. This combination of proposed changes would likely result in a transfer of some costs from covered entities to individuals and third-party recipients. This

---

[256] The Privacy Rule prohibits the sale of PHI, which is defined generally as a disclosure where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. However, a sale does not include a disclosure for a purpose permitted by and in accordance with the Privacy Rule, "where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law. *See* 45 CFR 164.502(a)(5)(ii). Further, the sale of PHI does not include providing access to the individual under 164.524, but it may include providing copies to a third party based on an authorization at a rate that is above a reasonable, cost-based fee. In that circumstance, the authorization must include a statement that the disclosure will result in remuneration to the covered entity.

[257] *See* 45 CFR 164.502(a)(5)(ii)(B)(2)(viii).

cost transfer would include requests to direct non-electronic copies of PHI in an EHR to third parties and would also include requests to direct electronic copies of PHI not in an EHR that previously would have been made as part of the right of access, and that could be provided based on a valid authorization under the proposed rule.

vii. Notice of Access and Authorization Fees

Individuals report some barriers to accessing PHI due to surprisingly high bills for requested copies. To increase an individual's awareness of the cost of access and of sending copies to third parties and to enhance the ability for an individual to plan for such expenses, the Department proposes to expressly require in regulation that covered entities provide advance notice of approximate fees for copies of requested PHI by: (i) posting a fee schedule online for all readily producible electronic and non-electronic forms and formats for copies if the covered entity has a website; (ii) providing the notice of fees to individuals upon request; and (iii) providing an individualized estimate of access and authorization fees upon request. The Department expects that this advance notice of fees requirement would provide certainty and improve access to PHI and payment for copies of PHI, to the benefit of individuals and covered entities. The Department also believes that many entities already provide such notice of fees, and thus the requirement to post the fee schedule should create only minimal additional expense beyond revising the fee schedule itself.

viii. Technical Amendment to Required Disclosures by Business Associates

The Department proposes a technical amendment to clarify in 45 CFR 164.502(a)(4)(ii) that a business associate is required to disclose PHI to the covered entity so the covered entity can meet its access obligations, but if the business associate agreement provides that the business associate will provide access directly to the individual or the individual's designee, the Privacy Rule requires the business associate to do so. The proposed change would expressly insert a reference to the business associate

agreement as the factor triggering required disclosures by the business associate to the individual or the individual's designee instead of to or through the covered entity.

b. Reduce Identity Verification Burden for Individuals Exercising the Right of Access

Some covered entities impose seemingly unreasonable verification requirements on individuals seeking to obtain their PHI pursuant to the individual right of access. Examples include requiring individuals to request their PHI in person, or even to go through the process (and potential added expense) of obtaining a notarization on a written request, to exercise their right of access.

To address these barriers to an individual's access to their health information, the Department proposes to modify 45 CFR 164.514(h)(1) to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual requesting PHI pursuant to the individual right of access. In addition, the Department would clarify that unreasonable verification measures include requiring individuals to provide proof of identity in person when a more convenient remote verification measure is practicable for the covered entity, requiring individuals to obtain notarization of access requests, or any other measure that creates a barrier to, or unreasonably delays, an individual's exercise of their rights. The Department also proposes to clarify that a covered entity that implements a requirement for individuals to submit a request for access in writing, pursuant to 45 CFR 164.524(b)(1), would not be permitted to do so in a way that imposes unreasonable burdens on individuals. This proposed change would provide additional clarity regarding the interaction between the individual right of access provisions and the verification provisions of the HIPAA Rules, and ensure that individuals do not have to expend unnecessary effort or expense when other methods are practicable for the covered entity.

While some covered entities would review and update their policies and procedures as a result of these proposals, which would cause them to incur some

additional costs, the Department believes that entities would benefit from the regulatory certainty, and most entities would not need to change their policies and procedures because they currently do not impose unreasonable requirements on individuals.

c. Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management

Some covered entities reported that, due to uncertainty about which provisions of the Privacy Rule apply in certain circumstances, they do not request or disclose PHI even when doing so would support care coordination and case management activities that constitute health care operations, which would facilitate the transformation of the health care system to value based care. Some have interpreted the existing definition of health care operations to include only population-based case management and care coordination, which would appear to exclude individual-focused case management and care coordination by health plans. Because health plans do not perform treatment functions under HIPAA, such an interpretation could limit a health plan's ability to perform such individual-level care coordination and case management activities.

The Department proposes to modify the definition of health care operations[258] to provide clarity to covered health care providers and health plans that "health care operations" includes not only population-based care coordination and case management, but also individual-focused care coordination and case management activities – and thereby facilitate those beneficial activities.

d. Creating an Exception to the Minimum Necessary Standard for Certain Disclosures for Care Coordination and Case Management

Uncertainty about how to apply the minimum necessary standard creates fears of HIPAA enforcement action among covered entities that could inhibit information sharing, and may result in less efficient and effective care. Because entities that qualify only as

---

[258] 45 CFR 164.501.

health plans do not perform treatment functions, any care coordination or case management activity conducted by such a health plan is a health care operation, subject to the minimum necessary standard. Disclosures by health care providers for treatment, including care coordination and case management, are subject to the minimum necessary standard only when the disclosure is made to a third party that is not a health care provider. Thus, the rule imposes greater restrictions on health plans than on covered providers when conducting care coordination and case management activities related to an individual.

The Department proposes to add an express exception to the minimum necessary standard for disclosures to or requests by a health plan or covered health care provider for individual-level care coordination and case management activities that constitute treatment or health care operations. This proposal would relieve covered entities from the requirement to make determinations about the minimum information necessary (or whether it is reasonable to rely on the requestor's representation that it is the minimum necessary PHI) when the request is from, or the disclosure is made to, a covered health care provider or health plan for individual-level care coordination and case management activities. This proposed exception would apply only to those activities that support individual-level care coordination and case management, and not population-based activities. As the Department described above, commenters on the 2018 RFI, including covered entities, expressed concern about permitting additional disclosures without minimum necessary restrictions. The Department believes drawing a distinction between disclosures for individual-level versus population-based activities is responsive to these concerns, as disclosures for population-based activities lack the same nexus that individual-level activities have to the treatment of specific individuals.

As such, the proposal would enable health plans and covered health care providers to more easily request and disclose PHI for care coordination and case management for

individuals. This proposal, in conjunction with the proposed clarification to the definition of health care operations, would result in significant cost savings to covered entities on an ongoing basis as they are relieved of conducting minimum necessary evaluations for care coordination and case management requests and disclosures among covered health care providers and health plans. Health plans and covered health care providers would continue to be responsible for meeting the minimum necessary requirements that apply to the *uses* of PHI for treatment and health care operations purposes[259] and to uses, requests, and disclosures for other purposes, including population-based activities, when applicable.[260]

e. Disclosing PHI to Social Services Agencies and Community based Organizations to Facilitate Care Coordination and Case Management.

Many covered entities that are health care providers make disclosures to social services agencies and community based organizations only after obtaining a valid authorization from the individual, or never disclose PHI to these health-related services--even when it would facilitate the individual's treatment. Some covered entities may not be aware that the Privacy Rule generally permits disclosure to social services agencies and community-based organizations for care coordination and case management.[261] Others may be uncertain about the scope of the permission to disclose or about when they need a business associate agreement with the recipient, and may fear that they will inadvertently violate the HIPAA Rules if they make such disclosures.

The Department therefore proposes to expressly permit covered entities to disclose PHI to social services agencies, community-based organizations, HCBS providers, or similar third parties that provide or coordinate health-related services that are needed for

---

[259] *See* 45 CFR 164.502(b)(1); 164.514(d)(2).
[260] *See* 45 CFR 164.502(b); 164.514(d).
[261] *See* 45 CFR 164.506. *See* OCR FAQ, Does HIPAA permit health care providers to share PHI about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? Available at https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html.

care coordination and case management with respect to an individual. Although such disclosures generally may be permitted as treatment or certain health care operations activities under the Privacy Rule, creating an express permission would provide clarity and assurance to covered entities about their ability to disclose PHI to such third parties for individual-level care coordination and case management. In addition, the premable explains when these third parties are business associates of the disclosing entities, and thus when a business associate agreement is required. This proposed change would facilitate greater wraparound care and targeted services for individuals, leading to better health outcomes. The Department expects that the costs for implementing this proposed change would be limited to changing policies and procedures, to the extent that some covered entities have limited their disclosures to agencies and organizations due to uncertainty about current policies.

f. Disclosing PHI when Needed to Help Individuals Experiencing Substance Use Disorder, Serious Mental Illness, and in Emergency Circumstances.

Some covered entities are reluctant to disclose PHI to family members and other caretakers of individuals facing health crises, including individuals experiencing SMI and SUD (including opioid use disorder), for fear of violating the Privacy Rule. To help address this reluctance, the Department proposes to amend the five following provisions of the Privacy Rule to replace "the exercise of professional judgment" with a "good faith belief" as the standard to permit uses and disclosures in the best interests of the individual: (1) Parent or guardian not the individual's personal representative, (2) Facility directories, (3) Emergency contacts, (4) Emergencies and incapacity, and (5) Verifying requestor's identity. The Department also proposes to apply a presumption of compliance when covered entities make a disclosure based upon a good faith belief that the disclosure is in the best interests of the individual with regard to those five provisions (by adding a new subsection (k) to 45 CFR 164.502), and to replace "serious and imminent threat" with

"serious and reasonably foreseeable threat" in 45 CFR 164.512(j)(1)(i)(A) as the standard under which uses and disclosures needed to prevent or lessen a threat are permitted.

The Department believes modifying the Privacy Rule to further encourage such disclosures would help health care providers, individuals, families, and caregivers assist in treatment and recovery. The Department also believes these proposed modifications would address the specific circumstances where more information disclosure is needed to better coordinate care for individuals experiencing SUD, SMI, and health related emergencies.

The Department anticipates that covered entities would incur costs to implement the changes due to revising policies and procedures and updating workforce member training, covered entities likely would experience (unquantified) cost savings due to improved patient care and harm reduction (*e.g.,* potentially decreasing the need for costly emergency care), and less perceived need to obtain legal review of each disclosure made under the changed provisions.

g. Changing the NPP Requirements

Comments on the 2018 RFI described the requirement for covered entities to make a good faith effort to obtain an individual's signed acknowledgment of receipt of the NPP as unduly burdensome and confusing to patients and health care workers, to the extent that, at times, it causes a barrier to treatment.

The Department proposes to eliminate the requirements for a covered health care provider to obtain a written acknowledgment of receipt of the NPP (and to retain such documentation for six years) and to replace them with an individual right to discuss the NPP with a person designated by the covered entity. In addition, the Department proposes to modify the content requirements of the NPP to specify to individuals that the notice provides information about: (1) how to access their health information, (2) how to file a HIPAA Privacy Rule complaint, and (3) individuals' right to receive a copy of the notice and ability to discuss its contents with a designated person. The required header also

would specify whether the designated contact person is available onsite and must include a phone number and email address by which to reach the designated person. Further, the Department proposes to modify the required element of NPPs to describe how an individual can exercise the right of access to obtain a copy of their records at limited cost or, in some cases, free of charge, and to direct a covered health care provider to transmit an electronic copy of PHI in an electronic health record to a third party. Finally, the Department proposes to add an optional element to the NPP to inform individuals of alternatives for obtaining or requesting to send copies of PHI to a third party when the individuals seek to send PHI to a third party in a manner that does not fall within the access right.

To implement these proposed changes, covered entities would incur one-time costs for revising policies and procedures and training, as well as for updating the NPP. However, by replacing the acknowledgment process for all new patient encounters with a right to discuss the NPP, upon request, covered health care providers would experience ongoing costs savings from reduced paperwork burdens and the (likely small) proportion of individuals who contact the designated person would benefit from having meaningful discussions about an entity's privacy practices.

h. Permitting Disclosures for Telecommunications Relay Service (TRS)

Stakeholders have requested that the Department ensure that covered entities and business associates are able to disclose PHI to TRS communication assistants for individuals and workforce members, and to specifically address the use of TRS by covered entity and business associate workforce members to share PHI with other workforce members or outside parties as needed to perform their duties. These stakeholders have shared anecdotal accounts in which a covered entity or business associate refuses to allow a workforce member to use this essential service because of

concerns about violating the Privacy Rule if they do not have a business associate agreement with the TRS provider.

The Department proposes in 45 CFR 164.512(m) to expressly permit covered entities (and their business associates, acting on the covered entities' behalf) to disclose PHI to TRS communications assistants to conduct covered functions.[262] This permission would cover all disclosures to TRS communications assistants, including communications necessary for care coordination and case management, relating to any covered functions performed by or on behalf of covered entities. The Department also proposes to add a new subsection (v) to 45 CFR 160.103(4) to expressly exclude TRS providers from the definition of business associate. This proposal would ensure that covered entities and business associates do not bear the burdens of analyzing whether they need business associate agreements with TRS providers (which provide services to the public, not covered entities and business associates) and, potentially, establishing such agreements, resulting in a cost savings for entities with workforce members who need TRS.

i. Expanding the Permission to Use and Disclose the PHI of Armed Forces Personnel to Cover all Uniformed Services Personnel

The existing rule limits the ability of the USPHS and NOAA Commissioned Corps to facilitate care coordination and case management for Corps personnel, because the Armed Forces permission to use and disclose PHI – which is important for ensuring that personnel meet medical readiness standards, and thus for fulfilling the Commissioned Corps' missions – does not apply to the USPHS and NOAA Commissioned Corps. The permission is important because personnel and the broader population are put at risk when personnel do not disclose medical conditions to Commissioned Corps leaders and are deployed on a Commissioned Corps mission, which often involve emergency situations or austere circumstances.

---

[262] The terms "Telecommunications Relay Service" and "Telecommunications Relay Service Communications Assistant" have the same meaning used in 47 CFR Part 64.

To improve care coordination and case management for individuals serving in the Uniformed Services, the Department proposes to expand to all Uniformed Services the Armed Services express permission for covered entities to use and disclose PHI, thus permitting USPHS and NOAA Commissioned Corps to use and disclose the PHI of such personnel for mission requirements and veteran eligibility.[263] The Department anticipates that the costs for covered entities to revise their policies and procedures to include such personnel would be minimal, as the proposed changes would merely extend existing permissions and the expanded disclosure permission would relieve covered entities of the need to obtain an individual's valid authorization.

3. Cost-Benefit Analysis

a. Overview and Methodology

For purposes of this RIA, the proposed rule adopts the list of covered entities and costs assumptions identified in the Department's 2019 Information Collection Request (ICR).[264] The Department also relies on certain estimates and assumptions from the 1999 proposed Privacy Rule[265] that remain relevant, and the 2013 Omnibus Rule,[266] as referenced in the analysis that follows.

In addition, the Department quantitatively analyzes and monetizes the impact that this proposed rule may have on covered entities' actions to re-train their employees on, and adopt policies and procedures to implement, the legal requirements of this proposed rule. The Department analyzes the remaining benefits and burdens qualitatively because of the uncertainty inherent in predicting other concrete actions that such a diverse scope of covered entities might take in response to this proposed rule. The Department requests comment on the estimates, assumptions and analyses contained herein – and any relevant

---

[263] 45 CFR 512(k), Standard: Uses and disclosures for specialized government functions.
[264] 84 FR 34905 (July 19, 2019).
[265] 64 FR 59918 (November 3, 1999).
[266] 78 FR 5566 (January 25, 2013).

information or data that would inform a quantitative analysis of proposed reforms that the Department qualitatively addresses in this RIA.

For reasons explained more fully below, the proposed changes to the right of access, acknowledgment of the NPP, and several use and disclosure permissions would result in net economic cost savings of approximately $3.2 billion over five years based on the proposed changes.

Table 2.

Accounting Table of Estimated Benefits and Costs of All Proposed Changes, in Millions						
COSTS	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total**
Undiscounted	$996	$55	$55	$55	$55	**$1,218**
3% Discount	$834	$45	$44	$43	$41	$1,007
7% Discount	$664	$35	$32	$30	$28	$789
COST SAVINGS	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total**
Undiscounted	$880	$880	$880	$880	$880	**$4,400**
3% Discount	$737	$716	$695	$675	$655	$3,477
7% Discount	$586	$548	$512	$479	$447	$2,573
NET (undiscounted)						**Savings $3,182**
Non-quantified benefits and costs are described below.						

b. Baseline Assumptions

The Department based its assumptions for calculating estimated costs and benefits on a number of publicly available datasets, including data from the U.S. Census, the U.S. Department of Labor, Bureau of Labor Statistics (BLM), CMS, and the Agency for Healthcare Research and Quality (AHRQ). All calculations using mean hourly wages include benefits and overhead by multiplying the mean hourly pay for an occupation by

two.[267] The Department relies on the annual number of U.S. health care encounters as reported by the AHRQ, 2.46 billion, for some of its calculated estimates.[268]

Table 3**.**

Annual U.S. Health Care Encounters	
Type of Encounters	**# of health care visits or days in residence**
Physician office visits	923 million
Hospital outpatient	803 million
Nursing home days	500 million
Hospice days in residence	120 million
Home health visits	117 million
TOTAL ANNUAL	**2,463 million or 2.46 billion**

Implementing the proposed regulatory changes likely would require covered entities to engage workforce members or consultants for certain activities. The Department assumes that a lawyer would draft or review needed changes to HIPAA policies, including revisions to the NPP and the access fee schedule, and that a medical and health services manager (*e.g.,* compliance manager) would develop related changes to procedures. The Department expects a training specialist would revise the needed HIPAA training and a web developer would post the online access fee schedule and updated Notice of Privacy Practices. The Department further anticipates that a medical records technician or another workforce member at that pay level would implement changes to the right of access, that a nurse or health professional at a similar pay level would disclose PHI to a patient's family, friends, or others in a position to prevent harm, that a medical assistant would submit requests for PHI to health care providers and health plans, and that a receptionist would implement changes to the disclosure of directory information. To the extent that these assumptions would impact the Department's estimate of costs, the Department welcomes comment on its assumptions, particularly those in which the Department identifies the level of workforce member (*i.e.,* clerical staff, professional) that would be engaged in

[267] This represents an increase of 50 percent from the Department's prior HIPAA Rules analyses.
[268] 2017 "National Healthcare Quality and Disparities Report," Agency for Healthcare Research and Quality (September 2018). AHRQ Pub. No. 18-0033-EF, available at https://www.ahrq.gov/research/findings/nhqrdr/nhqdr17/index.html.

activities, and the amount of time that particular types of workforce members spend conducting activities related to this NPRM as further described below.

Table 4.

Occupational Pay Rates[A]	
Occupation Code and Title	**Benefit Loaded Hourly Labor Wage[B]**
23-1011 Lawyer	$139.72
11-9111 Medical and Health Services Manager	$110.74
29-2098 Medical Records Technician	$44.80
31-9092 Medical Assistant	$34.34
13-1151 Training and Development Specialist	$63.12
29-1141 Registered Nurse	$74.48
43-4171 Receptionist and Information Clerk	$30.04
15-1134 Web Developer and Digital Interface Designer	$79.20

A Bureau of Labor Statistics (BLS), U.S. Department of Labor, "Occupational Employment and Wages," May 2019, available at https://www.bls.gov/oes/current/oes_stru.htm.
B To incorporate employee benefits, these figures represent a doubling of the BLS median hourly wage.

The Department assumes that the vast majority of covered entities would be able to incorporate changes to their workforce training into existing HIPAA training programs because the total time frame for compliance from date of finalization would be 240 days, just short of a year. In addition, the Department has included additional time spent in training by medical records technicians to the calculation of burden hours, due to the number of proposed changes to the right of access for which they would be responsible.

For a number of proposals where the Department is incorporating existing interpretive guidance into regulation, the Department assumes that a portion of covered entities are already voluntarily engaging in the best practices highlighted in OCR guidance. For example, the Department is aware that 35 percent of hospitals in one study had posted an access fee schedule online,[269] and assumes that many entities are voluntarily providing individuals with an estimate of access fees, consistent with its widely publicized

[269] See Lye CT, Forman HP, Gao R, et al. "Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records." JAMA Netw Open. 2018;1(6):e183014, available at https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2705850.

guidance,[270] although not necessarily doing so in writing. Even for entities that are not providing advance fee estimates, the Department assumes that they are providing some type of billing statement when charging fees for access requests, which would necessitate having a fee structure.

With respect to cost savings, the Department proposes to recognize a previously unquantified burden associated with covered entities making minimum necessary determinations. The Department assumes that this burden, associated with time spent by workforce member equivalent to a Medical and Health Services Manager, would necessarily be reduced by alleviating the need to make the determination for disclosures for care coordination or case management on behalf of an individual. For cost savings associated with the proposal to remove the requirement that covered entities obtain a signed acknowledgement of the covered entity's NPP or document a good faith effort to do so, the Department assumes that time spent by clerical staff for a direct treatment provider, such as a Receptionist or Information Clerk, will vary widely depending on the practice of that provider in managing its own NPP process and whether the process is paper-based or electronic. For all of the proposed regulatory changes that covered entities are currently allowed to implement, consistent with its interpretive guidance, the Department seeks comment on the extent to which covered entities are already voluntarily implementing the proposed requirements, and thus would not incur additional costs or realize savings as a result of the proposed changes.

c. Covered Entities

This proposed rule would apply to HIPAA covered entities (*i.e.,* health care providers that conduct covered electronic transactions, health plans, and in certain

---

[270] *See* 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

circumstances, health care clearinghouses[271]), which the Department estimates to be 774,331 business establishments (see Table 5). By calculating costs for establishments, rather than firms (which may be an umbrella organization over multiple establishments), there is some tendency toward overestimating some burdens, because certain costs would be borne by a parent organization rather than each separate facility. Similarly, benefits and transfers would be overestimated, as entity assumptions flow through to those quantifications as well. However, decisions about what level of an organization is responsible for implementing certain requirements likely vary across the health care industry. The Department requests data on the extent to which certain burdens are borne by each facility versus an umbrella organization.

The Department expects that covered health care providers and health plans would be most directly affected by the proposed rule. While certain proposed changes would affect some providers and plans differently than others, all affected covered entities would need to adopt or change some policies and procedures and re-train some employees. Affected health care providers would include many federal, state, local, tribal, and private sector providers. The Department has not separately calculated the effect on business associates because the primary effect is on the covered entities for which they provide services. To the extent that covered entities engage business associates to perform activities under the proposed rule, the Department assumes that any additional costs will be borne by the covered entities through their contractual agreements with business associates. The Department requests data on the number of business associates (which may include health care clearinghouses acting in their role as business associates of other covered entities) that would be affected by the proposed rule and the extent to which they

[271] Only certain provisions of the Privacy Rule apply to clearinghouses as covered entities. In addition, certain provisions apply to clearinghouses in their role as business associates of other covered entities. *See* 45 CFR 164.500(b) and (c). Because the provisions addressed in this proposed rule generally do not apply directly to clearinghouses, the Department does not anticipate that these entities would experience costs associated with this proposed rule.

may experience costs or other burdens not already accounted for in the estimates of covered entity burdens.

According to Census data, there are 880 Direct Health and Medical Insurance Carrier firms compared to 5,350 Insurance Carrier firms, such that health and medical insurance firms make up 16.4% of insurance firms. Also, according to Census data, there are 2,773 Third Party Administration of Insurance and Pension Funds firms. The Department assumes that 16.4% of these firms service health and medical insurance. As a result, the Department estimates that 456 of these firms are affected by this proposed rule. Similarly, the Department estimates that 783 associated establishments would be affected by this proposed rule. See Table 5 below.

There were 67,753 community pharmacies (including 19,500 pharmacy and drug store firms identified in US Census data) operating in the U.S. in 2015.[272] Small pharmacies largely use pharmacy services administration organizations (PSAOs) to provide administrative services, such as negotiations, on their behalf.[273] A 2013 study identified 22 PSAOs, and notes there may be more in operation.[274] Based on information received from industry, the Department adjusts this number upward and estimates that the proposed rule would affect 40 PSAOs. The Department assumes that costs affecting pharmacies are incurred at each pharmacy and drug store firm and each PSAO.

Unless otherwise indicated, the Department relies on data about the number of businesses from the U.S. Census.[275] The Department requests public comment on these estimates, including those for third party administrators and pharmacies where the

---

[272] *See* Qato, Dima Mazen; Zenk, Shannon; Wilder, Jocelyn; Harrington, Rachel; Gaskin, Darrell; Alexander, G. Caleb (2017). "The availability of pharmacies in the United States: 2007–2015." *PLOS ONE. 12 (8): e0183172,* available at https://doi.org/10.1371/journal.pone.0183172.
[273] Government Accountability Office, GAO-13-176, (January 29, 2013), discussing generally that small and independent pharmacies often lack internal resources to support these services, available at https://www.gao.gov/products/GAO-13-176.
[274] *Ibid*.
[275] *See* "2015 Statistics of U.S. Businesses (SUSB) Annual Data Tables by Establishment Industry," (January 2018), available at https://www.census.gov/data/tables/2015/econ/susb/2015-susb-annual.html.

Department has provided additional explanation. The Department additionally requests detailed comment on any situations in which covered entities other than those identified here would be impacted by this rulemaking.

Table 5.

Covered Entities			
NAICS Code	**Type of Entity**	**Firms**	**Establishments**
524114	Health and Medical Insurance Carriers	880	5,379
524292	Third Party Administrators	456	783
622	Hospitals	3,293	7,012
44611	Pharmacies	19,540	67,753
6211-6213	Office of Drs. & Other Professionals	433,267	505,863
6215	Medical Diagnostic & Imaging	7,863	17,265
6214	Outpatient Care	16,896	39,387
6219	Other Ambulatory Care	6,623	10,059
623	Skilled Nursing & Residential Facilities	38,455	86,653
6216	Home Health Agencies	21,829	30,980
532291	Home Health Equipment Rental	611	3,197
Total		**549,713**	**774,331**

d. Individuals Affected

The Department believes that, by having some contact with a HIPAA covered entity, a large proportion of the 329 million individuals in the United States[276] would be affected by this proposed rule, including those who do not have health insurance coverage or do not have a health care visit in the current year. The widespread effect on individuals would be due primarily to the proposed changes to the right of access, affecting the speed of access, the ability to easily direct the transmission of ePHI in an EHR to health plans and health care providers, notice of access and authorization fees, and the access and authorization fees that could be charged, as well as changes to covered entities' ability to

[276] U.S. Census Population Clock, available at https://www.census.gov/popclock/.

disclose PHI to an individual's family, friends, and others who are involved in care or payment for care, or who are in a position to prevent harm, and disclosures for care coordination and case management to third parties such as social services agencies, community-based support organizations, and HCBS providers. Eliminating the requirement for a covered health care provider to attempt to obtain a signed acknowledgment of the NPP, and replacing it with the individual right to discuss a covered entity's NPP, will affect nearly all individuals who receive services from a health care provider.

To calculate the potential monetary effect on individuals for the proposed changes to allowable fees for certain copies of PHI, the Department first estimated a baseline average cost for an access request under the current Privacy Rule requirements. The Department increased the estimated average time for providing a copy of PHI requested from 3 minutes in its prior analyses to 5 minutes, resulting in an average labor cost of $3.73 per request.[277] The Department requests data on costs from covered entities' data and comments on individuals' experiences when charged a fee for copies of PHI or when it is provided for free. The Department has heard that many individuals are able to obtain a copy of their PHI without charge, but in contrast, others receive unexpectedly large bills for obtaining copies, possibly in violation of the HIPAA right of access fee limitations.[278]

The Department believes the persons most affected by the proposed changes to the rule permitting certain disclosures based on "good faith" would include individuals who are unable to agree or object to the use or disclosure of PHI due to incapacity or who are at

---

[277] Based on 5 minutes of a medical records technician's hourly wage, as noted in Table 4.

[278] A recent study found access fees for a 200-page record to range from $0 to $281.54. Lye CT, Forman HP, Gao R, et al. "Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records." *JAMA Netw Open.* 2018:1(6):e183014. *See also* GAO-18-386, "MEDICAL RECORDS Fees and Challenges Associated with Patients' Access*,"* GAO Report to Congress (May 2018), available at https://www.gao.gov/assets/700/691737.pdf. *See also* 2016 Access Guidance, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

risk of harming themselves or others and loved ones and caregivers of such individuals. This would include those experiencing a health emergency, SUD, or SMI; and individuals to whom permissible disclosures would be made as a result of the rule, such as family members and other caregivers, and persons in a position to prevent or lessen (*e.g.,* make less likely or less severe) a threat to health or safety. The proposed changes also would include individuals experiencing temporary incapacity due to injuries or health conditions, and those with long-term incapacity, such as from Alzheimer's disease or, in some cases, traumatic brain injury or stroke.

The individuals most affected by the proposal to add a regulatory permission for workforce members to disclose PHI to a TRS communications assistant, would be the estimated 170,000 persons employed in the health care sector who are deaf, hard of hearing, deaf-blind, or who have a speech disability.[279]

e. Qualitative Analysis of Non-quantified Benefits

Clarity Regarding the Scope of EHRs and Personal Health Applications

The Department proposes to add a new definition within the Privacy Rule at 45 CFR 164.501 for the term "Electronic health record" or EHR to clarify the intended scope of the Privacy Rule provisions pertaining to ePHI in an EHR. Additionally, the Department proposes to add a new definition for the term "Personal health application" to clarify the intended scope of the proposed changes to the right of access, including the form and format requirements and adjustments to allowable access fees. These definitions would benefit covered entities and individuals by increasing the understanding of how to

---

[279] *See* "Task Force on Health Care Careers for the Deaf and Hard-of-Hearing Community, Final Report" (March 2012), p. 14, 79 (Table 4), available at https://www.rit.edu/ntid/healthcare/task-force-report; *see also* Moreland CJ, *et al.,"* Deafness among physicians and trainees: a national survey." Acad. Med. 2013 Feb; 88(2):224-32, available at https://journals.lww.com/academicmedicine/Fulltext/2013/02000/Deafness_Among_Physicians_and_Trainees___A.27.aspx.

apply the proposed changes to the right of access for PHI in an EHR, including allowable fees (if any).

Improved Access to Inspect PHI

The Department proposes to add a new subsection to amend the right of access provision at 45 CFR 164.524(a)(1) to establish that the right to inspect PHI generally includes the right to take notes, take photographs, and use other personal resources to capture their PHI in a designated record set, but that a covered entity is not required to allow an individual to connect a personal device to the covered entity's information systems when it would create a risk to the security of the covered entity's electronic systems. Expressly enabling individuals to take notes and photographs when inspecting their own PHI in person would help individuals exercise their right of access in a convenient way. Most individuals who inspect, rather than request a copy, of their PHI otherwise would be unable to retain the amount or details of PHI that would assist them with decision-making.

Reducing the Timeframe for Access to PHI (from 30 days to 15 calendar days)

The Department proposes to amend 45 CFR 164.524(b) to shorten the allowable time limit for covered entities to provide copies of PHI by half, from 30 days (with the possibility of one 30-day extension) to 15 calendar days (with the possibility of one 15 calendar-day extension). In addition, where other federal or state law time limit requires covered entities to provide individuals with access to the PHI requested in less than 15 calendar days, the Department proposes to deem such time limits "practicable" under the Privacy Rule. The Department also proposes to add a requirement for covered entities to develop and implement a policy to explicitly prioritize urgent or otherwise high priority requests (especially with respect to health and safety) so as to limit the need to use a 15 calendar day extension for such requests. The Department does not propose to define what constitutes an urgent or high priority request, and does not intend with this proposal to

encourage covered entities to require individuals to reveal the purposes for their requests for access. However, examples of urgent or high priority requests could include when an individual voluntarily reveals that the PHI is needed in preparation for urgent medical treatment, or that the individual needs documentation of a diagnosis of severe asthma to be allowed to bring medication to school the next day.

The proposal to shorten the time for covered entities to provide individuals with access to their PHI would improve patient-centered care by empowering individuals to review their health information in a timely manner and enhance patient decision making. It also would improve care coordination by enabling individuals to share their records more rapidly with other providers, informal caregivers, community based support services, and family members, as just a few examples. The Department believes that the overall effect would lead to improved health care communications and improved health outcomes. It also may reduce health expenditures due to a reduction in unnecessary, duplicative medical testing, reductions in medical errors, and more timely care delivery. For example, a research study found that the use of health information is "important for improving patient attitudes regarding their health status and confidence in caring for themselves. Perceived health-status and patient confidence, in turn, are associated with preventative health behaviors."[280]

Although nine states require some health care entities to provide access within 15 days or a lesser period,[281] these requirements do not apply to all entities within such states.

---

[280] Hearld, K. R., Hearld, L. R., Budhwani, H., McCaughey, D., Celaya, L. Y., & Hall, A. G. (2019). The future state of patient engagement? Personal health information use, attitudes towards health, and health behavior. *Health services management research*, *32*(4), 199-208.

[281] California, Cal. Health & Safety Code 123110 (5 days to inspect; 15 days to receive a copy); Colorado, 6 Colo. Regs. 1011:1:II-5.2 (24 hours to inspect; 10 days to receive a copy); Hawaii, HRS 622.57 (10 days to receive a copy); Louisiana, LSA-R.S. 40:1165.1 (15 days to receive a copy); Montana, MCA 50-16-541(10 days, copy and inspect); Tennessee, TCA 63-2-101 (10 days to receive a copy); Texas, Tex. Health & Safety Code 241.154 (hosp.) (15 days, copy and inspect); Tex. Occupations Code 159.006 (physicians) (15 days to receive a copy), Tex. Health & Safety Code 181.102 (15 days to receive electronic copies), Tex. Admin. Code 165.2 (physicians) (15 days to receive a copy); and Washington, Wash. Rev. Code 70.02.080 (15 days, copy and inspect).

Therefore, the proposed shortened time requirement within HIPAA would expand the benefits of the short time limits to individuals interacting with all covered entities, even in states that already require it for certain health care providers.

Improving Production of Required Formats of PHI

The Department proposes to modify 45 CFR 164.524(c)(2) to clarify that where a covered entity is subject to other federal law that requires the provision of access to individuals in a particular form and format, such form and format is deemed readily producible under the Privacy Rule's individual access right. To the extent that other applicable federal laws require production of copies of PHI in a certain form and format, the proposed inclusion of these finalized requirements within the Privacy Rule would not significantly increase covered entities' compliance burdens. However, by providing that a form and format required to be produced under other federal law are readily producible under the Privacy Rule, the change would allow the Department to enforce the individual's right to receive their PHI in that form and format. Although quantifying the impacts of this provision is challenging, the Department believes the proposed clarification would benefit individuals by enhancing their ability to receive PHI in the form and format requested. It also would benefit covered entities by providing greater certainty about the Department's expectations regarding when a requested form and format is "readily producible."

The Department also proposes in 45 CFR 164.524(c)(2(iv) and (d)(4) to add a new set of parallel requirements so that when covered entities offer to provide or direct a summary of PHI in lieu of requested copies, they must inform individuals that they retain the right to obtain or direct the requested copies if they do not agree with the offered summary. These requirements would not apply when the covered entity denies access on unreviewable or reviewable grounds, in which case the covered entity must implement the required procedures for such denial under 45 CFR 164.524(e). These requirements would

benefit individuals by ensuring that they are aware of their access rights and empowered to make choices about the form of access with full knowledge about the available options under the right of access. The proposals would benefit covered entities by engaging individuals in more robust discussions about requested forms of access early in the process, thus reducing potential complaints and fee disputes.

Clarifying the Right to Direct the Transmission of Certain PHI to Health Care Providers and Health Plans

The Department proposes to modify 45 CFR 164.524(c)(3)(ii) (and redesignate it as 45 CFR 164.524(d)) to clarify the access right to direct the transmission of an electronic copy of PHI in an EHR to another person designated by the individual and add a new provision for access requests to be submitted by covered health care providers and health plans at the request of the individual in 45 CFR 164.524(d)(7). The Department proposes to require covered health care providers and health plans to submit individuals' requests directing electronic copies of PHI in an EHR to be transmitted back to the entity that submitted the request. The new provision would specify that a covered health care provider or health plan must submit an individual's request to transmit an electronic copy of PHI in an EHR from another health care provider or health plan when the request is clear, conspicuous, and specific (which may be orally or in writing, including electronically) and that the covered health care provider or health plan must submit the access request as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and information needed to make the request. The Department also proposes to add language clarifying that covered entities that receive access requests under this new provision are required to respond based on an individual's clear, conspicuous, and specific request.

The proposal to expressly include individual access requests submitted by health care providers and health plans as part of the right to direct the transmission of ePHI in an

EHR to a third party would improve care coordination and patient-centered care by enhancing the individual's ability to direct the sharing of ePHI among health care entities. The change would improve health care communications and assist individuals' decision-making as they consult with various health care providers and health plans, and evaluate treatment alternatives, recommendations, and health plan coverage. All health care providers and health plans would benefit from receiving electronic records from other covered entities more quickly under the shortened timeframe, and the proposal to explicitly require covered health care providers and health plans to submit requests for copies of ePHI as directed by the individual within the right of access would enhance covered entities' compliance with responding to such requests received from other covered entities because such disclosures would be mandatory. This means of obtaining access also would ease the burden on individuals to separately contact their other providers and request that they transmit electronic records to their treating physician. Instead, the individual may initiate such requests through the provider (or health plan) with whom they are currently communicating or receiving services, and who will receive the ePHI. Taken together, these changes would empower individuals by clarifying the scope of a patient's HIPAA rights and providing a convenient means to effectuate certain mandatory transfers of electronic medical records between covered entities.

Improving Access to PHI by Specifying When Access Must be Free of Charge

The Department proposes to modify 45 CFR 164.524(c)(4) to prohibit covered entities from charging fees for access when an individual inspects PHI about the individual in person or accesses an electronic copy using an internet-based application method. The Department proposes to expressly provide that covered entities may not charge a fee when an individual, in the course of inspecting PHI, takes notes or photographs, or uses other personal resources to capture the information.

All individuals would benefit from improved access to their PHI and regulatory requirements stating the circumstances in which access is always to be provided free of charge. In addition to any quantifiable increases in the number of access requests fulfilled without charge, the Department believes that individuals' abilities to manage their own health care and payment for care would be improved by improving access to their own PHI.

Additionally, although the Department is not expressly prohibiting fees when an individual uses an internet-based method to direct the transmission of an electronic copy of PHI in an EHR to a third party, the Department expects that, in most cases, there will be no allowable labor costs for such access.

Improving Access to Pricing Information for Copies of PHI

The Department proposes to add a new subsection 525 to 45 CFR 164 to require a covered entity to provide advance notice to individuals of the fees the entity charges for providing access to and copies of PHI. Specifically, the Department proposes to require a covered entity to post a fee schedule online (if they have a website) and make the fee schedule available to individuals at the point of service upon request. The notice must include: (i) all types of access to PHI available free of charge; (ii) approximate fees for copies of PHI provided to individuals under 45 CFR 164.524(a), to third parties designated by the individual under 45 CFR 164.524(d), and to third parties with the individual's valid authorization under 45 CFR 164.508; (iii) provide, upon request, an individualized estimate of the approximate fee that may be charged for the requested copy of PHI; and (iv) upon request, provide an individual with an itemized list of charges for labor, supplies, and postage, if applicable, that constitute the total fee charged.

The Department anticipates that all individuals interested in access to PHI would benefit from having advance notice of a covered entity's approximate fee schedule for standard or common data access requests for PHI, by learning about how they may access

their PHI for free, and obtaining pricing information for copies prior to or at the time of making an access request or a request for copies with a valid authorization. Readily available public information about access fees would also serve to promote compliance with the Privacy Rule because covered entities will want to avoid posting fee schedules that show noncompliance with fee limitations,[282] or that publicly misrepresent their business practices, and individuals will be empowered to insist on covered entities' compliance as well.

Providing an access and authorization fee schedule, and an individualized estimate of fees for an individual's request for copies of PHI upon request, would also benefit covered entities because this information is likely to prevent or resolve potential fee disputes that occur when individuals are surprised by unexpectedly high fees.

Improved Coordination of Care by Covered Entities, including for Population-based Activities

The Department proposes to add an exception to the minimum necessary standard in 45 CFR 164.502(b)(2) for disclosures to, or requests by, a health plan or covered health care provider for individual-level (*i.e.*, not population-based) care coordination and case management that constitute health care operations. The Department first recognized the ongoing annual burden of compliance with the minimum necessary standard in the 2000 Privacy Rule[283] and now quantifies the burden of this existing requirement. The Department believes the proposed exception to the minimum necessary standard, in addition to decreasing quantifiable burdens as described elsewhere, would contribute to

---

[282] In addition to the access fees limits contained in 45 CFR 164.524, the Privacy Rule limits the fees that may be charged for uses and disclosures of PHI based on an authorization. Under the Privacy Rule's provisions on the sale of PHI, covered entities generally must limit fees for disclosures pursuant to an authorization to a "reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law" or must state in the authorization that the disclosure will result in remuneration to the covered entity. *See* 45 CFR 164.502(a)(5)(ii)(B)(*2*)(*viii*); 45 CFR 164.502(a)(5)(ii)(A); 45 CFR 164.508(a)(4).

[283] *See* 65 FR 82462, 82767, 82773 (December 28, 2000).

non-quantifiable but qualitative improvements in the scale and design of care coordination and case management, and therefore improve health of individuals. Facilitating health plans' involvement in care coordination and case management may prove instrumental in improving individual health outcomes. The proposed change would eliminate some of the differential treatment between health plans' care coordination and case management disclosures under the health care operations provisions and covered health care providers' care coordination and case management under the provisions regarding treatment disclosures (which are not subject to the minimum necessary standard). The proposed change also would address the concerns of both covered health care providers and health plans about having to determine what PHI is or is not the minimum necessary for requests by, and disclosures to, health plans and health care providers, a requirement that may be an ongoing impediment to value-based care delivery and a disincentive to information sharing.

Increased Coordination of Care between Covered Entities and Third Parties such as Social Services Agencies, Community-Based Organizations, and HCBS Providers.

The Department proposes to add an express permission for a covered entity to disclose PHI for individual-level care coordination and case management to a social services agency, community based organization, HCBS provider, or other similar third party that provides health-related services to those specific individuals, as a new paragraph (6) in 45 CFR 164.506(c). The Department believes the proposed changes and clarifications about the disclosures permitted for care coordination and case management would help covered entities and others achieve their health-related missions, particularly those that are not health care providers or HIPAA covered entities. The Department has continued to hear that health care providers and health plans want to refer individuals to such organizations for health-related supportive services, but are reluctant to do so because of uncertainty regarding the applicable permissions and obligations. The

Department interprets the Privacy Rule to allow health care providers to disclose PHI for their own treatment activities to both covered entities and entities that are not subject to HIPAA, which may include supportive services in the community related to health. By expressly identifying social services agencies, community based organizations, and HCBS providers and similar third parties as entities to which PHI may be disclosed for individual-level care coordination and case management that constitute treatment or health care operations, the Department will remove regulatory uncertainty and ease the ability of covered health care providers to facilitate comprehensive transitions of care. The Department believes these proposed clarifications would affect at least 137,052 organizations providing social assistance to individuals.[284] The proposed clarifications to these use and disclosure permissions would enhance the ability of such organizations to receive PHI to improve service coordination and delivery for the individuals served within the scope of their respective missions. These organizations serve many individuals for whom supportive services are essential to regain health and maintain recovery and individuals who lack stable housing or communications capabilities, making the need for immediate referrals (*i.e.,* without needing to obtain an individual's valid authorization) imperative.

Improved Treatment and Recovery Outcomes Resulting from a Good Faith Standard with a Presumption of Compliance

The Department proposes to amend five provisions of the Privacy Rule to replace the exercise of "professional judgment" with a "good faith belief" as the standard to permit uses and disclosures in the best interests of the individual, and include a presumption of compliance with the good faith requirements. These proposed modifications would apply to uses and disclosures involving a parent or guardian who is

---

[284] *See* "2015 SUSB Annual Data Tables by Establishment Industry," (January 2018), available at https://www.census.gov/data/tables/2015/econ/susb/2015-susb-annual.html.

not the individual's personal representative (45 CFR 502(g)(3)(ii)(c)), facility directories (45 CFR 164.510(a)(3)(i)(B)), emergency contacts (45 CFR 164.510(b)(2)(iii)), limited uses and disclosures when the individual is not present or incapacitated (45 CFR 164.510(b)(3)), and verifying a Requester-Recipient's identity (45 CFR 164.514(h)(2)(iv)). The proposed presumption of compliance could be overcome with evidence that a covered entity acted in bad faith.

The Department believes that replacing the professional judgment standard with one based on good faith, as proposed, would result in improved treatment and recovery outcomes for individuals who are most affected, for example, by the current opioid crisis, as well as those experiencing SMI or other SUD, by facilitating the increased disclosure of PHI by covered entities to persons who care about the individual and who need to be involved in the individual's care. The Department expects that health care providers who have confidence in their ability to disclose information to individuals' family members, friends, and others involved in care or payment for care when it is in an individual's best interests, without fear of violating HIPAA, would be more likely to disclose PHI that could be used by those persons to provide needed care and support.

The Department does not have data to quantify such benefits, but research supports the conclusion that family involvement improves the engagement in treatment and recovery of these individuals.[285] For example, a study by Dobkin, Civita, Paraherakis, and Gill examined the effect of social support on substance use and treatment retention. They

---

[285] *See* "Alcohol and Drug Addiction Happens in the Best of Families . . . and it Hurts," U.S. Dept. of Health and Human Services, Substance Abuse and Mental Health Services Administration, available at https://store.samhsa.gov/shin/content//PHD1112/PHD1112.pdf; "Incorporating the family in a culturally appropriate fashion within routine clinical settings improves access to treatment, client participation in care, integration of care, and ultimately, clinical outcomes for populations with SMI and SED." Interdepartmental Serious Mental Illness Coordinating Committee, "The Way Forward: Federal Action for a System That Works for All People Living With SMI and SED and Their Families and Caregivers," U.S. Dept. of Health and Human Services, Substance Abuse and Mental Health Services Administration, (December 2017), Publication ID PEP17-ISMICC-RTC, available at https://store.samhsa.gov/system/files/pep17-ismicc-rtc.pdf.

found that "higher functional social support at intake is a positive predictor of retention in treatment, and a modest predictor of reductions in alcohol intake, but not in drug use."[286] Another study examined the effect of social support on women's substance abuse relapse within 6 months following residential treatment and found that "positive activities such as families getting along and helping each other during the post-discharge period significantly decreased the likelihood of relapse."[287] According to the National Institute on Drug Abuse of the National Institutes of Health, the degree of support from family and friends influences the degree of engagement by individuals with treatment and retention in treatment programs.[288] Therefore, the changes to the Privacy Rule proposed in this NPRM may result in improved outcomes in treatment and recovery.

Avoidance of Harm from Serious and Reasonably Foreseeable Threats

The Department proposes to amend the Privacy Rule at 45 CFR 164.512(j)(1)(i)(A) to replace the "serious and imminent threat" standard with the "serious and reasonably foreseeable threat" standard. This proposed change would permit covered entities to use or disclose PHI without determining whether the threat is imminent (which may be impossible to determine with any certainty), but rather whether it is likely to happen. The Department expects this proposed modification to improve the timeliness of uses and disclosures of PHI that would have otherwise occurred, but for the covered entity's uncertainty about whether a threat is "imminent." The Department believes that individuals, covered entities, and communities would benefit from threat reduction and

---

[286] Dobkin, P. L., Civita, M. D., Paraherakis, A., & Gill, K. (2002). The role of functional social support in treatment retention and outcomes among outpatient adult substance abusers. *Addiction*, *97*(3), 347-356.

[287] Ellis, B., Bernichon, T., Yu, P., Roberts, T., & Herrell, J. M. (2004). Effect of social support on substance abuse relapse in a residential treatment setting for women. *Evaluation and Program Planning*, *27*(2), 213-221.

[288] *See* Principles of Drug Addiction Treatment: a Research-Based Guide (3rd Edition), "What helps people stay in treatment?", U.S. Dept. of Health and Human Services, National Institutes of Health, National Institute on Drug Abuse, (January 2018), available at https://www.drugabuse.gov/publications/principles-drug-addiction-treatment-research-based-guide-third-edition/frequently-asked-questions/what-helps-people-stay-in-treatment.

improved health and safety as a result. The Department also proposes to add a new paragraph (5) to this provision to define "reasonably foreseeable." The Department's proposed definition of "reasonably foreseeable" would apply a reasonable person standard to permit uses and disclosures by covered health entities in instances where similarly situated covered entities would use or disclose PHI to avert a threat based on facts and circumstances known at the time of the disclosure. The proposed definition also would include an express presumption that threats to health or safety identified by a covered health care provider with specialized training, expertise, or experience in assessing an individual's risk to health or safety (such as a licensed mental or behavioral health professional)--and whose assessment relates to their specialized training, expertise, or experience--meet the definition of "reasonably foreseeable." A covered entity, however, need not have such specialized training, expertise, or experience in order to meet the reasonably foreseeable standard. The Department expects that these proposed changes to the standard at 45 CFR 164.512(j) would improve communication and coordination between health care providers, caregivers and others in a position to lessen harm and avert threats, including opioid overdose and incidents of mass violence.

Improved Understanding of Covered Entities' Privacy Practices

The Department proposes to add subsection (G) to 45 CFR 164.520(b)(1)(iv), to give individuals the right to discuss the NPP with a person designated by the covered entity as the contact person pursuant to section 164.520(b)(1)(vii). The Department proposes to include information about this right in the header of the NPP to ensure that individuals are aware of their ability to discuss the NPP with a designated person. Requiring that an entity's NPP include the name or title and contact information for a designated person who is available to provide further information about the covered entity's privacy practices, and adding an individual right to discuss the notice with the designated person, would help improve an individual's understanding of the covered

entity's privacy practices and the individual's rights with respect to his or her PHI. Even for individuals who do not request a discussion under this proposal, knowledge of the right may promote trust and confidence in how their PHI is handled.

Improved Access to Communications Assistance and Enhanced Service Delivery for Workforce Members who are Deaf, Hard of Hearing, or Deaf-blind, or who have a Speech Disability.

The Department proposes to amend the Privacy Rule at 45 CFR 164.512, by adding a new standard in paragraph (m) to expressly permit covered entities (and their business associates, when acting on the covered entities' behalf) to disclose PHI to Telecommunication Relay Service (TRS) communications assistants when such disclosures are necessary for a covered entity, or a business associate to conduct covered functions. This permission would cover all disclosures to TRS communications assistants, including communications necessary for care coordination and case management, relating to any covered functions performed by or on behalf of covered entities. The Department also proposes to expressly exclude TRS providers from the definition of business associate. The Department intends for these new provisions to ensure that regulated entities do not bear the burdens of analyzing whether they need a business associate agreement with a TRS and, potentially, establishing one before a workforce member discloses PHI to a TRS communications assistant, to assist the workforce member, in the course of performing their duties. Adding an express permission for covered entities' workforce members to share PHI via a TRS communications assistant would improve communications for health care delivery and benefit covered entities by supporting their compliance with employment nondiscrimination laws, such as the ADA. Further, by enhancing the ability of an estimated 170,000 workforce members[289] to perform the necessary communication tasks of their jobs, the proposed change would also have a

[289] *See "*Task Force on Health Care Careers for the Deaf and Hard-of-Hearing Community, Final Report," available at https://www.rit.edu/ntid/healthcare/task-force-report.

positive effect on health service delivery generally and improve health care services and payment for such services.

The Department requests comment or examples that could assist the Department in quantifying costs or cost savings in relation to the following:

- Any relationship between individuals' access to medical records and improved health outcomes, including data about any health effects related to the amount of time between a request for access and the provision of access;
- Any relationship between fees individuals pay to obtain medical records and the frequency with which the individual seeks treatment;
- Any relationship between the ease or difficulty faced by covered health care providers and health plans to make minimum necessary determinations and health outcomes of individuals or populations;
- Any relationship between the ease or difficulty faced by covered health care providers' and health plans' to disclose PHI based on a professional judgment standard or a good faith belief standard, and the frequency with which an individual will seek care from that provider or enroll with that plan, especially for treatment or coverage related to substance use disorders or serious mental illness.
- The frequency with which different types of covered entities currently disclose PHI based on:
    - Professional judgement about an individual's best interests; and
    - A good faith belief that a threat or harm is serious and imminent, and the type of harm; and
- Any relationship between improved compliance with non-discrimination laws, such as the ADA, and health outcomes of populations protected by those laws.

f. Estimated Cost Savings and Costs Arising From Proposed Changes

The Department provides below the basis for its estimated costs and savings due to the proposed changes to specific provisions of the Privacy Rule and invites comments on the Department's assumptions, data, and calculations, as well as any additional considerations that the Department has not identified here. Many of the estimates are based on assumptions formed through OCR's experience in its compliance and enforcement program and accounts from stakeholders received at outreach events. The Department welcomes information or data points from commenters to further refine its estimates and assumptions.

To evaluate the potential benefit and burden of changes to the right of access, the Department calculated a range of estimated total annual numbers of access requests for covered entities, from 1.5 million to 3.3 million. The Department's initial projections were drawn from prior rulemaking and burden estimates; however, based on its experience and comments received on the 2018 RFI, the Department believes an upward adjustment to the estimated number of access requests is needed. The Department developed the estimates herein based on three datasets: the total number of covered entities; the total number of U.S. health care encounters with a health care provider in a year; and the total population of the U.S. The calculated results are as follows: (1) 1.5 million, by estimating that 774,331 covered entities receive an average of two access requests per year; (2) 2.46 million, by estimating that in one year one-tenth of a percent of health care encounters[290] with health care providers results in an access request (.001 X 2.46 billion); and (3) 3.3

---

[290] *See* 2017 "National Healthcare Quality and Disparities Report," Agency for Healthcare Research and Quality (September 2018). AHRQ Pub. No. 18-0033-EF, available at https://www.ahrq.gov/research/findings/nhqrdr/nhqdr17/index.html, reporting 923 million total annual physician office visits, including visits to physicians in health centers, 803 million annual hospital outpatient visits, 117 million annual home health visits, 500 million annual patient days in nursing homes, 213 million annual days in hospitals, and 120 million annual days in hospice.

million, by estimating that one percent of the U.S. population in 2019 makes an access request (.01 X 329,001,648).[291] For purposes of this analysis, the Department selected the mid-point estimate of the number of total annual access requests, 2.46 million.

The Department received widely varying reports from covered entities that commented on the RFI regarding the number of access requests they receive annually and it was unclear whether the numbers included requests that are not part of the right of access, such as disclosures accompanied by a valid authorization, disclosures for purposes of treatment, payment, or health care operations, or other disclosures permitted by the Privacy Rule.[292] In addition, while large covered entities may receive many more than two requests per year, the Department assumes that small doctor's offices, which make up the majority of covered entities, receive very few requests. The Department requests comment on these assumptions.

i. Estimated cost savings and costs from adding a definition of EHR

The Department believes that covered entities would benefit from the certainty offered by its interpretation of the proposed definition of EHR; however, the Department lacks sufficient data to develop a quantifiable estimate. The Department does not anticipate additional costs for covered entities from the proposal to codify in regulation a definition of EHR because the definition itself imposes no requirements, the proposed definition is based on the statutory definition in the HITECH Act which has been in effect for more than a decade, and the proposed definition incorporates existing Privacy Rule definitions, such as direct treatment relationship, that are familiar to regulated entities.

---

[291] "U.S. Census Population Clock," available at https://www.census.gov/popclock/ (visited June 5, 2019). Projections are based on a monthly series of population estimates starting with the April 1, 2010 resident population from the 2010 Census.

[292] For example, the Veterans Health Administration, reported that it receives 1.7 million access requests annually; however, rather than individuals' exercising the right of access, many of these requests likely are for benefit determinations, and may be based on an authorization. A Cincinnati health system reported that two of its hospitals receive 31,102 and 22,000 requests from individuals per year, respectively.

Costs savings and costs related to limiting the scope of the access right to direct a copy of PHI to a third party to PHI in an EHR are addressed elsewhere.

ii. Estimated cost savings from changes to the right to inspect PHI

The Department proposes to add a requirement to the right of access at 45 CFR 164.524 (a)(1) to establish that the right to inspect PHI in a designated record set includes the right to take notes, take photographs, and use other personal resources to capture the information, but that a covered entity is not required to allow an individual to connect a personal device to the covered entity's information systems. The Department assumes that requests to inspect PHI may result in a reduction in requests for covered entities to make copies because individuals may choose to capture the information they need through notetaking, photographing, or other means, and that reviewing the PHI may enable individuals to narrow the scope of any request for copies. This could reduce costs for covered entities; however, the Department lacks sufficient data about the number of inspection requests received by covered entities to make a reasonable estimate of the projected savings. For individuals who prefer to view PHI in person and use their own resources, the proposed changes may offer out-of-pocket cost savings. Individuals who would not want to view their PHI in person would simply not exercise this new right, but would continue to access their PHI as before, thus not incurring any new costs or achieving any new savings. The Department requests data on the number of requests to inspect PHI received by covered entities and the experiences of entities and individuals with how the inspection of PHI affects the number, frequency, or scope of requests for copies.

iii. Costs arising from changes to the right to inspect PHI

Upon consideration of the instances where PHI is readily available at the point of service, such as when viewing x-rays or lab results, the Department anticipates that there may be a much greater demand by individuals for the ability to use one's own device to

capture the images or other PHI as a result of this proposal. The Department anticipates this would result in individuals having better access to their medical information, leading them to potentially make better decisions about their health. The Department does not anticipate that covered entities would incur additional costs for allowing this type of access to "readily available" PHI, but requests comment on this assumption and data on potential costs.

To the extent that covered entities are currently prohibiting individuals from notetaking, photographing, or other ways of capturing PHI using their own devices, they would incur costs involved in changing the existing policy for in-person access. The Department anticipates that a covered entity would need 25 minutes of lawyer time[293] to change its policy and procedure for individuals to inspect their own PHI to include taking notes and photographs or using other resources to capture the PHI (without connecting to the covered entity's system), and may experience costs for adding this policy to its HIPAA training content. This would amount to approximately 322,638 total burden hours for changing related policies and procedures and total costs of approximately $45 million. Revising the related training content would incur average costs for 20 minutes of a training specialist's time[294] for each covered entity, resulting in total increased burden hours of 258,110 and a total cost of approximately $16 million. The Department seeks comments on the extent to which covered entities already have policies permitting individuals to photograph or otherwise capture the PHI, and how changing policies to allow such activities would increase or decrease costs to the entity or individuals. For example, taking a photograph may decrease the time spent by individuals reviewing medical records in the covered entity's office, decrease the number of subsequent calls to the physician for information, or increase adherence to treatment regimens. In particular,

---

[293] *See* Table 4.
[294] *Ibid*.

the Department seeks comments providing any quantifiable projected cost increases or decreases due to the proposed changes, including allowing individuals to photograph PHI that is readily viewable at the point of service in conjunction with a health care appointment.

iv. Estimated cost savings from shortening the access time limits

The Department proposes to shorten the time for covered entities to provide copies of PHI from 30 days (with the possibility of one 30-day extension) to 15 calendar days, or shorter where practicable (with the possibility of one 15 calendar-day extension). The Department lacks sufficient data to quantify any potential cost savings to covered entities resulting from this proposal; however, the receipt of PHI more rapidly from other covered entities may create efficiencies throughout the entire health system and contribute to improved health outcomes and decreased treatment costs. While the Department believes that many covered entities already are providing copies of PHI in far less than 30 days, the increased certainty provided by the proposed regulatory time limit would create additional benefits. For individuals, shortened access times may result in cost savings due to an improved ability to make timely and cost-effective decisions about treatment options and a reduction in duplicative procedures, such as repeat lab tests. For example, an individual who is able to receive a timely copy of a lab result would be able to share it with a consulting provider who otherwise may need to re-order the test, thus saving time and money and enabling timely treatment; or a patient considering surgery who is able to receive a timely copy of PHI would be able to evaluate treatment alternatives with different providers to select which best fits the patient's circumstances. In short, the Department projects that the ability to obtain health information faster may result in cost savings overall. The Department invites comments providing data on projected cost savings from shortening the access time limits from 30 days to 15 calendar days.

v. Costs arising from shortening the access time limits

The Department estimates that at least 50 percent of access requests are already being fulfilled in 15 calendar days or less, taking into account those covered entities (primarily health care providers) subject to state laws with 15-day (or shorter) requirements[295] and other covered entities that fulfill requests in 15 calendar days or less voluntarily.[296] The Department estimates that the burden to covered entities to provide copies of PHI to individuals in half the time than currently permitted would result in increased costs for responding to access requests by 1 minute of a medical records technician's labor which can be attributed to search and retrieval activities that are not included in the allowable labor costs that may be charged to individuals. Based on an estimated 1.46 million annual total access requests for copies of PHI provided to individual at an average increased labor cost of $.75 per request, the Department calculates the total additional annual burden would be approximately $918,400. The Department requests comment on these assumptions.

---

[295] At least eight states require some health care entities to provide copies within 15 days (or a shorter time) by law. Three additional states require access to view records within 10 days or a shorter period. New York State has published guidance that copies should be provided within 14 days, even though it is not a mandatory time limit. Thus, providers in three high-population states are currently subject to expectations of providing access within 15 days or less: New York, California, and Texas. As a percentage of the U.S. population, the 8 states with shorter requirements plus New York, represent over one-third of individuals (using 2018 projections based on the 2016 Census Bureau estimates drawn from 2010 data). There is variability as to how the days are counted within the state laws (*e.g.*, working days vs. calendar days); however, allowing for the proposed 15-day extension, these state requirements are still shorter than the total to be allowed under the proposed HIPAA changes.

[296] Half of the entities commenting on the RFI access question indicated that they are providing access within 15 days or less, including some in states where it is not required. In addition, an ONC report found that, "In 2018, about half of individuals were offered online access to their medical record by a health care provider or insurer. Among these individuals, 58 percent viewed their online medical record at least once within the past year. Nationally, this represents about three in 10 individuals." Patel V & Johnson C. (May 2019). Trends in Individuals' Access and Use of Online Medical Records and Technology for Health Needs: 2017-2018. ONC Data Brief, no.48 Office of the National Coordinator for Health Information Technology: Washington DC, (May 2019), available at https://www.healthit.gov/sites/default/files/page/2019-05/Trends-in-Individuals-Access-Viewing-and-Use-of-Online-Medical-Records-and-Other-Technology-for-Health-Needs-2017-2018.pdf (last accessed June 14, 2019).

vi. Estimated costs and cost savings from addressing the form and format of access

The Department proposes to clarify that a readily producible form and format includes access through an application programming interface (API) using a personal health application. It also proposes that a covered entity must inform any individual to whom it offers to provide a summary in lieu of a copy of PHI that the individual retains the right to obtain a copy of the requested PHI if the individual does not agree to receive such summary. The Department lacks sufficient information to quantify the potential costs or cost savings from these proposals and requests information about how these proposals would affect covered entities, business associates, and individuals.

vii. Cost savings from addressing the individual access right to direct copies of PHI to third parties

The Department proposes to limit the access right to direct a copy of PHI to a third party to only electronic copies of PHI in an EHR. The Department proposes to implement this proposal by adding an optional element to the Notice of Privacy Practices and changing the allowable fees for transmitting such copies—thus, most of the estimated costs and cost savings for those changes are discussed as cost transfers in separate sections on those topics. However, the Department recognizes that covered entities may incur some labor costs for requests by individuals under the right of access to direct electronic copies of ePHI to a third party and estimates that costs may increase for 25 percent of the estimated annual 615,000 such requests (153,750) in the amount of 2 minutes of labor at the hourly wage of a medical records technician ($44.80) or $1.49 per request that cannot be charged to the individual as an allowable fee for copies.

The Department also assumes that many covered entities correctly interpret the current HIPAA right to direct the transmission of electronic copies of PHI in an EHR to a third party to apply to individuals' requests to direct the transmission of such ePHI to another provider or to their health plan. With respect to such requests, the Department

assumes that many covered health care providers and health plans are already disclosing PHI to other providers and plans in a timely manner, which in most instances would be far less than 30 days. The Department further expects that providers using HIEs and certified EHR technology (CEHRT) are disclosing ePHI to other providers in much less than 15 calendar days, as indicated by comments the Department received in response to the RFI. Thus, the Department projects that the costs for complying with the proposed changes for sending electronic copies of PHI in an EHR to health care providers and health plans in no more than 15 calendar days would be limited to a small percentage of covered entities and that those costs would mostly be attributable to changes in 45 CFR 164.524(c)(3), as described in the section above. However, in recognition that covered entities are unlikely to recoup costs for requests by individuals under the right of access to direct electronic copies of ePHI to health plans and health care providers, the Department estimates that costs may increase for 25 percent of the estimated annual 615,000 of such requests (153,750) in the amount of 4 minutes of labor at the hourly wage of a medical records technician ($44.80) or $2.99 per request. This is greater than the uncompensated burden estimate for copies sent to other third parties because the Department understands that health care providers and health plans may not routinely charge any fees for disclosures to other covered entities.

Additionally, the Department proposes, at 45 CFR 164.524(d)(7), to require that a covered health care provider or health plan must submit a request for an electronic copy of PHI in an EHR from another health care provider, to be directed to the requesting covered entity (*i.e.,* the third party recipient), when the request is clear, conspicuous, and specific, which may be orally or in writing (including an electronically executed request). The Department proposes to require that the covered health care provider or health plan must submit the access request as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and information needed to make the request. A health

care provider that receives the access request would be required to provide the electronic copy requested under this section as soon as practicable but no later than 15 calendar days upon receipt of an individual's request that is clear, conspicuous, and specific. The Department considers that a signed, written request and use of a personal health application are both examples of means that an individuals may use that meet the condition that the request be clear, conspicuous, and specific, and that a signature may be provided in electronic form.

Based on comments on the 2018 RFI, in many instances covered entities are already requesting copies of PHI from other health care providers within 30 days or less of communicating with an individual who requests such information to be added to his or her health record. The disclosure of PHI to the covered entity that submitted the request is permitted without an individual's authorization for purposes of treatment, payment, and certain health care operations, as applicable, and required under the current right of access when an individual submits a written request.[297] The Department anticipates that with the clear and certain path provided by this proposal to obtain ePHI from other covered health care providers (who are required to respond), covered entities may experience savings from spending less time attempting to obtain electronic copies of PHI in an EHR from other covered health care providers based on an individual's request. The Department has not quantified these cost savings, but invites comments on any projected savings to covered entities and/or individuals from this regulatory clarification.

viii. Costs arising from changes to the individual access right to direct copies of PHI to third parties

The Department anticipates that once individuals and third party recipients learn about the changes (*i.e.,* limiting the right to only directing electronic copies of PHI in an EHR) they likely would shift to submitting access requests *and* authorizations when

[297] Following the court's ruling in *Ciox v. Azar*, the Department is limiting the right to direct the transmission of PHI to third parties to requests for electronic copies of PHI in an EHR.

requesting that a complete medical record be sent to a third party. Although covered entities may bear some initial costs while the public is adjusting to the new requirements, they would benefit financially from the increased number of copies for which they can charge a less restricted fee (an effect categorized as a "transfer" from the society-wide perspective reflected in this regulatory impact analysis). The Department estimates that covered entities may incur some one-time costs for changing their policies and procedures and revising their training program for employees who handle access requests, as well as initial implementation costs for adjusting to the revised policies and procedures. Specifically, the Department estimates that covered entities will incur an increase in burden hours for 30 minutes of a lawyer's time to revise policies and procedures related to the changes to this part of the right of access. Additionally, the Department estimates that covered entities will incur an increase in labor expenses for 20 minutes of a training specialist's time to incorporate the newly revised policies and procedures into the covered entity's existing HIPAA training program.

As stated in the discussion of changes to the proposed access fees, the Department estimates a total of 2.46 million access requests per year and that half of these are for the individual to obtain his or her own records, one-fourth (615,000) are to direct the transmission of records to a health care provider or health plan, and the remaining one-fourth (615,000) are to direct the transmission of records to a third party. Of the 615,000 estimated requests to direct the transmission of PHI to a third party other than a health care provider or health plan, the Department estimates that covered entities would not fulfill half (307,500) on the basis that the request is for non-EHR copies of PHI (*i.e.,* are requests that do not fall within the right of access).

The cost savings associated with these changes are discussed separately as cost transfers in the sections on the proposed changes to access fees.

The Department estimates that covered entities, primarily providers, would incur some costs from the proposed new requirement to submit requests for access on behalf of individuals who are seeking to direct the transmission of electronic copies of PHI in an EHR from another health care provider ("Discloser") to the requesting entity ("Requester-Recipient"). The Department estimates that the proposed requirement would increase costs for 15 percent of the 615,000 annual requests to direct copies of ePHI to health plans and providers (92,250) by 3.5 minutes per request at the adjusted labor rate of a medical assistant ($34.34, see Table 4), for a total of 5,381 burden hours at a total annual cost of $184,792. These costs are presented in Table 12 as ongoing costs of the proposed rule. The Department does not anticipate that covered entities would incur a significant additional burden from an express inclusion of health care providers and health plans as recipients to whom disclosures are mandated when the individual exercises the right to direct the transmission of electronic copies of PHI in an EHR to a third party. Based on a notable lack of comments or concerns expressed by stakeholders about directing PHI to covered entities as part of the right of access, the Department expects that most covered entities have correctly interpreted the Privacy Rule and included individuals' requests to direct the transmission of ePHI to health care providers and health plans into their access request fulfillment process. The small proportion of covered entities or business associates who are not already fulfilling individuals' access requests to transmit ePHI to health care providers or health plans may experience a small increase in costs resulting from their current noncompliance. The Department estimates that 25 percent of these requests (153,750 total) would result in transmitting an electronic copy of ePHI via a non-internet based means (*e.g.*, mailing a copy of ePHI stored on electronic media to a health plan or health care provider), at a labor cost of 4 minutes of a medical records technician's adjusted hourly rate of $44.80, for a total annual cost of $459,200.

Overall, the Department believes that, for covered health care providers and health plans, any costs to fulfill requests made under this proposal would be counterbalanced by the increased responsiveness from other covered entities that would transmit records to them, when requested, on a timelier basis, which would improve care and contribute to cost reductions.

ix. Estimated cost savings and cost transfers from changes to access fees

The Department proposes to expressly prohibit covered entities from charging fees for access when an individual inspects PHI about the individual in person and for copies of PHI that an individual accesses using an internet-based method.

Expressly permitting individuals to copy and photograph their PHI for free during an in-person inspection may reduce the number and scope of subsequent access requests made by such individuals. In addition, to the extent that covered entities increase the free availability of PHI via an internet-based method, they may experience a decrease in other types of access requests for which costs are incurred. The Department expects that individuals may increasingly choose to initiate and obtain access via an internet-based method, which will result in cost savings to individuals.

Prohibiting covered entities from recouping certain costs for providing electronic copies of PHI, or transmitting an electronic copy of PHI in an EHR to third parties, would increase expenses for these items: electronic media onto which copies of PHI from an EHR are transferred, and actual mailing and shipping costs for electronic copies.[298] At the same time, covered entities' ability to charge fees for directing non-electronic copies of PHI and electronic copies of PHI not in an EHR to third parties based on a valid authorization would reduce unreimbursed costs for covered entities. Of an estimated 2.46

[298] OCR's Breach Portal reflects numerous breaches involving the loss or destruction during transit of mailed electronic media, such as USB drives and CDs, affecting thousands (more) of individuals. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

million annual access requests, the Department assumes that 50 percent (1.23 million) are for individuals to directly access PHI, 25 percent (615,000) direct copies to health care providers or health plans, and the remaining 25 percent (or 615,000) direct copies to other third parties, as indicated in Table 6. Of the 615,000 requests directed to other third parties, assuming an average record size of 200 pages,[299] the Department assumes 100 pages are electronic copies and 100 pages are non-electronic copies (a "hybrid" records request) because it lacks sufficient data to estimate the average length of a record that is requested by an individual. The Department expects that there is considerable variation, ranging from individuals who seek only billing records, those who want only records of a single hospitalization, those who request only lab results or a copy of a single doctor's order, to those who need a complete longitudinal record of all of their medical visits. The Department requests data that would refine its assumptions and estimates about the average size of a request for access.

Table 6. Estimated Number of Annual Access Requests, by Recipient

Recipient of PHI Copies	Number of Access Requests
Individuals	1,230,000
Health Care Providers and/or Health Plans	615,000
Third Parties other than Providers and/or Plans	615,000
Total	2,460,000

Under the Department's proposed changes, covered entities would be disallowed from charging for certain expenses that the Privacy Rule currently allows when providing copies to an individual and when directing an electronic copy of PHI in an EHR to a third party under the right of access. The non-chargeable expenses would be the portion of costs attributable to emailing, mailing, or shipping the electronic copies and the costs of

[299] *See* Lye CT, Forman HP, Gao R, et al. "Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records." JAMA Netw Open. 2018;1(6):e183014, available at https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2705850, citing a study evaluating the state of medical records request processes in US hospitals in which a hypothetical assumption of 200 pages per request was used. The Department requests comment and evidence regarding the actual lengths of medical records.

electronic media requested by individuals. Labor costs for copying or transferring EHR records to another electronic format (such as a PDF) or onto electronic media (e.g., CDs, USB drives) would continue to be allowed as part of a reasonable, cost-based access fee. Table 7 indicates the allowable and non-allowable expense items for directing copies of PHI to third parties under the current right of access and as proposed.

Table 7. Allowable and Non-allowable Elements of Expenses Incurred for Transmitting Copies of Electronic PHI in an EHR to a Third Party

Cost Elements	**Expense Item Currently Allowed**	**Expense Allowed under Proposed Rule**
Labor for making requested copies	Yes	Yes
Postage and shipping	Yes	No
Electronic media	Yes	No
Copying supplies	Yes	No
Costs of searching, retrieving, collating or preparing the PHI for copying	No	No
Costs of EHR and other electronic information systems	No	No

The Department has not estimated postage or shipping costs in earlier Privacy Rule rulemaking because the rule permitted actual costs for those expenses to be passed on to the individual making the request for copies of PHI. To estimate how the proposed changes would affect covered entities, the Department has estimated that a 100-page paper record (one pound of material) can be shipped via U.S. Mail for $7.50 and a CD or USB drive can be shipped for $3.00.

To readily compare the potential burden or burden reduction from various types of requests to direct copies of PHI to third parties, the Department presents its estimates in the charts below and provides detailed explanations of the included cost items for each calculation under the current rule, state law, and the proposed rule in the paragraphs that follow. State law remains a relevant consideration in two ways. First, to the extent that state law limits on fees for copies of medical records for individuals are lower than the limits in the Privacy Rule, the state law applies. For instance, some states require a free

copy for individuals who are indigent or who are applying for public benefits. Second, for copies of PHI provided in response to a valid authorization, the Privacy Rule limits the allowable fee to "a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law"[300] (absent an authorization including a statement that the disclosure will result in remuneration to the covered entity). "Other law" includes, among other sources of law, state medical records laws addressing allowable fees for copies.

Table 8. Estimated Fees for Copying and Sending a 200-page Hybrid Record (100 electronic pages and 100 non-electronic pages) to a Third Party

Estimated Allowable Fees for a 200-page Hybrid Record under the Current Rule	**Estimated Allowable Fees for a 200-page Hybrid Record under State Law**
$25.23	$133.50

Table 9. Estimated Fees for Copying and Sending a 100-page Record to a Third Party

Estimated Allowable Fees for 100 Non-electronic Pages under State Law	**Estimated Allowable Fees for 100 Electronic Pages under State Law**	**Estimated Allowable Fees for 100 Non-electronic Pages under the Current Rule**	**Estimated Allowable Fees for 100 Electronic Pages under the Current Rule**	**Estimated Allowable Fees for 100 Electronic Pages under the Proposed Rule**
$88.16	$76.70	$16.74	$8.49	$1.41

Allowable Access Fees under Current Rule to Send a Copy to a Third Party

The Department's estimate of allowable costs that may be charged for a 200-page hybrid record directed to a third party under the current right of access is approximately $14.73 (estimating $3.73 for 5 minutes of labor[301] and $11 for supplies[302]) per request, plus estimated postage and shipping of $10.50 or $25.23 total. See Table 8. This

[300] 45 CFR 164.502(a)(5)(ii)(B)(*2*)(*viii*).
[301] *See* Table 4, median adjusted wage rate for medical records technician of $44.80.
[302] The costs of supplies includes $7 for paper, toner, etc., and $4 for electronic media such as a USB drive.

represents an overall increase in labor of 2 minutes above the Department's prior burden estimates of 3 minutes for all access requests. The updated estimate allows 3 minutes of labor for the non-electronic copies and 2 minutes of labor for electronic copies, resulting in total allowable labor costs of 5 minutes for a hybrid record. The updated estimated allowable fee under the current rule for only the electronic portion of the request (100 pages in electronic format) is $5.49 ($1.49 for 2 minutes of labor and $4 for electronic media) plus postage of $3.00 or $8.49 total per request. See column 4 of Table 9. The estimated allowable fee under the current rule for only non-electronic copies (100 pages) is $9.24 (estimating $2.24 for 3 minutes of labor and $7 for supplies), plus postage of $7.50 or $16.74 total. See column 3 of Table 9.

In addition to the costs that may be charged as fees for providing copies, the Department estimates a previously unacknowledged burden of 2 minutes of labor per request that is not allowed to be charged to the individual or the third party recipient of the ePHI for copies that are sent via a non-internet method (e.g. on electronic media that is mailed). The Department assumes that none of the costs for electronic copies of ePHI sent to third parties that are health plans and health care providers through a non-internet method would be recouped as fees charged to individuals or the covered entity recipients. In recognition of this burden, the Department also estimates that all of the labor for sending electronic copies of ePHI to third parties that are health plans and health care providers is uncompensated, resulting in a previously unacknowledged uncompensated burden of 4 minutes of labor per request for electronic copies of ePHI sent to third parties that are health plans and health care providers through a non-internet method at the direction of the individual. The Department acknowledges the lack of data on actual labor associated with sending electronic copies of ePHI because some copies will be sent on electronic media and some by internet. The Department estimates no labor for sending copies via an internet-based method. These adjusted estimates are included in the

uncertainty analysis in subsection m. and the burden estimates in section G., Paperwork Reduction Act.

Allowable Fees under State Law for Sending Copies of Medical Records to a Third Party

The Department estimates that the average charge allowed by state law for a 200-page hybrid record directed to a third party is $123 per request (including a handling or administrative fee[303] not allowed by the Privacy Rule), plus postage and shipping of approximately $10.50. This would result in an estimated total of $133.50 in state-allowed fees for a 200-page hybrid request. See Table 8. The estimated state-allowed fee for 100 electronic pages that are not contained in an EHR is $73.70 plus $3 postage for sending a USB drive or $76.70 total. See column 2 of Table 9. The estimated state-allowed charge for 100 non-electronic pages is $80.66 plus $7.50 for postage or $88.16 total. See column 1 of Table 9.

Allowable Fees under Proposed Rule for Sending an Electronic Copy of PHI in an EHR to a Third Party

The estimated average allowable fee under the proposed rule (100 pages in electronic format) is $1.49 per request (estimating 2 minutes for labor).

In developing its estimated costs and cost benefits the Department employed several methods to arrive at a range of costs and cost benefits and average estimated costs and cost benefits for the proposed adjustments to the allowable access fees.

Methodology 1

The Department applied its estimated fees to a 200-page hybrid record and compared the costs under the proposed changes to a baseline of $25.23 in estimated allowable costs under the current right of access. See Table 8. The resulting estimated cost savings for three different types of requests are as follows.

---

[303] In states that have one search fee for electronic copies and another search fee for paper copies, the Department assumes that a covered entity would only charge the individual one administrative fee for a hybrid request.

When a request is entirely for copying and sending copies that are not contained in an EHR (100 non-electronic pages and 100 electronic pages) to a third party

Under the proposed rule, a covered entity could charge the state law rate ($133.50) or $108.27 more for the request than allowed under the current rule.[304] For an estimated annual total of 615,000 requests directed to a third party, this type of request would generate an estimated cost savings for covered entities of $66,586,050.

When a request is for 100 electronic pages that are not in an EHR and 100 electronic pages that are in an EHR

Under the proposed rule, a covered entity could charge the state law rate for copying and sending 100 electronic pages not in an EHR ($76.70) plus the allowable labor for copying the 100 EHR pages ($1.49) for a total of $78.19 or $52.96 more per request than allowed under the current rule.[305] For an estimated annual total of 615,000 requests directed to a third party, this type of request would generate an estimated cost savings for covered entities of $32,570,400.

When a request is for 100 non-electronic pages and 100 electronic pages that are in an EHR

Under the proposed rule, a covered entity could charge the state law rate for copying and sending 100 non-electronic pages ($88.16) based on a valid authorization, plus the allowable labor for copying the 100 EHR pages ($1.49) under the right of access, for a total of $89.65 or $64.42 more per request than allowed under the current rule.[306] For an estimated annual total of 615,000 requests directed to a third party, this type of request would generate an estimated cost savings for covered entities of $39,618,300.

To summarize, under the options presented above, the Department estimates that the cost savings of the proposed changes to the access right to direct an electronic copy of

---

[304] $133.50 minus $25.23.
[305] $78.19 minus $25.23.
[306] $89.65 minus $25.23.

PHI in an EHR to a third party and allowable fees for directing copies of PHI to third parties, would range from $53 to $108 per request.

Methodology 2

The Department also applied a second method for estimating the potential costs and cost savings of the proposed fee changes. Under the second approach, the Department assumed that half of the 615,000 annual requests to direct copies of PHI to a third party would be for electronic copies of PHI in an EHR (307,500) and that half would no longer fall within the right of access (307,500), but then would be disclosed with a valid authorization. Costs for covered entities would increase for the estimated 307,500 requests that are accepted (for electronic copies of PHI in an EHR) by an estimated $7 per request in supplies and postage they would no longer be able to recoup in fees, for a total estimate of $2,152,500 annually.[307] Cost savings for covered entities would accrue for the estimated 307,500 requests that are no longer within the right of access (for non-electronic copies or electronic copies not in an EHR) by an estimated $108.27 for a total estimate of $33,293,025[308] annually. This estimation method would result in an estimated net cost savings for covered entities of $31,140,525 annually ($33,293,025 minus $2,152,500).[309]

Summary Results of the Department's Estimated Costs and Cost Savings for Proposed Fee Adjustments

Under the proposed changes, a covered entity would be allowed to charge less per request to transmit an electronic copy of PHI to a third party under the right of access and significantly more per request to send non-electronic copies or electronic copies not maintained in an EHR to a third party with a valid authorization, as compared to what is allowed under the current right of access. Under the several methods for calculating estimated fees for copies of PHI the Department estimates total annual cost savings for

[307] $7 multiplied by 307,500 requests.
[308] $108.27 multiplied by 307,500 requests.
[309] Estimated net costs subtracted from estimated net savings.

covered entities ranging from $31 million to $67 million, or an average of $43 million. However, the Department estimates that all of these cost savings on the part of covered entities would be transferred to individuals and/or their third party designees as costs. The Department estimates that 50 percent of these costs savings would be transferred as an additional cost imposed on individuals and the other 50 percent would be transferred to the third parties to whom the PHI is directed. For each of the estimated 615,000 requests that would have been made under the current rule to direct the transmission of copies of PHI to a third party under the right of access the allowable fee for copies would increase by an estimated average of $70 ($43 million in estimated annual cost savings divided by 615,000 requests).

The Department seeks comments on these estimates, averages, and assumptions underlying its analysis and invites comments on the number and type of access requests received by covered entities, costs incurred, and fees charged.

x. Costs arising from changes to access fees

The Department anticipates that the burden on covered entities for drafting or updating their access fee schedules would include the one-time costs for lawyer to review the new HIPAA provisions and evaluate the entity's fee structure based on changes to allowable access fees. This would include lawyer time at an adjusted mean hourly rate of $139.72. For each covered entity, the Department estimates an average of three hours for a lawyer to make policy and procedure revisions related to all the proposed changes to the right of access, including allowable fees. In total, the Department estimates 2,322,993 burden hours, for approximately $325 million in lawyers' costs related to the proposed changes to the right of access.

Covered entities also would need to add new access fee policies and procedures to their HIPAA training content. In its estimates, the Department includes two hours and thirty minutes of a training specialist's time for each covered entity to revise the training

content for all of the proposed changes to the right of access, including fees and responding to requests for fee estimates, at an adjusted mean hourly rate of $63.12. The Department believes this estimate is reasonable, but welcomes comment and data to further inform its assumption. In total, the Department estimates 1,935,828 burden hours for all of the revisions to training content related to the right of access and costs of approximately $122 million. The Department assumes, for all of the proposed changes, that entities would incorporate the updated training content into their ongoing HIPAA training program, and that for most workforce members there would be no additional training costs for the time spent in HIPAA training. However, for medical records technicians, the Department has estimated an average seven minute increase in the time for spent in training on the proposed right of access changes in the first year of implementation, for a total estimate of 90,339 burden hours at a total estimated cost of $4 million.

Free Access for Inspecting PHI In-Person: To the extent that covered entities are charging individuals for the copies individuals make with their own devices or resources, the covered entities would incur some loss of revenue; however, the Department anticipates that any loss would be minimal and that covered entities do not view this as a significant source of revenue, if any do charge a fee to inspect PHI in person. The Department seeks comments on the number of requests covered entities receive to inspect PHI in person and on the number of covered entities that charge fees for or prohibit individuals from making copies with their own devices or taking notes of their own PHI, and if so, the amount of fees charged for such activities.

Free Internet-Based Access: Because covered entities do not incur additional costs for labor, supplies, or postage for this method of providing access and because it only applies to covered entities that choose to use this method, the Department does not anticipate an increased burden for expressly requiring entities to provide such access for

free. The Privacy Rule requires a covered entity to provide an individual with access to existing PHI maintained electronically in the electronic form and format requested, if it is readily producible, but neither the current access standard nor this proposed change would require covered entities to create a patient portal or other internet-based access method. In practice, such internet-based access is "readily producible" for most covered entities that use EHRs because the Office of the National Coordinator of Health IT requires an EHR to implement API technology in order to be certified.[310]

Reducing the Expenses that can be Included in Calculated Access Fees for Providing Individuals with Copies of PHI in an EHR on Electronic Media: The Department proposes to disallow covered entities from charging individuals for the costs of electronic media and postage when providing access by mailing copies of PHI in an EHR on electronic media. The Department estimates that the costs of electronic media may range from $1 for a CD to $4 for a USB drive and the postage may range from $1 to $3, resulting in a range of estimated increased costs of $2 to $7 per request of this type or an average estimated increase of $4.50. The Department estimates that half of the 2.46 million total estimated annual access requests (or 1.23 million) would be made by individuals to obtain copies of PHI for themselves, and that half of those requests would be for non-electronic copies of PHI (or 615,000), one-fourth would be for internet-based access (or 307,500), and one-fourth would be subject to the proposed fee limitations for sending copies on electronic media (or 307,500). Thus, the Departments estimates a total cost incurred by covered entities of $1,383,750 due to this proposal. At the same time, these are costs that would have been borne by individuals, and thus may be considered a cost transfer from individuals to covered entities as reflected in Table 17.

---

[310] In the Cures Act Final Rule, ONC has adopted a new secure, standards-based API certification criterion in § 170.315(g)(10) to implement the 21st Century Cures Act's requirement that developers of certified health IT publish APIs that can be used "without special effort." See https://www.healthit.gov/cures/sites/default/files/cures/2020-03/APICertificationCriterion.pdf.

Narrowing the Scope of Requests to Direct PHI to Third Parties that are Subject to the Access Fee Limits: Allowing covered entities to charge higher access fees than currently permitted when directing non-electronic copies of PHI or electronic copies of PHI not in an EHR to third parties, based on a valid authorization rather than an access request, would reduce their burden for directing copies of PHI to a third party, and shift the costs to the individuals or to the third parties to whom the responses to such requests are directed. Because individuals still may request copies of records to be sent to the individuals themselves at the lower rate currently allowed under the Privacy Rule, this proposed change would not impede individuals from receiving their own PHI; however, it may cause some individuals to bear the burden of transmitting non-EHR ePHI to some third parties to avoid the higher fees, expend higher amounts for using a valid authorization to request that the PHI be disclosed to a third party, or avoid making some requests to direct copies of non-electronic PHI to a third party. The Department has insufficient information to quantify the potential increased burden on individuals for these options and welcomes information and comment on these potential changes to individuals' expenditures of time and money.

xi. Estimated cost savings from requiring covered entities to provide access and authorization fee information

The Department proposes, in a new subsection 525 to 45 CFR 164, to require a covered entity to provide advance notice to individuals of the fees the entity charges for providing copies of PHI. Specifically, the Department proposes to require a covered entity to (i) post a fee schedule for standard or common types of access requests, including all types of access which are free, on the entity's website (if it has one), and make the fee schedule available to individuals; (ii) provide, upon request, an individualized estimate of the approximate fee that may be charged for the requested copy of PHI, including any associated fees that may impact the form, format, and manner in which the individual requests or agrees to receive a copy of PHI; and (iii) upon request, provide an individual

with an itemized list of charges for labor, supplies, and postage, if applicable, that constitute the total access fee charged. Finally, the Department proposes that such requests not automatically extend the deadline by which a covered entity is required to respond to an access request.

The Department thinks it is likely that covered entities that provide fee estimates for access and disclosures pursuant to a valid authorization would find that such action results in a narrower scope for some requests than would exist without the changes, improved collection rates for access fees, and reduced time needed for workforce members to resolve access payment disputes and complaints. Thus, the Department believes that the benefits of changing covered entities' access procedures in a way that incentivizes individuals to make more targeted access requests and informs them of fees in advance would counterbalance the burdens on covered entities. However the Department has no data with which to estimate the reduction in burden and welcomes comments on this change, including covered entities' experiences with the collection of access and authorization fees, the factors affecting the scope of individuals' requests for copies, and the costs to covered entities for handling fee disputes.

xii. Costs arising from requiring covered entities to provide access and authorization fee information

Posting the fee schedule online or otherwise making the access and authorization fee schedule available: In calculating covered entities' burdens for posting a notice of access and authorization fees, the Department presumes that a number of entities charge no fees for copies provided under the access right[311] or for copies sent to other covered

[311] OCR's 2016 Access Guidance encourages covered entities to provide individuals with a free copy. At least one state, Kentucky, requires certain health care entities to provide an initial free copy, KRS section 422.317(1). Several states require a free copy for persons who are indigent and/or applying for public benefits. *See*, *e.g.,* California, CA Health and Safety Code § 123110(d), (e), Connecticut, Conn. General Statutes § 20-7c(d), Massachusetts, MGLA Ch. 111 § 70 and MGLA Ch. 112 § 12CC, Michigan, Mich. Comp. Laws 333.26269, sec. 9(4), Nebraska, Neb. Rev. Stat § 71-8405, Nevada, Nev. Rev. Stat. § 629.061(5), Ohio, Ohio Revised Code, section

entities. These entities would have no burden for complying with the new notice provision.

The Department seeks comments on the number of covered entities that charge fees only for copies provided based on a valid authorization, no fees for fulfilling requests pursuant to the right of access.

The Department assumes that all entities that charge for providing copies of PHI already have some type of standard fee structure. The Department also presumes that some covered entities have already posted an online access and authorization fee schedule consistent with existing guidance recommending this practice, although this is not required by the Privacy Rule, and have been making it available to individuals. For those covered entities that have not yet posted the fee schedule online, the costs of doing so should be minimal because this requirement only applies to entities that have a website. The Department anticipates that posting an online notice of access and authorization fees would require the costs of reviewing, formatting, and posting one document. Making the notice available may include, for example, having copies available in the office where individuals make access and authorization requests or emailing it to individuals upon request.

Because the proposed change requires covered entities to make the access and authorization fee schedule available at the point of service and upon request (in addition to posting online when a website is utilized), it may be least burdensome for entities to add the fee schedule to their access and authorization request forms (although the Department does not propose to require this, or to require the use of a standard form for access requests), resulting in no additional labor costs for distribution. Further, for covered entities that already have a fee schedule, the proposed change would only require revisions

---

3701.741(C), Rhode Island, RI § 23-17-19.1(16), Tennessee, TCA § 68-11-304(a)(2)(B), Texas, Texas Code, Health & Safety § 161.202 , Vermont, 18 V.S.A. § 9419, and West Virginia, WV Code § 16-29-2(g).

to an existing document, resulting in no additional costs for paper. The Department estimates the potential burden on all covered entities (774,331) as the cost of 10 minutes of a web developer's time at a rate reported in Table 4, for a total labor cost of approximately $10 million. Although the Department assumes that 35 percent of covered entities have already posted an access and authorization fee schedule available, as discussed in the baseline assumptions following Table 4, it recognizes that all covered entities may need to post an updated fee schedule and accounts for this in its estimates. In addition, the Department estimates that all covered entities will incur first-year and ongoing capital costs for making the fee schedule available at a cost of $0.10 for paper and printing or a total of $232,299. This assumes each covered entity prints an average of three copies of the fee schedule as a separate document. We anticipate that covered entities will provide the fee estimate in a variety of ways, not all of which will incur additional costs, such as including the fee schedule on the access and/or authorization form and providing it electronically. The Department seeks comments and data on its assumptions, and on the number of covered entities that require individuals to use an access request form and how many currently make an access and/or authorization fee schedule available to individuals, either online or through other means, such as email or telephonically.

Providing the individual, upon request, with an individualized estimated access and/or authorization fee: The proposed changes would require billing information to be provided to individuals in advance as an estimate, upon request. Providing advance notice of the fees for providing the requested PHI would require a statement of charges pertinent to the individual's request (*e.g.,* giving some estimate of the number of pages if a per page fee is involved, identifying whether records are in paper or electronic form, and giving an estimate of the individual's access and/or authorization fees). The Department assumes that three percent of 2.46 million total access requests, or 73,800, would result in a request

for a fee estimate at a cost per request of three minutes of a medical records technician's time, at the rate reported in Table 4, for a total new labor cost of approximately $165,312. The Department assumes that most of the requested fee estimates will be provided electronically or orally, and that only a small proportion will result in mailing a paper copy of the estimate to the individual. Thus, the Department estimates that 15 percent of 73,800 requests for an access fee estimate (or 11,070) would need to be printed and mailed, at a total estimated capital expense of $7,638 at a cost of $0.69 per estimate. The Department anticipates that many covered entities are already providing access fee estimates, as recommended in OCR's 2016 Access Guidance; however, the Department seeks comments on the number of covered entities that provide estimates of access and authorization fees.

Providing an itemized list of allowable access and authorization charges for labor, copying, and postage: The Department assumes that: (a) many entities are already providing this information when requested by an individual as recommended in OCR's existing guidance, although it is not required by the Privacy Rule; and (b) a small proportion of individuals who request copies of PHI will make such requests. Limiting this requirement to instances when the cost details are requested would further minimize the burden of this proposed change. The Department estimates the potential labor costs as one minute of a medical records technician's time at the hourly rate of $44.80 for an estimated 24,600 annual requests for an itemized list of access charges, or a total of 410 burden hours and $18,368 in total costs. The Department estimates that covered entities would incur capital costs for printing one sheet of paper at a cost of $0.10 per request for an itemized list of charges and no additional postage because the itemized list of charges would be included with the copies of PHI sent to the individual, for a total cost of $2,460 annually. The Department seeks comments on the number (and relative volume) of

requests for the specific details of allowable charges for copies of PHI that covered entities receive from individuals or their personal representatives.

xiii. Estimated cost savings from changes to the verification requirements

The Department proposes to add a new paragraph (v) to 45 CFR 164.514(h)(1), which would state that a covered entity may not impose identity verification requirements on an individual that would serve as a barrier to or unreasonably delay the individual from exercising an individual right under HIPAA when a less burdensome measure is practicable for the covered entity. Individuals would accrue cost savings by reductions in expenses for obtaining notarized documents, traveling in person to request access, paying verification fees, or meeting other unreasonable verification practices. Because the Department assumes that most entities do not impose such barriers to individual access, the Department anticipates that the total cost savings will be modest, but they may be significant for any particular affected individual. The Department invites comment and examples of the extent to which covered entities impose measures that some may view as unreasonable and create costs for individuals when seeking to request access to PHI.

xiv. Costs arising from changes to the verifications requirements

The Department, based on OCR's experience with HIPAA enforcement and recommendations in guidance, anticipates that most entities already are avoiding unreasonable verification measures. However, OCR has received some complaints and anecdotal reports that some entities are forcing individuals to engage in these burdensome practices, such as obtaining a notarized signature or appearing in-person to make an access request. The Department estimates that 5% of covered entities (38,717), and any business associates that fulfill requests for access on their behalf, would need to modify their verification policies and forms and update related HIPAA workforce training content. The Department estimates that these covered entities would incur costs for 30 minutes of a

lawyer's time (or $69.86) to revise these policies and procedures, and costs for 10 minutes of a training specialist's time (or $10.52) to update the HIPAA training content on this provision for a total of approximately $80.38 per covered entity. As the Department does not have data upon which to refine its assumptions and estimates, the Department invites comments in this regard for future consideration, as well as on any costs associated with implementing the proposed changes.

xv. Estimated cost savings from adding an exception to the minimum necessary standard for care coordination and case management for individuals

The Department proposes to add, at 45 CFR 164.502(b)(2), an express exception to the minimum necessary standard for disclosures to or requests by a covered health care provider for individual-level care coordination and case management activities that constitute treatment or health care operations. The Department expects to achieve significant cost savings from this proposal. The Privacy Rule generally requires a covered entity to make reasonable efforts to limit use of, disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose and to make an assessment of what PHI is reasonably necessary for a particular purpose. These requirements apply to all requests for, and disclosures of PHI for payment and health care operations purposes, including care coordination and case management. In some circumstances, a covered entity may, but is not required to, rely on representations by a requesting covered entity that the amount of PHI requested is the minimum necessary. In such cases, the disclosing covered entity remains responsible for determining when such reliance is reasonable under the circumstances.[312]

The Department lacks quantifiable data on the number of such determinations that occur in every covered entity and requests comment on the number of determinations, the type and level of workforce members making the determinations, and how such

[312] *See* 45 CFR 164.514(d)(3)(iii).

determinations are made consistent with an entity's minimum necessary policies and procedures. The Department assumes that any covered entity makes numerous minimum necessary determinations daily as to whether a request or disclosure related to patient information can be made consistent with the covered entity's policies and procedures. The Department estimates that each covered health care provider and health plan would save 25 minutes per month in time currently spent considering requests for care coordination and case management disclosures, to determine whether the information requested could be provided consistent with its internal minimum necessary policies, and to follow the requisite procedure for doing so.

The Department assumes that this proposal would relieve covered entities from the requirement to make determinations about the minimum information necessary to accomplish the purpose of a disclosure (or whether it is reasonable to rely on the requestor's representation that it is requesting the minimum necessary) when the request is from, or the disclosure is made to, a covered health care provider or health plan for individual-level care coordination and case management activities. In the 2000 Privacy Rule, the Department estimated that the minimum necessary requirement was one of the two largest cost items of the Privacy Rule, imposing a likely burden of $926.2 million in the first year and $536.7 million annually in subsequent years.[313] Specifically, the Department estimated that on "an annual ongoing basis (after the first year), hospitals will require 320 hours, health plans 100 hours, and nonhospital providers 8 hours to comply with this provision."

The Department has attempted to refine its estimates related to minimum necessary by reviewing publically available materials from the Agency for Healthcare Research and Quality Medical Expenditure Panel Survey,[314] and the Centers for Disease Control and

---

[313] 65 FR 82461, 82760, 82767 (December 28, 2000).
[314] *Available* at https://www.meps.ahrq.gov/mepsweb/.

Prevention National Health Interview Survey[315] for additional data but was unable to locate recent responsive information. Most recently, commenters on the 2018 RFI described how the minimum necessary standard had a negative impact on the ability of a covered entity to promote care coordination and case management. For example, one commenter noted that accountable care organizations rely on care coordination and case management to improve quality and costs, but believed that the current rule hampered the ability to receive complete data sets to conduct these activities.[316] Another commenter noted that minimum necessary requirements, when applied to population-based services and wellness activities, "hindered" the advancement of population-based analytics,[317] while yet another commenter described it having a "detrimental impact" on the ability of clinical registries to contribute expertise and research toward value-based care models.[318] None of the commenters estimated the amount of time it takes a covered entity to make a minimum necessary determination. The Department does not intend to more heavily weight the comments cited herein above other comments submitted in response to questions about minimum necessary determinations in the 2018 RFI. The Department does intend to illustrate that some covered entities continue to view minimum necessary determinations as burdensome and to the extent a new exception for care coordination and case management would relieve this burden, should be quantified as a cost savings. The Department requests comment on this approach.

The public comments on the 2018 RFI make clear that there is a burden associated with making minimum necessary determinations with respect to uses and disclosures of PHI for care coordination and case management, and therefore savings will be associated with relief from the burden. The Department's proposed estimates are informed first by

---

[315] *Available* at https://www.cdc.gov/nchs/nhis/index.htm.
[316] Comment No. HHS-OCR-2018-0028-0601.
[317] Comment No. HHS-OCR-2018-0028-0998.
[318] Comment No. HHS-OCR-2018-0028-0990.

the cost burdens the Department first identified in the 2000 Privacy Rule and for which the Department has not received public input to the contrary. The proposed estimates also are informed by the understanding that a covered entity is able to rely on the representations of certain requestors about the minimum necessary information to accomplish the purpose of a use or disclosure, and that minimum necessary determinations are a component of every covered entity's workflow. For purposes of calculating burden, the Department assumes that minimum necessary determinations generally are made outside of a patient encounter by workforce members at a registered nurse level, although the Department believes workforce members at a variety of levels in an organization may apply a covered entity's minimum necessary policies and procedures to routine disclosures of PHI. Recognizing the variability among the types and complexity of requests for PHI received by various types of covered health care providers and health plans, and that some record requests are not subject to the minimum necessary standard (*e.g.*, requests from treating providers or requests accompanied by authorizations from individuals), the Department has calculated a range of estimates for cost savings resulting from the combined effects of the proposed regulatory modifications to the definition of health care operations, and to the minimum necessary standard for disclosures for care coordination. At the low end, the Department estimates a cost savings of 1 hour of labor annually per covered entity at the adjusted mean hourly rate of a health services manager ($110.74, including benefits) for a total reduction of 774,331 burden hours and an annual cost savings of $85,749,415. At the high end, the Department estimates costs savings of 7 hours of labor for a total annual reduction of 5,420,317 burden hours and $600,245,905 in cost savings.

The Department proposes to adopt the mid-range estimate of burden reduction, which is 4 hours per covered entity per year for an annual reduced total of 3,097,324 burden hours and $342,997,660 in total annual projected cost savings. The estimate assumes that covered entities already are making minimum necessary determinations as

part of normal workflow. These proposals do not introduce a new process into that workflow, but likely will tilt the scale in favor of disclosure rather than non-disclosure. The difference in the low and high end of the range is based on the Department's assumption that there is a wide range in the level of complexity of minimum necessary determinations that each covered entity makes for routine and non-routine requests for, or disclosures of, PHI. Using the mid-range estimate, the Department estimates that under the current rule covered entities spend, on average, one and a half hours of workforce member time per month evaluating uses and disclosures to comply with the minimum necessary requirement, or 18 hours annually. The Department estimates that the cost savings from its proposed changes with respect to uses and disclosures in connection with care coordination and case management would equal 25 minutes of burden reduction for each covered entity for a total annual burden reduction of 4 hours per covered entity, resulting in remaining annual burden for complying with the minimum necessary requirement of 14 hours on average. The Department welcomes comments and information about its estimates and the assumptions underlying its proposed burden calculations and cost savings, including:

- The level of workforce member (*e.g.*, clerical staff, professional) responsible for making minimum necessary determinations on behalf of covered health care providers and health plans and a description of how the determination is made based on a covered entity's minimum necessary policies and procedures;
- Time spent by a covered health care provider or health plan to make a minimum necessary determination;
- The frequency with which a covered health care provider or health plan makes minimum necessary determinations (*i.e.,* the number of determinations by day or month); and

- The frequency with which a covered health care provider or health plan currently obtains individuals' authorizations prior to making a disclosure of PHI for care coordination or case management for that individual.

xvi. Costs arising from adding an exception to the minimum necessary standard for disclosures for individual-level care coordination and case management

The proposed changes to the minimum necessary standard are deregulatory in nature, so the Department anticipates that the costs arising from the proposal to add an exception to the minimum necessary standard would be due primarily to time spent revising policies and procedures for using and disclosing information and updating the content of workforce training. While the expenses of actually conducting such training typically would be included in such estimates, the Department would expect covered entities to include the updates in their existing HIPAA training and, thus, to incur additional training costs only for updating the training content. The Department estimates that changes to policies and procedures for minimum necessary and disclosures for care coordination and case management would require 75 minutes of lawyer time at an adjusted mean hourly rate of $139.72, and revisions to training content would require one hour of training specialist time (including related training for care coordination and case management definitions and disclosures to third parties, such as social services agencies, community based support programs, and HCBS providers) at an adjusted mean hourly rate of $63.12.

xvii. Estimated cost savings from changing "professional judgment" to "good faith" and "imminent" to "reasonably foreseeable"

The Department proposes to amend five provisions of the Privacy Rule to replace the exercise of "professional judgment" with a "good faith belief" as the standard to permit certain uses and disclosures in the best interests of the individual, to apply a presumption of compliance with the good faith requirement, and to replace "serious and

imminent threat" with "serious and reasonably foreseeable threat" in 45 CFR 164.512(j)(1)(i)(A). As discussed in the analysis of non-quantifiable benefits, the Department does not have data sufficient to estimate the reduction in professional time spent analyzing the risk of harm; however the Department believes this change would result in cost savings to covered entities, in addition to the cost savings from improved patient safety and treatment outcomes, as well as, potentially, the decreased costs due to avoided public safety incidents The Department seeks comment on the potential cost savings from this proposed change.

xviii. Costs arising from changing "professional judgment" to "good faith" and "imminent" to "reasonably foreseeable"

The Department anticipates that some covered entities, such as covered entity facilities that maintain patient directories and covered entity facilities and providers that routinely treat patients with SMI or SUD, would need to update their policies and procedures and train their workforce about the modifications to the Privacy Rule. The Department estimates that these costs would be due to one hour of a lawyer's time to update policies and procedures (for a total of 768,169 burden hours at a cost of $107,328,573) and 40 minutes of a training specialist's time to update related HIPAA training content (for a total of 512,113 burden hours at a cost of $32,324,552). The Department believes there may be some initial increase in costs for health plans, including Medicare and state Medicaid agencies, who pay for treatment or recovery of individuals experiencing substance use disorder due to the increase in disclosures to family members and other caregivers. In this regard, the Department believes that family members and caregivers are likely to encourage and support these individuals in seeking treatment, and thus that these individuals will be more likely to seek or remain in treatment. However, the Department would expect lower long-term costs for potentially avoiding public safety incidents, emergency health care services to offset any initial higher utilization costs. The Department also acknowledges the concerns that the proposed changes could have the

unintended adverse effect of deterring some individuals from seeking care, due to concerns about providers disclosing PHI to family members and others. The Department seeks comment on the extent to which the proposed changes would support or frustrate access to effective treatment, or impose costs and burdens on individuals or covered entities.

xix. Estimated cost savings from eliminating the acknowledgment of receipt of the NPP

The Department proposes to eliminate the requirements in 45 CFR 164.520 for certain covered health care providers[319] to obtain a written acknowledgment of receipt of the providers' NPP and, if unable to obtain the written acknowledgment, to document their good faith efforts and the reason for not obtaining the acknowledgment. The proposal also would remove the current requirement to retain copies of such documentation for six years. The Department estimates that approximately 613 million individuals annually receiving care for the first time from a covered health care provider would receive the NPP from the health care provider.[320] In a prior Paperwork Reduction Act burden estimate, the Department projected that the requirements related to disseminating and obtaining an acknowledgment would impose, on average, three minutes for each covered health care provider with a direct treatment relationship with an individual to disseminate each notice and obtain a documented acknowledgment of receipt, or document the good faith effort to obtain the acknowledgment and reason it was not obtained.[321] This estimate was based on the assumption that the required notice and acknowledgment would be

---

[319] The requirements related to the acknowledgment of receipt of an NPP apply only to covered health care providers that have direct treatment relationships with individuals. *See* 45 CFR 164.520(c)(2)(ii) and (3)(iii); 45 CFR 164.520(e).

[320] *See* 81 FR 31646 (May 19, 2016). The ICR estimated 613 million individuals would receive the notice of privacy practices from a health care provider and 100 million would receive the notice from their health plan via direct mail and another 100 million individuals would receive the notice from their health plan electronically.

[321] *Ibid.*

bundled with and disseminated with other patient materials. The total annual burden associated with this requirement was calculated to be 30,650,000 hours.[322]

In the 2018 RFI, the Department solicited public input to evaluate the accuracy of its burden estimates associated with obtaining an individual's acknowledgement of receipt of the NPP. Question 43 of the 2018 RFI asked "[w]hat is the burden, in economic terms, for a covered health care provider that has a direct treatment relationship with an individual to make a good faith effort to obtain an individual's written acknowledgement of receipt of the provider's NPP? OCR requests estimates of labor hours and any other costs incurred, where available."[323] Question 49 asked "[w]hat is the burden, in economic terms, for covered health care providers to maintain documentation of the good faith effort to obtain written acknowledgement and the reason why the acknowledgment was not obtained? What alternative methods might providers find useful to document that they provided the NPP?"[324] Comments highlighted the burden but did not provide estimated numbers of labor hours associated with these activities. For example, one commenter representing community pharmacies noted that pharmacists spend "many hours" verifying and making good faith attempts to obtain an individual's written acknowledgment of receipt of the providers' NPPs in face-to-face or mail interactions. Removing this requirement would lead to "additional labor hours" to spend with patients.[325] Another commenter discussed the burden associated with its field-based programs to obtain a signed acknowledgment of receipt, but did not describe the economic burden. This same commenter also noted that its NPP was always bundled with patient intake forms described as "numerous" and a part of a lengthy process but did not provide more specific data other than to state that the full NPP was eight pages.[326] Yet another commenter, a

---

[322] *Ibid.*
[323] *See* 83 FR 64302, 64308 (December 14, 2008).
[324] *Id*. at 64309.
[325] Comment No. HHS-OCR-2018-0028-0995.
[326] Comment No. HHS-OCR-2018-0028-0559.

large medical group, responded that NPPs are part of a package of documents provided to patients at intake or registration, but the number of pages "varies widely" depending on the setting and nature of the particular provider. This same commenter explained that NPP acknowledgement forms were stored in the patient record but rarely, "if ever," referenced.[327]

The Department acknowledges the uncertainty and wide variability in how different covered health care providers disseminate the NPP acknowledgement and make a good faith attempt to obtain the signed acknowledgement and store and maintain it. The comments to the 2018 RFI, described above, demonstrate that quantifying the burden would necessarily include examining the manner or process by which a covered entity obtains the acknowledgement, as well as the format. With the increasing use of technology by covered entities (*e.g.*, electronic check-in), it is reasonable to assume that the time associated with this burden is low in some instances but higher for those covered entities that have not integrated technology into the process, or who have fully integrated the acknowledgment into other NPP processes that may need to be revised if the proposal is finalized. Therefore, the Department is estimating a range, from 30 seconds to 2 minutes and 55 seconds, taken to disseminate the NPP acknowledgement, request the patient's signature, explain what the acknowledgement consists of, wait for the patient to sign, complete the check-off or other procedure applied when the patient is unable or unwilling to sign, file the acknowledgement documentation, and store the documentation for six years. The Department estimates that covered health care providers would experience total annual savings of: 5,108,331 burden hours and $153,454,272 in cost savings at the low end, up to 29,798,610 burden hours and $895,150,257 in cost savings at the high end. The Department utilizes the mid-range estimate of 17,879,169 reduction in burden hours for an annual cost savings of $537,090,228 associated with the proposal to eliminate the

[327] Comment No. HHS-OCR-2018-0028-0649.

requirements associated with the good faith attempt to obtain acknowledgment of receipt of the NPP.

While the wide variation in procedures that covered health care providers use to fulfill the current requirements does not allow for precise quantification of burdens, the Department's assumptions and estimates reflect reasonable analysis of the available data and consideration of public input. With respect to the low end of the range, the Department assumes that in some instances, such as when a covered health care provider uses electronic means to disseminate and obtain the acknowledgement, the burden hours associated with these activities may be near negligible. For estimates at the high end of the range, the Department assumes that these covered entities expend more labor hours to disseminate and collect paper forms with individuals' signed acknowledgments of receipt of the NPP and file the forms. The Department accounts elsewhere in this regulatory impact analysis (RIA) for the increased time associated with the new individual right to discuss a covered entity's privacy practices. The remaining burden of one minute and 15 seconds encompasses time for direct treatment providers to copy and distribute each NPP. The Department calculates, based on the mid-range estimate of hours of a clerical employee's time (based on an adjusted mean hourly rate of $30.04) that this proposal would result in an estimated annual savings of $537,090,228. The Department seeks comment and other examples of how these reductions in compliance burdens translate into quantifiable cost savings, including the time spent by a covered health care provider to conduct the following health care activities, including by electronic means if applicable:

- Disseminate the NPP, including an acknowledgement form;
- Collect the NPP acknowledgment form;
- Determine whether an individual's acknowledgement form is current, including for processes that are paper-based or electronic.

The Department also assumes that eliminating the related requirement to maintain documentation of the acknowledgment of the NPP for six years would result in significant cost savings to direct treatment health care providers in the form of a reduction of one page (electronic or paper) of each patient's record, and reduced space needed for one page of medical records (if that is where such documentation is stored) per patient or reduced electronic storage space for systems that store these notices electronically; however, the Department has not quantified the potential savings. The Department anticipates that most of the savings would result from eliminating the collection and maintenance of these records in the future. The Department seeks comments on the cost savings covered health care providers would be likely to accrue as a result of these proposed changes.

xx. Costs arising from eliminating the acknowledgment of receipt of the NPP

The Department anticipates no costs for eliminating the requirement for direct treatment providers to make a good faith effort to obtain an individual's signed acknowledgment of receipt of the NPP and to maintain related documentation. The Department welcomes comments on this assumption.

xxi. Estimated cost savings arising from changes to the NPP content

The Department proposes to modify the header of the NPP to specify to individuals that the notice provides information about: (1) how to access their health information, (2) how to file a HIPAA complaint, and (3) individuals' right to a copy of the notice and ability to discuss its contents with a designated person. The required header also would have to specify whether the designated contact person is available onsite and must include a phone number and email address an individual could use to reach the designated person.

The Department does not anticipate quantifiable cost savings to covered entities from making the required changes to the NPP; however, the improvements to individuals'

right of access may contribute to improvements to health care delivery and the health of patients overall.

xxii. Costs arising from changes to the NPP content

The Department believes the burden associated with revising the NPP consists of costs related to developing and drafting the revised NPP for covered entities. The Department estimates that the proposal to update and revise the language in the NPP (including drafting the language in the header) would require one hour of professional legal services at the wage reported in Table 4. There are no new costs for providers associated with distribution of the revised notice other than posting it on the entity's website (if it has one), as providers have an ongoing obligation to provide the notice to first-time patients. The Department bases the estimate on its previous estimates from the 2013 Omnibus Rule, in which the Department estimated approximately 613 million first time visits with health care providers annually.[328] Health plans that post their NPP online would incur minimal costs by posting the updated notice, and then, including the updated NPP in the next annual mailing to subscribers.[329]

The Department further estimates the cost of posting the revised NPP on the covered entity's website would be ten minutes of a web developer's time at the wage reported in Table 4.

The Department assumes that about 1% of an estimated 613 million new patients[330] will ask for further discussion with the designated contact person. The Department believes this estimate is reasonable, given public comments indicating that individuals rarely ask questions about the NPP, and the assumption that most requests for discussion will be made in the context of a visit with a health care provider. The

---

[328] 78 FR 5566, 5675 (January 25, 2013).
[329] 45 CFR 164.520(c)(1)(v)(A).
[330] *See* 81 FR 31646 (May 19, 2019) and related explanation that there are an estimated 613 million individuals who would receive the NPP.

Department therefore estimates that 6,130,000 individuals may ask for a discussion on the NPP as a result of OCR's media campaigns as well as through general awareness of individual privacy rights under HIPAA. The Department does not have data to support a different assumption or estimate at this time, and the Department requests such data for future consideration. In particular, the Department seeks comments addressing the likelihood and any associated burden that individuals will contact their health plans to request a discussion of the plans' privacy practices, and if so, the frequency with which health plans would be contacted for these conversations. The Department estimates that its proposal to require covered entities to make available a person who may be contacted for further information on the covered entity's privacy practices would add $8.69 in burden per request for information or $53 million (or 715,167 burden hours) total per year. The Department assumes each discussion between the contact person and individual will last an average of 7 minutes as individuals ask questions and receive answers, at the adjusted mean hourly rate for a registered nurse, as reported in Table 4.

The Department invites comments on all aspects of its estimates and assumptions, including the time spent on the identified activities and the occupations or professions of persons designated to perform those tasks.

xxiii. Estimated cost savings from adding a permission to disclose PHI to a TRS communications assistant

The Department proposes to expressly permit covered entities (and their business associates, acting on the covered entities' behalf) to disclose PHI to TRS communications assistants to conduct covered functions, at proposed 45 CFR 164.512(m), and to expressly exclude TRS providers from the definition of business associate at 45 CFR 160.103.

Based on information from stakeholders, the Department believes that some covered entities with workforce members who are deaf, hard of hearing, or deaf-blind, or who have a speech disability may have entered into, or tried to enter into, a business associate agreement with a TRS provider before permitting a workforce member to

disclose PHI to a TRS communications assistant, while others limited the use of TRS communications assistants by workforce members. Thus, some covered entities incurred legal costs for entering into a BAA or for analyzing the legal risk of not permitting workforce members to use needed accommodations, which they would not have to incur under the proposed changes. The Department lacks sufficient data to quantify the cost savings of this proposed change, and requests comment on the extent to which covered entities and business associates currently have business associate agreements with TRS providers, and on any costs such entities incur when analyzing whether a business associate agreement is needed.

xxiv. Costs arising from adding a permission to disclose PHI through TRS

The Department has not identified any additional costs to covered entities arising from the proposed change other than changes to policies and procedures and training, as TRS is provided without charge to the user.[331]

g. Quantifiable Cost Savings Estimates

Table 10 summarizes the estimated annual cost savings of the proposed rule for covered entities, as described in the preceding section.

Table 10.[a]

Cost Item	Burden Count	Multiplier	Savings (Millions)
Clarifying Minimum Necessary	4 hours of health manager time X $110.74 = $442.96	Total CEs (774,331)	$343
Eliminating NPP Acknowledgment	1 minute 45 seconds (.0292) of clerk/receptionist time X $30.04 = $.877	613,000,000 1st time encounters	$537
TOTAL ANNUAL COST SAVINGS			**$880**
TOTAL CUMULATIVE COST SAVINGS (5 years) (undiscounted)			**$4,400**

a. Totals may not add up due to rounding

[331] *See* FCC's 2017 "Consumer Guide, Telecommunications Relay Service", available at https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.

h. Estimated Quantifiable Costs to Covered Entities

The Department summarizes in Table 11 the additional estimated administrative costs that entities would incur on a one-time basis in the first year of implementing the proposed regulatory changes. The Department anticipates that these costs would be for posting an access fee schedule online for entities that have not already done so and posting a revised NPP online.

Table 11.

One-Time Costs	**Burden Count**	**Multiplier**	**Total Administrative Cost (Millions)**
Post access fee schedule online	10 min. X web developer ($79.20) = $13.20	Total covered entities (774,331)	$10
Post revised NPP online	10 min. X web developer ($79.20) = $13.20	Total covered entities (774,331)	$10
Total One-Time Administrative Burden			**$20[a]**

a. Totals may not add up due to rounding.

Table 12 summarizes the ongoing labor costs that the Department anticipates covered entities would incur as a result of the proposed regulatory changes. These new requirements would be based on an individual's request and include providing copies of PHI and ePHI under the right of access within a shorter time, providing an estimate of access and authorization fees, providing an itemized list of allowable access charges, discussing privacy practices with individuals, and submitting requests for copies of PHI to health care providers or health plans.

Table 12a.[a]

Ongoing Costs	**Burden Hours & Pay**	**Multiplier**	**Total Annual Administrative Cost (Millions)**
Access for Individuals —Search and retrieval within shorter times	1 min. X records technician time ($44.80) = $.75	50% of 2,460,000 access requests = 1,230,000	$.9

Sending copies of ePHI to third parties other than covered entities—Non-internet based method	2 min. X records technician time ($44.80) = $1.49	25% of 615,000 access requests = 153,750	$0.230[b]
Sending copies of ePHI to health plans and providers under the right of access—Non-internet methods	4 min. X records technician time ($44.80) = $2.99	25% of 615,000 access requests = 153,750	$0.459[c]
Providing good faith fee estimates upon request	3 min. X records technician time ($44.80) = $2.24	3% (.03) of 2,460,000 access requests = 73,800	$0.165
Providing itemized list of access and authorization fees upon request	1 min. X records technician time ($44.80) = $0.75	1% (.01) of 2,460,000 access requests = 24,600	$[d].018
Discussing privacy practices with individuals upon request	7 min. X registered nurse time ($74.48) = $8.69	1% (.01) of 613 million 1st time encounters = 6,130,000 requests	$53
Submitting access requests to providers & plans for individuals	3.5 min. X medical assistant time ($34.34) = $2.00	15% (.15) of 615,000 access requests = 92,250	$0.185
Total Ongoing Annual Administrative Burden			**$55**

a. Totals may not add up due to rounding.
b. The estimate is $229,600.
c. The estimate is $459,200.
d. The estimate is $18,368.

The total estimated additional first year administrative labor costs (including costs that will be ongoing) would be approximately $76 million (Table 11 total and Table 12a total).

Table 12b summarizes the increased capital costs that covered entities are estimated to incur as a result of the proposed new section 45 CFR 164.525 with respect to fee estimates for copies of PHI provided under the right of access and with a valid authorization.

Table 12b

Fees Estimates Section	Proposed Regulatory Requirement	Number of Pages to be Printed	Average Cost	TOTAL
164.525	Making fee schedule available at the point of service and upon request	2,322,993	$0.10	$232,299
164.525	Provide an individualized estimate of fees by mail[a]	11,070	0.69[b]	$7,638
164.525	Printing itemized list of copy charges[c]	24,600[d]	$0.10	$2,460
Total Capital Costs				**$242,398**

a. This represents only the requests for which the individual asks for a written estimate to be mailed to them, which the Department estimates to be 10% of the annual 2.46 million total access requests.
b. This includes costs for printing ($0.08), postage ($0.55), paper ($.02), and an envelope ($.04).
c. This estimate assumes that the itemized list of charges would be included in the mailing of requested copies of protected health information, so postage costs are not added here.
d. 1% of 2.46 million annual total access requests.

i. Additional Costs for Revising Policies and Procedures

Table 13 summarizes the total projected costs for covered entities to revise their policies and procedures to comply with the proposed regulatory changes to the Privacy Rule. The Department includes the costs for legal review and drafting of policies and for a compliance manager to revise procedures for relevant workforce members or departments.

Table 13.

Revising Policies & Procedures	Time (mins.)	Covered Entities Affected	Burden Hours
Minimum Necessary, Disclosures for Care Coordination & Disclosures to Social Services Agencies & CBOs	75	774,331	967,914
Right of access (multiple provisions, including fee schedule)	180	774,331	2,322,993
Disclosures to family & friends of individual; Disclosures to prevent harm	60	768,169 (providers)	768,169
Revise NPP	60	774,331	774,331

Disclosures for Uniformed Services & TRS	10	774,331	129,055
Simplify verification & revise form	30	5% of 774,331 covered entities = 38,717	19,358
TOTAL Burden Hours			**4,981,820**
TOTAL Costs			**$696 million**

j. Estimated Additional Costs for Revising HIPAA Training Programs

Table 14.

Training Content to be Revised	Time (mins)	Covered Entities Affected	Burden Hours
Minimum Necessary, Disclosures for Care Coordination, & Disclosures to Social Services Agencies & CBOs	60	774,331	774,331
Changes to Access Times, Changes to Access Procedures, Submitting PHI to Providers & Plans, and Fees and Estimates	150	774,331	1,935,828
Disclosing PHI to Family & Friends; Uses and Disclosures to Prevent Harm	40	768,169 - Providers	512,113
Disclosures for Uniformed Services; Telecommunications Relay Services	15	774,331	193,583
Right to Discuss NPP	5	774,331	64,528
Verification of Identity	10	5% of covered entities = 38,717	6,453
Total Time to Update Training Content			**3,486,834**
Total Costs for Updating Training Content	1 hour of Training Specialist time = $63.12		**$220 million**

The Department also estimates potential increased first-year costs for training medical records technicians to initially implement the changes to the right of access procedures, as shown in Table 14b.

Table 14b.

Staff in Training	Hourly Wage[a]	Time (in minutes)	Covered Entities Affected	Burden Hours	Costs (in millions)
Medical Records Technician	$44.80	7	774,331	90,339	$4,047

a. *See* Table 4.

Table 14c. Total estimated training costs (Table 14a and 14b)

Cost Item	Burden Hours	Costs (in millions)[a]
Updated Training Content	3,486,834	$220
Increased Time in Training	90,339	$4
TOTAL NEW TRAINING COSTS	**3,577,173**	**$224**

a. Totals may not add up due to rounding.

k. Costs Borne by the Department

The Department expects that it would incur costs related to disseminating information about the proposed regulatory changes to covered entities, including health care providers and health plans. However, the Department expects that many of these costs could be made part of the ongoing dissemination of guidance and other explanatory materials that OCR already provides. The covered entities that are operated by the Department would be affected by the proposed changes in a similar manner to other covered entities, and those costs have been factored into the estimates above.

l. Comparison of Benefits and Costs

The Department expects the benefits of the proposed rule to outweigh any costs because covered entities will save costs each year after the first year, having experienced initial higher costs related to implementation of proposed changes. The proposed changes to, or clarifications of, the minimum necessary standard, access fees, and the

acknowledgment of the NPP would be largely deregulatory. The Department expects covered entities and individuals to benefit from the increased flexibility and confidence covered entities would have to act in individuals' best interests without undue concerns about HHS enforcement actions. The Department also expects covered entities to realize savings from less frequent consultations with legal counsel about when they can disclose PHI regarding individuals who are incapacitated or experiencing another emergency and reductions in minimum necessary analyses when disclosing PHI for individual-level health care coordination and case management activities that constitute treatment or health care operations. The Department further expects that, by involving family members and others, this proposed action would result in improved care coordination and case management and better patient health outcomes. The Department also expects that changes to the right of access, such as a shortened time limit for responding to a patient's request, the right to photograph or otherwise capture PHI using the individual's own device, and the right to an estimate of access and authorization fees, would significantly strengthen the access right, to the benefit of individuals. Additionally, replacing the requirement to obtain an acknowledgment of an individual's receipt of the NPP with an individual right to discuss a covered entity's privacy practices upon request would improve access to care and strengthen individual's understanding of their rights. The Department expects these benefits would substantially outweigh estimated costs, such as covered entities providing access in a shorter time, providing the new discussion right, posting an access fee schedule, modifying internal policies, and providing new trainings to workforce members.

The Department requests comment on these assumptions and on all aspects of this regulatory impact analysis. The tables below present the Department's summary of estimated quantifiable costs and cost savings (Tables 15 and 16), cost transfers (Table 17), and non-quantifiable costs and benefits (Table 18).

Table 15. First Year Estimated Quantifiable Costs/Cost Savings to Covered Entities, in Millions[a]

Cost Item	Costs	Savings
Revised Training	$224	
Revising P&P	$696	
Administrative Costs	$76	
Capital Costs	$0.242	
Eliminating NPP Acknowledgment		($537)
Clarifying Minimum Necessary		($343)
TOTAL	**$996**	**($880)**
NET SAVINGS/COST- FIRST YEAR		**$116**

a. Totals may not add up due to rounding

Table 16. Ongoing Estimated Quantifiable Annual Costs/Costs Savings Estimates to Covered Entities, in Millions (years 2 – 5)[a]

Cost Item	Costs	Set-off Amount (Savings)
Access & Administrative Costs	$55	
Capital Costs	$0.242	
Eliminating NPP Acknowledgment		($537)
Clarifying Minimum Necessary		($343)
TOTAL	**$55**	**($880)**
NET COSTS/SAVINGS		**($825)**

a. Totals may not add up due to rounding.

Table 17. Estimated Transfers, in Millions

Cost Item	Amount of Costs Transferred (transferors)	Amount of New Costs Incurred (transferees)
Decreased fees for providing electronic copies in an EHR on electronic media to individuals	$1.4 (individuals)	$1.4 (covered entities, primarily providers)
Additional fees for authorizing copies of non-EHR PHI to a third party	$43 (covered entities, primarily health care providers): 615,000 access requests X $70 average estimated increased fee	$21.5 (individuals)
		$21.5 (third party recipients)

Covered entities would benefit from a total estimated net increase of $41.6 million in transferred costs for allowable fees for providing copies of PHI, while individuals would incur the same amount.

Table 18. Non-quantifiable Costs/Benefits for Covered Entities and Individuals

Regulatory Changes	Costs	Benefits
Changing to minimum necessary, health care operations definition, and the addition of permissible disclosures to social services agencies	Potential increase in number of requests for disclosures for certain care coordination and case management purposes	Improved care coordination and case management, resulting in better health outcomes
Changing from "professional judgment" to "good faith" and from "imminent" to "reasonably foreseeable"	Potential increased complaints to OCR from individuals who did not want their PHI used or disclosed; potential to chill some individuals' willingness to access care	Improved care coordination and case management; increased harm reduction; likely increase in adherence to treatment and increased service utilization
Changing verifications		Improved access to PHI
Adding permission to disclose to TRS and excluding TRS providers from the definition of business associate		Improved employment conditions and opportunities for workforce members who are deaf, hard of hearing, or deaf-blind, or who have a speech disability; improved compliance with non-discrimination laws
Adding right to discuss covered entity privacy practices, eliminating NPP acknowledgment requirement & changes to NPP		Improved understanding of individuals' rights & covered entities' privacy practices; improved access to care
Better enabling individuals to direct the transmission of electronic PHI in an EHR among providers and plans as part of the right of access		Improved care coordination and case management; increased individual control over directing ePHI for health-related purposes
Strengthening right of access (free online access; shorter access times; right to inspect; access fee information)	Increased burden on individuals to directly obtain lower cost copies of non-EHR PHI and send it to third parties to avoid paying higher fees under an authorization	Improved access to PHI by individuals—receiving PHI twice as fast; improved access to ePHI by providers & plans; reduction in access fee disputes/improved

		collection of access fees; increased certainty about allowable fees; increased adoption and utilization of EHR technology
Restricting the right to request that a covered entity direct the transmission of certain PHI to a third party	Increased burden on individuals to submit two forms: an access request and an authorization, when seeking to send a complete medical record to a third party	Improved clarity and certainty for covered entities;
Adding an optional element of the NPP for covered entities to provide information about alternate ways to obtain PHI directly or have it sent to a third party, for certain requests to direct the transmission of certain PHI to a third party		Increased knowledge by individuals of their rights to access and their options for accomplishing their information sharing goals.

The Department's costs-benefits analysis asserts that the proposed regulatory changes would significantly advance care coordination and the transformation to value-based care and strengthen individual rights. Although there is a projected total net cost of $116 million in the first year, the total estimated annual net cost savings to covered entities in subsequent years would be approximately $825 million, with total projected net savings of $3.2 billion and an average increase in allowable fees for copies of $70 per request to direct copies of PHI to third parties.

m. Uncertainty Analysis for Estimated Costs and Cost Savings

The Department has analyzed a range of estimated costs and costs savings for key compliance burdens that are likely to be affected if the proposed regulatory changes are implemented as outlined. The Department performed an uncertainty analysis for each of the main drivers of costs and cost savings, reporting low, mid, and high values for each category, and for the proposed rule as a whole to better capture the range of potential outcomes. In summary, the Department estimates total costs of implementation over a five-year period ranging from a low of approximately $0.8 billion to a high of

approximately $4 billion and a range of five-year cost savings of approximately $1.2 billion to $7.5 billion.

Table 19. Range of Total Estimated Costs over Five Years (2021-2025)

Cost Item	Low	Mid	High
Training	$195,651,092	$224,136,148	$250,512,185
Policies & Procedures	$542,791,420	$696,059,917	$1,302,384,017
Access & Administrative Tasks	$40,984,833	$296,648,766	$2,879,447,799
Capital Costs	$1,175,457	$1,211,988	$1,979,493
TOTAL COSTS	**$780,602,802**	**$1,218,056,819**	**$4,434,323,494**

Table 20. Range of Total Estimated Cost Savings over Five Years (2021 – 2025)

Cost Savings Item	Low	Mid	High
Eliminating NPP Acknowledgement	$767,271,360	$2,685,451,140	$4,475,751,287
Clarifying Minimum Necessary	$428,747,075	$1,714,988,299	$3,001,229,523
TOTAL COST SAVINGS	**$1,196,018,434**	**$4,400,439,439**	**$7,476,980,809**

i. Cost Estimates

Updated Training Content

Because required HIPAA training is based on covered entities' policies and procedures, changes to the policies and procedures are accounted for separately, and a training specialist's time is allocated for time spent in updating existing training content. The burden hours are based on an adjusted hourly cost of $63.12 (see table 4). The content area for which the greatest training burden is estimated is due to the combination of proposed changes to the right of access and the new right to request fee estimates and itemized lists of charges for copies of PHI. At the low end, the Department estimates a burden of two hours for updating this section of the training content, and at the high end, three hours. This results in a low estimate of 1,548,662 total annual burden hours for all

covered entities at a one-time cost of $97,751,545 and a high estimate of 2,322,993 burden hours at a cost of $146,627,318 for updating the access portions of the training program. The Department proposes to adopt a mid-range estimate of 2 hours and 30 minutes to update the access and fee estimate portions of the training content for a total of 1,935,828 burden hours at a cost of $122,189,432. The Department also estimates additional time spent in training for an average of one medical records technician per covered entity in the first year at an adjusted hourly labor cost of $44.80 (see Table 4), ranging from a low of 5 minutes to a high of 10 minutes. Overall one-time training costs for all proposed changes to the Privacy Rule are estimated to range from a low of $198,541,928 (and 3,164,196 burden hours) to a high of $250,512,185 (and 4,006,281 burden hours). The Department proposes adopting a mid-range estimate of 3,577,173 total burden hours at a one-time cost of $224,136,148. The 2013 Omnibus Final Rule contained no cost estimates for updates to HIPAA training programs and in the 2000 Privacy Rule the Department based its estimates on the time spent by covered entity workforce members to participate in training and not the time for a training specialist to update training content. In 2000, the Department anticipated that, in part, professional associations and other organizations would develop training for different types of covered entities, thus reducing potential burden for implementing the new requirement. Because time spent in training by workforce members is already an acknowledged burden, the training estimates developed for this proposed rule reflect only the new burden: the time to update training program content. These estimates are slightly less than those for updating policies and procedures, to reflect that the foundation for the work is already laid by the updated policies and procedures established by legal counsel.

Updated Policies and Procedures

The Department estimates a range of average total burden hours per covered entity to update policies and procedures as a result of the proposed modifications to the Privacy

Rule, based on only the adjusted hourly wage for a lawyer of $139.72 (see Table 4) for the low and mid-range estimates, and adds the adjusted hourly wage for a health care manager of $110.74 for the high-range estimate. At the low end, the Department estimates a total burden per covered entity of 5 hours and 30 minutes (for a total of 3,884,851 hours and a cost of $542,791,420) for updating policies and procedures and at the high end 13.51 hours (for a total of 10,014,867 hours and a cost of $1,302,384,017). The Department proposes adopting a mid-range estimate of 6 hours and 55 minutes for a total estimate of 4,981,820 burden hours at a one-time cost of $696,059,017**.**

Access and Administrative Tasks

Post an Access Fee Schedule Online

The Department estimates a low burden of 8 minutes of a web developer or designer's hourly wage of $79.20 (see Table 4) to post an access fee schedule online per covered entity and a high estimated burden of 15 minutes. These costs would range from 103,244 total annual burden hours to 193,583 burden hours, and costs of $8,176,935 at the low end to $15,331,754 at the high end. The Department proposed to adopt the mid-range estimate of 10 minutes for posting the new access fee schedule for a one-time total of 129,055 burden hours and a cost of $10,221,169.

Post an Updated Notice of Privacy Practices (NPP)

The Department estimates a range of costs for covered entities to post an updated NPP at the hourly wage of a web developer or designer from a low of 8 minutes (and total burden hours of 103,244) to a high of 15 Minutes (and total burden hours of 193,583), and total costs from a low of $8,176,935 to a high of $15,331,754. The Department proposes to adopt the mid-range estimate of 10 minutes for posting the revised NPP for a one-time total of 129,055 burden hours and a cost of $10,221,169.

Unreimbursed Costs of Providing Access

The Department has separately estimated the charges that a covered entity may pass on to individuals who request copies of their PHI in the form of fees and allocated those as a transfer of costs. However, the Department estimates that due to the proposed changes to the access right covered entities may incur some costs above those that are allowed to be charged as fees. The Department has developed a range of cost estimates based on the hourly wage of a medical records technician ($44.80, see Table 4), ranging from .5 to 2.5 additional minutes of labor, and total burden hours ranging from a low of 10,250 total annual burden hours to a high of 51,250 hours. Annual cost estimates range from a low of $459,200 to a high of $2,296,000. The Department proposes to adopt the mid-range estimate of 1 minute per request of uncompensated labor for providing access within a shorter time period for a total of 20,500 annual burden hours and an annual cost of $918,400. All of these estimates are based on an estimate that 50 percent of the total estimated 2,460,000 annual access requests (or 1.23 million) will be from individuals seeking copies of their own PHI or ePHI.

Submit Access Requests for Individuals to Health Plans and Providers

The Department estimates on the low end that 10 percent of the total 615,000 requests by individuals to direct electronic copies of their PHI to their health care provider or health plan will be made by requesting that the receiving health care provider or health plan submit the request on the individual's behalf (or 61,500) and on the high end that 20 percent of such requests (or 123,000) will be made by requesting the assistance of the receiving health care provider or health plan. The Department believes that a medical assistant would submit these access requests to health plans and providers for individuals, at an hourly wage of $34.34 (see Table 4). The range of estimated costs is based on a low estimate that this task, on average, will take 2 minutes to complete, to a high estimate of 5 minutes. The total estimated annual burden hours ranges from 2,050 (and a cost of $70,397) to 10,250 (and a cost of $351,985). The Department proposes to adopt the mid-

range estimate of 3.5 minutes for submitting 92,250 requests (15 percent of 615,000) for individuals for a total of 5,381 annual burden hours and an annual total cost of $184,792.

Transmit ePHI to health plans and providers through non-internet means

The Department's proposal to prohibit covered entities from charges fees for the labor associated with sending electronic copies of PHI through non-internet means (e.g., the mail) could result in some unreimburseable costs for covered entities. The Department estimates that the costs would be based on the hourly wage of a medical records technician ($44.80, see Table 4) and a low estimate of 3 minutes to a high estimate of 5 minutes for 153,750 requests (representing 25 percent of the estimated 615,000 total annual requests to direct copies of PHI to health plans and providers). This results in a low estimate of 7,688 total annual burden hours at a cost of $344,400 and a high estimate of 12,813 total annual burden hours at a cost of $574,000. The Department proposes to adopt the mid-range estimate of 4 minutes per request for transmitting ePHI to health plans and providers through non-internet means for a total of 10,250 annual burden hours and a cost of $459,200. These estimated costs have not been previously calculated as a potential burden on covered entities and the Department requests comment on these ranges and the assumptions underlying them.

Transmit ePHI to Third Parties through Non-internet Means

The Department estimates that the unreimburseable costs for transmitting electronic copies of ePHI to third parties other than health plans and providers would be half of that for transmitting the same information to health plans and providers because some of the costs are likely to be charged as fees to individuals for copies. The estimated costs are based on the hourly wage of a medical records technician ($44.80, see Table 4), ranging from a low estimate of 1.5 minutes to a high estimate of 2.5 minutes for 153,750 requests (representing 25 percent of the total estimated 615,000 annual requests to direct copies of PHI to third parties other than health plans and providers). This results in a low

estimate of 3,844 total annual burden hours at a cost of $172,200 and a high estimate of 6,406 total annual burden hours at a cost of $287,000. The Department proposes to adopt the mid-range estimate of 2 minutes per request for transmitting ePHI to health plans and providers through non-internet means for a total of 5,125 annual burden hours and a cost of $229,600.00.

Providing Fee Estimates

The Department estimates costs for providing good faith individualized fee estimates to individuals for a low of 24,600 requests (1% of total 2.46 million annual access requests) to a high of 123,000 requests (5% of 2.46 million annual access requests). The Department has also estimated the time it would take a medical records technician to develop a good faith individualized fee estimate from a low of 3 minutes to a high of 5 minutes per request, or an annual total of burden hours ranging from 1,230 (at a cost of $55,104) to 10,250 (at a cost of $459,200). The Department proposes to adopt the low-range estimate of 3 minutes of labor and the mid-range number of 73,800 requests (3 percent of 2.46 million total annual access requests) resulting in a total of 3,690 annual burden hours and a total annual cost of $165,312.

Providing Itemized Lists of Charges

The Department estimates costs for providing an itemized list of charges for requested copies of requested PHI, ranging from a low of 2,460 requests (0.1% of total 2.46 million annual access requests) to a high of 123,000 (5% of total annual access requests). The Department has also estimated a range of burden from a low of 41 total annual burden hours (at a cost of $1,837) to a high of 2,050 total annual burden hours (at a cost of $91,840). The Department proposes to adopt the mid-range estimate of 410 annual burden hours and a total annual cost of $18,368.

Discussing Privacy Practices

The Department estimates a range of costs for the requirement to discuss a covered entity's privacy practices with an individual upon request. The range is based on a low of 5 minutes of a registered nurse's time for 613,000 health care encounters (.1% of 613,000,000 total new health care encounters per year) to a high of 10 minutes of a health care manager's time for 30,650,000 health care encounters (5% of total new health care encounters per year). The total estimated annual burden hours for this proposed regulatory change ranges from 51,083 at the low end to 5,108,333 at the high end, and costs of $3,804,687 at the low end to $565,696,833 at the high end. The Department proposes to adopt the mid-range estimate of 7 minutes of a registered nurse's time for 6,130,000 requests (1 percent of 613,000,000) for a total estimate of 715,167 annual burden hours and a total annual cost of $53,265,613.

Capital Costs

The Department estimates annual capital costs for three elements of the proposed rule: making an access fee schedule available, providing fee estimates for copies of PHI, and providing itemized lists of charges for copies of PHI. The capital costs for fee estimates and itemized lists of charges are based on the estimated number of requests, while the range of access fee schedule costs varies due to the number of copies provided by each covered entity. The total annual capital cost estimates range from a low of $235,091, a mid-range of $242,398, to a high of $395,899.

ii. Cost Savings Estimates

Minimum Necessary

Because the Department is without data to estimate the actual average compliance burden, it has calculated a range of estimates for the costs savings resulting from the combined effects of the proposed regulatory modifications to the definition of health care operations and the minimum necessary standard. At the low end, the Department estimates a cost savings of 1 hour of labor annually per covered entity at the hourly rate of a health

services manager ($110.74, see Table 4) for a total reduction of 774,331 burden hours and an annual cost savings of $85,749,415. At the high end, the Department estimates costs savings of 7 hours of labor for a total annual reduction of 5,420,317 burden hours and $600,245,905 in cost savings. The Department proposes to adopt an approximate mid-range estimate of burden reduction, which is 4 hours per covered entity for an annual total of 3,097,324 burden hours and $342,997,660 in total annual projected cost savings.

NPP Acknowledgement

The Department has previously estimated a burden of 3 minutes for providing the NPP and obtaining the signed acknowledgement of receipt or documenting a good faith effort to do so. The Department estimates that the requirement to obtain the signed acknowledgement or document a good faith effort accounts for a large portion of the 3-minute burden because it involves engaging with the individual or their personal representative, obtaining or creating documentation, and storing the documentation for each individual. Lacking data to precisely estimate the amount of burden reduction for the proposed removal of the acknowledge requirements, the Department estimates a range of labor cost savings from a high of two minutes and 55 seconds to a low of 30 seconds for each NPP that is provided by a direct treating health care provider to a new patient. On an annual basis for all covered entities, this would range from a total savings of 5,108,331 burden hours and $153,454,272 in cost savings at the low end to 29,798,610 burden hours and $895,150,257 in cost savings at the high end. The Department proposes adopting a mid-range estimate of burden reduction in the amount of one minute and 45 seconds of labor for each NPP due to the proposed regulatory modifications for a total annual reduction of 17,879 burden hours and $537,090,228 of cost savings.

4. Consideration of Regulatory Alternatives

The Department carefully considered several alternatives to issuing this NPRM, including the option of not pursuing any regulatory changes, but rejected that approach for

several reasons. First, the proposed regulatory changes would further the Administration's goal of reducing regulatory burden on individuals and the regulated community and promoting care coordination. Second, many commenters on the 2018 RFI believed the Privacy Rule could be improved, and offered comments supportive of some of the ideas suggested in the RFI that now are proposed in this NPRM. Revising the Privacy Rule would clarify covered entities' obligations and flexibilities, improve individuals' access to their PHI, and improve care coordination and case management overall.

a. Increase outreach and issue additional clarifying guidance without rulemaking

As an alternative to rulemaking, the Department considered expanding OCR outreach, guidance, and educational materials to address misconceptions about (1) when HIPAA permits uses and disclosures of PHI, including to social services agencies and to family, friends, caregivers, and others; (2) what fees may be charged for providing access to PHI; (3) when the minimum necessary standard applies to disclosures for case management and care coordination; (4) when covered entities are required to transmit PHI to third parties, including health care providers and health plans; and (5) when individuals have the right to take photos of their own PHI.

The Department has published extensive guidance on existing standards in the form of videos, fact sheets, FAQs, decision trees, and infographics. Still, OCR has received comments and heard anecdotal evidence that, despite the existing guidance and ongoing outreach efforts, covered entities remain fearful of incurring HIPAA penalties for using and disclosing PHI in the circumstances addressed in this proposed rule. In addition, some of the beneficial disclosures that this NPRM proposes to expressly permit currently are not permitted, or are burdensome to complete, under the existing Privacy Rule, as described throughout the preamble. Therefore, in addition to continued outreach efforts, the Department believes it would effectively address the concerns outlined in the preamble discussion by modifying the existing standards.

b. Alternative Regulatory Proposals Considered

The Department welcomes public comment on any benefits or drawbacks of the following alternatives it considered while developing this proposed rule.

Right of Access

Changing the Right to Direct Electronic Copies of EHR to a Third Party and Form and Format for Such Requests

The Department considered how to modify the Rule consistent with the HITECH Act and the *Ciox v. Azar* decision. An approach considered and not adopted would have created two new unreviewable grounds to deny an access request to direct a copy of PHI to a third party: 1) if the requested copy was for PHI not contained in an EHR; and 2) if the request was for a copy of PHI not in electronic format. As part of the response to the written denial a covered entity would have been required to provide information about how the individual could access the requested PHI directly or how to request it with a valid authorization.

The Department also considered a simplified approach, which would have required a covered entity to inform the individual about other options to obtain PHI, but without creating new grounds for denying the request. Instead, the Department decided to propose an optional element that covered health care providers may add to their Notice of Privacy Practices (NPP) that would address individuals' requests to direct copies of PHI to a third party that are not in an EHR or that are not electronic copies of PHI by informing them of the ability to request the copies of PHI directly and how to use a valid authorization to request the disclosure of the requested copies to a third party.

The Department also considered requiring covered health care providers to provide the electronic copies to third parties in a readable form and format as agreed to by the individual and the covered entity. This approach would not have required health care providers to provide the copies in the format requested by the individual, but would have

required some mutual agreement about the format. The Department, however, believes that the *Ciox v. Azar* decision does not permit it to propose requirements with respect to the form and format of copies of PHI directed to an individual's designated third party. Instead, the preamble to this NPRM encourages covered health care providers to produce copies in a readable electronic format that provides meaningful access to the requested PHI. The preamble also describes several examples of commonly accepted electronic formats for copies of PHI from an EHR.

As raised in the 2018 RFI, the Department considered whether to require covered entities to disclose PHI to other covered entities for purposes of treatment, payment, or health care operations and variations on that idea, such as limiting the requirement to health care providers or limiting such required disclosures to treatment purposes only. The Department also considered how much individual control should be permitted for disclosures between covered entities, such as an opt-in or opt-out mechanism or some type of express permission. Due to the privacy concerns raised in comments on the RFI, the Department adopted a different approach whereby an individual could direct their current health care provider or health plan to submit an access request to another health care provider ("Discloser") on the individual's behalf to have the individual's PHI sent to the current provider or plan ("Requester-Recipient"). This new pathway promotes disclosures to individuals' current health care providers and health plans in a manner that retains individual control. The Department believes that this proposal would be less burdensome than imposing mandatory disclosures for all requests for PHI for treatment, payment, and health care operations purposes.

Access Time Limits

The Department considered the feasibility of changing the access time limits by requiring covered entities to provide copies of electronic PHI within a shorter time period than non-electronic PHI. The comments on this question in the 2018 RFI revealed that

multiple factors affect how long it takes a covered entity to provide access to PHI, separate from whether the PHI was created, or is maintained, in electronic or non-electronic format. Given this input, the Department believes that imposing a shorter time limit in the Privacy Rule for individual's access to electronic PHI than for non-electronic PHI would create unnecessary complexity and add to covered entities' burdens. For example, a request for a complete medical record may require the production of copies of both electronic and non-electronic PHI, and complying with differing time limits for different parts of a request would be difficult to track. However, the Department's proposals would result in different timelines for electronic and non-electronic copies of PHI sent to third parties because certain requests could be made by means of the right of access (for electronic copies of PHI in an EHR) and other requests would not be within the right of access (for non-electronic copies or electronic copies not in an EHR), and there is no time limit for disclosures requested using an authorization which are not required disclosures.

The Department also considered whether to modify the Privacy Rule to require covered entities to disclose PHI for continuity of care or medical emergencies within a shorter time than required under the access right. Many commenters on the 2018 RFI supported this concept; however, commenters also stressed the importance of streamlined and simplified requirements for ensuring compliance with any changes to the Privacy Rule. In light of this feedback, rather than impose a different time requirement for providing access for continuity of care or emergencies, the Department proposes at 45 CFR 164.524(b)(2)(ii)(C) to require entities to adopt a policy addressing the prioritization of access requests, to reduce or avoid the need for an extension of the time limit for providing copies of PHI at the direction or with the agreement of the individual. The Department understands that many covered health care providers already prioritize requests for PHI for these purposes. This proposed change would require covered entities

that do not yet have such a policy to incur the one-time cost of developing a new policy and procedures and incorporate them into existing HIPAA training content.

The Department also considered whether to change the access time limits overall to a period shorter than the 15 calendar-day proposed time and did not pursue this approach because that is more stringent than many of the short time limits contained in state access laws and may overly burden covered entities and affected business associates. However, to the extent a shorter requirement in which to provide access to individuals already exists in state or other laws, the Department is proposing at 45 CFR 164.524(b)(2)(iii) that said requirement be deemed practicable under the Privacy Rule. The Department requests comment on whether a time limit shorter than 15 calendar days would be appropriate, and welcomes data on the burdens and benefits such a time limit would impose or concerns about using others laws as a measure of practicability.

Access Fees

The Department considered retaining the existing access fee structure without change. However, the Department believes it can address the concerns of some commenters on the 2018 RFI that multiple, voluminous access requests to direct copies of PHI to third parties may be taking entities' time and resources away from fulfilling access requests to provide copies to individuals themselves and requests from other covered entities for disclosures for care coordination and case management.

The Department also considered allowing covered entities to charge no more than the limited access fee amounts for directing non-electronic copies of PHI to a third party for any treatment, payment, and health care operations purposes, while permitting higher fees for directing non-electronic copies of PHI to a third party for any other purposes. The Department does not propose this approach because it would open the door for covered entities to inquire into individuals' purposes in directing their own PHI to third parties. Instead, the Department proposes to adopt an approach that decreases the fees for access

requests to direct electronic copies of PHI in an EHR to third parties. However, covered entities could charge higher fees for disclosing non-electronic copies of PHI or electronic copies of PHI that is not in an EHR, provided the fee does not result in an impermissible "sale" of PHI under 45 CFR 164.502(a)(5)(ii).

Verification of Identity

The Department considered modifying the individual right of access provision to prohibit burdensome paperwork requirements for individuals without also changing the identity verification provisions. However, the Department determined that changing both would help covered entities and individuals understand how the access and verification provisions interact. The Department also considered applying the proposed prohibition against unreasonable measures only to identity verification related to access requests, which would be more narrowly tailored to situations the Department has seen in complaints filed with the Department. However, the Department does not see a meaningful distinction between the access right and the other individual rights under HIPAA that would justify treating them differently with respect to verification of identity.

Exceptions to the Minimum Necessary Standard

The Department considered limiting the new exception to the minimum necessary standard to disclosures to and requests by covered health care providers for all health care operations purposes. This would have relieved the burden on covered health care providers who conduct population-based care coordination and case management of needing to assess the minimum necessary PHI when exchanging information with other covered health care providers. Limiting the exception to health care providers also would have addressed the concerns of commenters who opposed an exception for disclosures to health plans due to concerns that the plans may use the information against patient interests. The Department rejected this option, however, because health plans collaborate with health care providers, other health plans and other entities, including public health

agencies, to improve patient health through care coordination and case management activities. In response to concerns raised about privacy protections, the Department is limiting this proposal to disclosures for individual-level activities that constitute treatment or health care operations. In addition, covered health care providers and health plans would continue to be responsible for meeting the minimum necessary requirements that currently apply, including when using PHI for treatment and health care operations purposes, as applicable. The proposed exception should reduce overall compliance burdens for both health plans and health care providers.

Disclosures to Third Parties such as Social Services Agencies, Community Based Organizations, and HCBS Providers

The Department considered proposing to clarify in the definition of treatment when a covered health care provider's disclosures to a social services agency, community based organization, or HCBS provider are considered part of that covered health care provider's treatment activities, without adding an express disclosure permission. The Department also considered limiting the proposed disclosure permission to only covered entity health care providers and excluding health plans from the proposed policy. Ultimately, the Department rejected that option and proposed a permission for covered health care providers and health plans to encourage beneficial information sharing that would support care coordination and case management for individuals. As described more fully in the preamble above, the Department seeks comments on the appropriate recipients of PHI under this proposal, activities and purposes for which the PHI should be used or disclosed, and the covered entities to which an expanded disclosure permission would apply.

"Professional Judgment" and "Good Faith"

Replace the professional judgment standard with the good faith standard throughout the Privacy Rule

The Department considered applying a presumption of good faith to all fourteen provisions in the Privacy Rule that allow covered entities to use or disclose PHI based on the exercise of professional judgment. However, the Department intends this proposed modification to carefully expand the ability of covered entities to use or disclose PHI to facilitate the involvement of family and caregivers in the treatment and recovery of people experiencing the impacts of the opioid crisis, serious mental illness, and health emergencies. The Department believes the remaining nine provisions would be beyond the scope of this goal.

The Department further believes there likely could be unintended consequences if it replaced the exercise of professional judgment standard with a good faith standard across all fourteen provisions, including those provisions not rooted in emergency circumstances. For example, in the case of disclosures to government agencies pursuant to 45 CFR 164.512(c), *Standard: Disclosures about victims of abuse, neglect or domestic violence,* the Department believes these provisions are well suited to ensuring that the necessary reporting can occur, and it does not believe replacing the professional judgment standard would change or prevent a course of action related to an individual affected by the opioid crisis or other urgent health situations. Covered entities still would be permitted to exercise professional judgment to use or disclose PHI under the nine remaining provisions.

The Department requests comment on whether the Department should apply the good faith standard to any or all of the other nine provisions in the Privacy Rule that call upon health care providers to exercise professional judgment, identified below.

- Disaster relief. 45 CFR 164.510(b)(4).
- Law enforcement – crime victims. 45 CFR 164.512(f)(3).
- Reviewable grounds for denying individual access to records**.** 45 CFR 164.524(a)(3).

    - Safety or endangerment. 45 CFR 164.524(a)(3)(i).
    - References another person. 45 CFR 164.524(a)(3)(ii).
    - Personal representative. 45 CFR 164.524(a)(3)(iii).
- Victims of abuse, neglect, domestic violence. 45 CFR 164.512(c)(1)(iii)(A).
    - Informing the individual. 45 CFR 164.512(c)(2)(i)
    - Informing the personal representative. 45 CFR 164.512(c)(2)(ii).
- Personal representative suspected of abuse or neglect. 45 CFR 164.502(g)(5)(ii).

Apply a presumption of compliance to all Privacy Rule provisions referencing professional judgment without changing the professional judgment standard to a good faith standard

The Department considered proposing to apply a presumption of compliance to all existing provisions that permit covered entities to make decisions about uses and disclosures of PHI based on the exercise of professional judgment, without replacing the standard with a good faith standard. However, as noted above, where the Department summarizes its proposed application of the good faith standard, the Department intends not only to presume compliance with existing permissions, but to broaden the circumstances in which covered entities will use or disclose PHI in order to help address the needs of individuals experiencing opioid use disorder and other similarly situated individuals. The exercise of professional judgment generally is limited to covered entities who can, for example, draw upon a professional license or training and therefore, by definition, limits the scope of persons who could use or disclose PHI to aid individuals experiencing substance use disorder, SMI, or a health emergency.

Replace the professional judgment standard with a good faith standard only in specified provisions of 45 CFR 164.510

The Department considered replacing the professional judgment standard with a good faith standard only in those provisions in 45 CFR 164.510 that are included in this

rulemaking: 45 CFR 164.510(a)(3)(B), 164.510(b)(2)(iii) and 164.510(b)(3). However, modifying only 45 CFR 164.510 would encourage the disclosure of information only to family members, friends, caregivers, and other involved persons and only in the circumstances addressed at 45 CFR 164.510. As previously stated, the Department intends through this proposal to carefully broaden the permissible uses and disclosures of PHI by covered entities in circumstances that relate to the opioid crisis, serious mental illness, and health emergencies, to ensure that covered entities are able to share information as needed to care for individuals and protect the public. Changing only the applicable provisions at 45 CFR 164.510 would limit the scope of individuals and circumstances that would benefit from this proposed rule.

Define "imminent" in 45 CFR 164.512(j)(1)(A) instead of replacing the term with "reasonably foreseeable"

The Privacy Rule does not define the term "imminent," although common understanding of the term conveys that an event will happen soon.[332] The Department considered defining the term to provide improved clarity, but believes that defining the term could have the unintended consequence of further restricting uses and disclosures under this provision. Instead, the Department proposes to create a standard based on reasonable foreseeability because the Department believes it would provide needed flexibility for covered entities to address serious threats to health and safety that are likely to occur. The new standard would address serious threats that might only be prevented if the covered entity is free of the constraint of having to predict the timeframe for a serious threat to occur.

NPP and Acknowledgment of Receipt

---

[332] *See* Merriam-Webster definition of "imminent": ready to take place: happening soon; often used of something bad or dangerous seen as menacingly near, available at https://www.merriam-webster.com/dictionary/imminent.

The Department considered requiring the online posting of the NPP by all covered entities, including those that do not currently have a website. However, the Department believes the burden of creating a website solely to post the NPP for those few covered entities without a website outweighed the benefits to individuals of such a requirement.

Telecommunications Relay Service

The Department considered an alternative proposal to categorize TRS providers as "conduits" because of their temporary access to PHI,[333] and thus deem them not to be business associates. However this alternative would not have addressed the lack of an applicable permission to disclose PHI for some necessary communications not contemplated under the current Privacy Rule. In addition, TRS communications assistants have "access on a routine basis" to PHI, which is clearly distinguishable from the narrow category of conduits with only transient access, which was intended to exclude only those entities providing mere courier services such as the U.S. Postal Service or United Parcel Service and their electronic equivalents such as internet service providers (ISPs) providing mere data transmission services.[334] In addition, the Department considered clarifying that the definition of health care operations includes activities for purposes of providing accommodations for persons with disabilities; however, the Department believes the permission to disclose PHI for health care operations would be too narrow to fully address circumstances in which a covered entity's workforce member needs to disclose PHI to a communications assistant helping another entity's workforce member to perform activities of the second entity. Thus, the Department believes it is necessary to propose an express permission to disclose PHI to TRS communications assistants without a business associate agreement.

---

[333] *See* OCR's guidance on conduits, available at https://www.hhs.gov/hipaa/for-professionals/faq/245/are-entities-business-associates/index.html and https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html#_ftn14.

[334] *See* 78 FR 5566, 5571(January 25, 2013), available at https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

5. Request for Comments on Costs and Benefits

The Department requests comments on all of the assumptions and analyses within the cost-benefits analysis. The Department also requests comments on whether there may be other indirect costs and benefits resulting from the proposed changes in the proposed rule, and welcomes additional information that may help quantify those costs and benefits.

B. Executive Order 13771

Executive Order 13771 (January 30, 2017) declares that "it is important that for every one new regulation issued, at least two prior regulations be identified for elimination," and that "whenever an executive department or agency (agency) publicly proposes for notice and comment or otherwise promulgates a new regulation, it shall identify at least two existing regulations to be repealed." The Department intends to comply as necessary with Executive Order 13771 at the time a final rule is issued.

The Department believes this proposed rule will be deemed an Executive Order 13771 deregulatory action when finalized. The Department estimates that this final rule would generate $0.6 billion in net annualized savings at a 7% discount rate (discounted relative to year 2016, over a perpetual time horizon, in 2016 dollars).

EO 13771 Summary Table (in millions of 2016 dollars, Over an Infinite Time Horizon)

Item	Primary Estimate (7%)
Present Value of Costs	$1,122,453,212
Present Value of Cost Saving	$9,209,556,752
Present Value of Net Costs	-$8,087,103,541
Annualized Costs	$78,571,725
Annualized Cost Savings	$644,668,973
Annualized Net Costs	-$566,097,248

C. Regulatory Flexibility Act

The Department has examined the economic implications of this proposed rule as required by the Regulatory Flexibility Act (5 U.S.C. sections 601-612). If a rule has a

significant economic impact on a substantial number of small entities, the Regulatory Flexibility Act (RFA) requires agencies to analyze regulatory options that would lessen the economic effect of the rule on small entities. For purposes of the RFA, small entities include small businesses, nonprofit organizations, and small governmental jurisdictions. The Act defines "small entities" as (1) a proprietary firm meeting the size standards of the Small Business Administration (SBA), (2) a nonprofit organization that is not dominant in its field, and (3) a small government jurisdiction of less than 50,000 population. Because 90 percent or more of all health care providers meet the SBA size standard for a small business or are nonprofit organization, the Department generally treats all health care providers as small entities for purposes of performing a regulatory flexibility analysis. The SBA size standard for health care providers ranges between a maximum of $8 million and $41.5 million in annual receipts, depending upon the type of entity.[335]

With respect to health insurers, the SBA size standard is a maximum of $41.5 million in annual receipts, and for third party administrators it is $35 million.[336] While some insurers are classified as nonprofit, it is possible they are dominant in their market. For example, a number of Blue Cross/Blue Shield insurers are organized as nonprofit entities; yet they dominate the health insurance market in the states where they are licensed.

For the reasons stated below, it is not expected that the cost of compliance would be significant for small entities. Nor is it expected that the cost of compliance would fall disproportionately on small entities. Although many of the covered entities affected by the proposed rule are small entities, they would not bear a disproportionate cost burden compared to the other entities subject to the proposed rule.

---

[335] *See* U.S. Small Business Administration, *Table of Small Business Size Standards* (Version 2019), available at https://www.sba.gov/document/support--table-size-standards.

The projected costs and savings are discussed in detail in the regulatory impact analysis. The Department does not view this as a burden because the result of the changes would be a net average estimated cost per covered entity of $150 in year one, followed by an average of $1,065 of estimated annual savings thereafter, for an average estimated total savings over five years of approximately $4,110 per covered entity. Thus, this proposed rule would not impose net costs on small entities, and the Secretary certifies that this proposed rule would not result in a significant negative impact on a substantial number of small entities.

D. Unfunded Mandates Reform Act

Section 202(a) of The Unfunded Mandates Reform Act of 1995 (URMA) (section 202(a)) requires the Department to prepare a written statement, which includes an assessment of anticipated costs and benefits, before issuing "any rule that includes any federal mandate that may result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more (adjusted annually for inflation) in any one year." Section 202 of UMRA also requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates require spending that may result in expenditures in any one year of $100 million in 1995 dollars, updated annually for inflation. In 2019, that threshold is approximately $154 million. This proposed rule is not anticipated to have an effect only on state, local, or tribal governments, in the aggregate, of $154 million or more, adjusted for inflation. The Department believes that the proposed rule would impose mandates on the private sector that would result in an expenditure of $154 million in at least one year. As the estimated costs to private entities alone may exceed the $154 million threshold, UMRA requires the Department to prepare an analysis of the costs and benefits of the rule. The Department

has already done so, in accordance with Executive Orders 12866 and 13563, and presents this analysis in the preceding sections.

E. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. The Department does not believe that this rulemaking would have any federalism implications.

The federalism implications of the Privacy and Security Rules were assessed as required by Executive Order 13132 and published as part of the preambles to the final rules on December 28, 2000 (65 FR 82462, 82797), February 20, 2003 (68 FR 8334, 8373), and January 25, 2013 (78 FR 5566, 5686). Regarding preemption, the preamble to the final Privacy Rule explains that the HIPAA statute dictates the relationship between state law and Privacy Rule requirements, and the Rule's preemption provisions do not raise federalism issues. The HITECH Act, at section 13421(a), provides that the HIPAA preemption provisions shall apply to the HITECH Act provisions and requirements.

The Department anticipates that the most significant direct costs on state and local governments would be the cost for state and local government-operated covered entities to revise policies and procedures, including drafting, printing, and distributing NPPs for individuals with first-time health encounters, which would include the cost of mailing these notices for state health plans, such as Medicaid. The regulatory impact analysis above addresses these costs in detail.

In considering the principles in and requirements of Executive Order 13132, the Department has determined that these proposed modifications to the Privacy Rule would not significantly affect the rights, roles, and responsibilities of the states.

F. Assessment of Federal Regulation and Policies on Families

Section 654 of the Treasury and General Government Appropriations Act of 1999 requires federal departments and agencies to determine whether a proposed policy or regulation could affect family well-being. If the determination is affirmative, then the Department or agency must prepare an impact assessment to address criteria specified in the law. The Department believes that these regulations would positively impact the ability of individuals and families to coordinate treatment and payment for health care by increasing access to PHI, particularly for families to participate in the care and recovery of their family members experiencing SMI, SUD, or health emergencies. These changes must necessarily be carried out by the Department through the modification of the Privacy Rule. The Department does not anticipate negative impacts on family well-being as a result of this regulation.

G. Paperwork Reduction Act of 1995

Under the Paperwork Reduction Act of 1995 (PRA) (Pub. L. 104-13), agencies are required to submit to the Office of Management and Budget (OMB) for review and approval any reporting or record-keeping requirements inherent in a proposed or final rule, and are required to publish such proposed requirements for public comment. The PRA requires agencies to provide a 60-day notice in the ***Federal Register*** and solicit public comment on a proposed collection of information before it is submitted to OMB for review and approval. To fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that the Department solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;

2. The accuracy of the agency's estimate of the information collection burden;

3. The quality, utility, and clarity of the information to be collected; and

4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

The PRA requires consideration of the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section. The Department explicitly seeks, and will consider, public comment on its assumptions as they relate to the PRA requirements summarized in this section. To comment on the collection of information or to obtain copies of the supporting statements and any related forms for the proposed paperwork collections referenced in this section, email your comment or request, including your address and phone number to *Sherrette.Funn@hhs.gov,* or call the Reports Clearance Office at (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above email address within 60 days.

In this NPRM, the Department is revising certain information collection requirements and, as such, is revising the information collection last prepared in 2019 and previously approved under OMB control # 0945-0003. The revised information collection describes all new and adjusted information collection requirements for covered entities pursuant to the implementing regulation for HIPAA at 45 CFR Parts 160 and 164, the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules.

The estimated annual burden presented by the proposed regulatory modifications in the first year of implementation, including one-time and ongoing burdens, is 9,577,626 burden hours at a cost of $996,122,087 (including capital costs of $242,398), reduced by first year annual costs savings of $880,087,888, for an estimated first year net cost of $116,034,199 and $880,087,888 of estimated annual cost savings in years two through five, resulting in annual net cost savings of $824,604,205. The overall total burden for respondents to

comply with the information collection requirements of all of the HIPAA Privacy, Security, and Breach Notification Rules, including one-time and ongoing burdens presented by proposed program changes, is 952,089,673 burden hours at a cost of $93,937,597,924, plus $118,269,943 in capital costs for a total estimated annual burden of $94,055,867,867 in the first year following the effective date of the final rule, assuming all changes are adopted as proposed. Details describing the burden analysis for the proposals associated with this NPRM are presented below.

1. Explanation of Estimated Annualized Burden Hours

Due to the number of proposed changes to the Privacy Rule that would affect the information collection, the Department presents in separate tables, in Section V.G.2 below, the collections that reflect estimates to existing burdens, new and previously unquantified ongoing burdens, and new one-time burdens. Below is a summary of the significant program changes and adjustments made since the 2019 information collection. These program changes and adjustments form the bases for the burden estimates presented in the tables that follow:

Adjusted Estimated Annual Burdens of Compliance

(1) Increasing the number of covered entities from 700,000 to 774,331 based on program change;

(2) Increasing the number of access requests under 45 CFR 164.524 from 200,000 to 2,460,000 annually based on program change;

(3) Increasing the estimated burden hours for responding to access requests under 45 CFR 164.524 from 3 to 5 minutes per request due to program change and allocating 1 minute as uncompensated;

(4) Increasing the burden hours by a factor of two for responding to individuals' requests for restrictions on disclosures of their protected health information under 45 CFR 164.522 due to program change;

(5) Newly estimating the burdens resulting from the pre-existing, ongoing requirement for covered entities to make minimum necessary evaluations under 45 CFR 164.514 before using or disclosing protected health information for payment and health care operations purposes (and for using protected health information for treatment) in the amount of 18 hours annually per covered entity, and decrease the annual minimum necessary burden to by 4 hours per covered entity due to program change, resulting in a total ongoing annual burden of 14 hours per covered entity;

(6) Recognizing for the first time burdens associated with providing electronic copies of PHI to third parties designated by individuals under 45 CFR 164.524 in the amount of 2 minutes per request for 25 percent of 615,000 such requests received annually;

(7) Recognizing for the first time burdens associated with providing electronic copies of PHI to health plans and health care providers as third parties designated by individuals under 45 CFR 164.524 in the amount of 4 minutes per request for 25 percent of 615,000 such requests received annually; and

(8) Decreasing the estimated burden for disseminating the Notice of Privacy Practices and obtaining an acknowledgement of receipt under 45 CFR 164.520, from 3 minutes to 1 minute and 15 seconds due to program change.

New Burdens Resulting from Program Changes

In addition to these changes, the Department added new burdens as a result of program changes:

(1) An annualized burden of 10 minutes per covered entity for posting an updated Notice of Privacy Practices due to program changes;

(2) An annualized burden of 3.5 minutes per request for submitting an access request for an individual to another provider for an estimated 92,250 annual requests;

(3) An annualized 10-minute burden per covered entity for posting an access and authorization fee schedule online under 45 CFR 164.525;

(4) An annualized 7-minute burden for each of an estimated 6,130,000 annual requests from individuals to discuss their direct treating health care provider's Notice of Privacy Practices under 45 CFR 164.520;

(5) An annualized three-minute burden for each of an estimated 73,800 annual requests from individuals for an individualized estimate of the fees to provide copies of requested protected health information under 45 CFR 164.525;

(6) An annualized one-minute burden for each of an estimated 24,600 annual requests from individuals for an itemized list of charges for their requested copies of protected health information under 45 CFR 164.525;

(7) A one-time burden of 6 hours and 55 minutes for each covered entity to update its policies and procedures under 45 CFR 164.530 due to program changes; and;

(8) A one-time burden of 4 hours and 40 minutes for each covered entity to update the content of its HIPAA training program under 45 CFR 164.530 and a related one-time burden of 7 additional minutes of workforce member time spent in training on 45 CFR 164.524 per covered entity.

2. Tables Demonstrating Estimated Burden Hours

Ongoing Annual Burdens of Compliance with the Rules

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
160.204	Process for Requesting Exception Determinations — states or persons	1	1	1	16[a]	16
164.308	Contingency Plan—Testing and Revision	1,774,331	1	1,774,331	8	14,194,648

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.308	Contingency Plan—Criticality Analysis	1,774,331	1	1,774,331	4	7,097,324
164.310	Maintenance Records	1,774,331	12	21,291,972	6	127,751,832
164.314	Security Incidents – Business Associate reporting of non-breach incidents to Covered Entities	1,000,000	12	12,000,000	20	240,000,000
164.316	Risk Analysis—Documentation, 164.308	1,774,331[b]	1	1,774,331	10[C]	17,743,310
164.316	Information System Activity Review—Documentation, 164.308	1,774,331	12	21,291,972	.75	15,968,979
164.316	Security Reminders—Periodic Updates, 164.308	1,774,331	12	21,291,972	1	21,291,972
164.316	Security Incidents—Other than breaches—Documentation, 164.308	1,774,331	52	92,265,212	5	461,326,060
164.316	Documentation—Review and Update, 164.306	1,774,331	1	1,774,331	6	10,645,986
164.404	Individual Notice—Written and E-mail Notice—Drafting	58,482[d]	1	58,482	.5	29,241
164.404	Individual Notice—Written and E-mail Notice—Preparing and documenting notification	58,482	1	58,482	.5	29,241
164.404	Individual Notice—Written and E-mail Notice—Processing and sending	58,482	1,941[e]	113,513,562	.008	908,108

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.404	Individual Notice—Substitute Notice—Posting or publishing	2,746[f]	1	2,746	1	2,746
164.404	Individual Notice—Substitute Notice—Staffing toll-free number	2,746	1	2,746	3.42[g]	9,391
164.404	Individual Notice—Substitute Notice—Individuals' voluntary burden to call toll-free number for information	113,264[h]	1	113,264	.125[i]	14,158
164.406	Media Notice	267[j]	1	267	1.25	334
164.408	Notice to Secretary—Notice for breaches affecting 500 or more individuals	267	1	267	1.25	334
164.408	Notice to Secretary—Notice for breaches affecting fewer than 500 individuals	58,215[k]	1	58,215	1	58,215
164.410	Business Associate notice to Covered Entity—500 or more individuals affected	20	1	20	50	1,000
164.410	Business Associate notice to Covered Entity— Less than 500 individuals affected	1,165	1	1,165	8	9,320
164.414	500 or More Affected Individuals—Investigating and	267	1	267	50	13,350

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	documenting breach					
164.414	Less than 500 Affected Individuals—Investigating and documenting breach	2,479 (breaches affecting 10-499 individuals)	1	2,479	8	19,832
		55,736 (breaches affecting <10 individuals)	1	55,736	4	222,944
164.504	Uses and Disclosures – Organizational Requirements	774,331	1	774,331	0.083333333	64,528
164.508	Uses and Disclosures for Which Individual Authorization is Required	774,331	1	774,331	1	774,331
164.512	Uses and Disclosures for Research Purposes	113,524[l]	1	113,524	0.08333333	9,460
164.520	Notice of Privacy Practices for Protected Health Information—Health plans—Periodic distribution of NPPs by paper mail	100,000,000[m]	1	100,000,000	0.00416666 [1 hour per 240 notices]	416,667
164.520	Notice of Privacy Practices for Protected Health Information—Health plans—Periodic distribution of NPPs by electronic mail	100,000,000	1	100,000,000	0.00278333 [1 hour per 360 notices]	278,333
164.520	Notice of Privacy Practices for Protected Health Information—Health care providers—Dissemination	613,000,00[n]	1	613,000,000	0.02083333[o]	12,770,833

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.522	Rights to Request Privacy Protection for Protected Health Information	40,000[p]	1	40,000	0.05	2,000
164.524	Access of Individuals to Protected Health Information—Copies of PHI	1,230,000[q]	1	1,230,000	0.0166667[r]	20,500
164.526	Amendment of Protected Health Information—Requests	150,000	1	150,000	0.08333333	12,500
164.526	Amendment of Protected Health Information—Denials	50,000	1	50,000	0.08333333	4,167
164.528	Accounting for Disclosures of Protected Health Information	5,000[s]	1	5,000	0.05	250
TOTAL						931,691,910

New or Previously Unquantified Ongoing Burdens of Compliance, Annualized Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.514	Minimum necessary evaluations for treatment, payment, and health care operations—Uses and disclosures	774,331	1	774,331	14[t]	10,840,634[u]
164.520	Notice of Privacy	6,130,000	1	6,130,000[v]	0.1166667	715,167

New or Previously Unquantified Ongoing Burdens of Compliance, Annualized Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	Practices for Protected Health Information — Right to discuss privacy practices					
164.524	Access of Individuals to Protected Health Information —Provider submitting individual's access request to another provider or plan	92,250	1	92,250[w]	.0583333[x]	5,381
164.524	Access of Individuals to Protected Health Information —Directing copies of ePHI to health plans and providers	153,750[y]	1	153,750	0.0666666	10,250
164.524	Access of Individuals to Protected Health Information —Directing copies of ePHI to third parties other than health plans and providers	153,750[z]	1	153,750	0.0333333	5,125
164.525	Notice of Access and Authorization Fees—	73,800	1	73,800[aa]	0.05	3,690

New or Previously Unquantified Ongoing Burdens of Compliance, Annualized Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	Individual-ized estimates					
164.525	Notice of Access and Authorization Fees—Item-ized list of charges for copies	24,600[bb]	1	24,600	0.0166667	410
TOTAL						**11,580,657**

a. The figures in this column are averages based on a range. Small entities may require fewer hours to conduct certain compliance activities, particularly with respect to Security Rule requirements, while large entities may spend more hours than those provided here due to their size and complexity.
b. This estimate includes 774,331 estimated covered entities and 1 million estimated business associates. The Omnibus HIPAA Final Rule burden analysis estimated that there were 1-2 million business associates. However, because many business associates have business associate relationships with multiple covered entities, the Department believes the lower end of this range is more accurate.
c. The figures in this column are averages based on a range. Small entities may require fewer hours to conduct certain compliance activities, particularly with respect to Security Rule requirements, while large entities may spend more hours than those provided here due to their size and complexity.
d. Total number of breach reports submitted to OCR in 2015. Breaches reported to OCR in 2015 affected more individuals than have been affected by breaches reported in each subsequent year; therefore, the Department bases its burden estimates on 2015 data to ensure that it fully accounts for the annual burdens of the Breach Notification Rule.
e. Average number of individuals affected per breach incident reported in 2015.
f. This number includes all 267 large breaches and all 2,479 breaches affecting 10-499 individuals that were reported to OCR in 2015. As the Department stated in the preamble to the Omnibus HIPAA Final Rule, although some breaches involving fewer than 10 individuals may require substitute notice, it believes the costs of providing such notice through alternative written means or by telephone is negligible.
g. This assumes that 10% of the sum of (a) all individuals affected by large breaches in 2015 (113,250,136) and (b) 5% of individuals affected by small breaches (0.05 x 285,413 = 14,271) will require substitute notification. Thus, the Department calculates 0.10 x (113,250,136 + 14,271) = 11,326,441 affected individuals requiring substitute notification for an average of 4,125 affected individuals per such breach. The Department assumes that 1% of the affected individuals per breach requiring substitute notice annually will follow up with a telephone call, resulting in 41.25 individuals per breach calling the toll-free number. The Department assumes that call center staff will spend 5 minutes per call, with an average of 41 affected individuals per breach requiring substitute notice, resulting in 3.42 hours per breach spent answering calls from affected individuals.
h. As noted in the previous footnote, this number equals 1% of the affected individuals who require substitute notification (0.01 x 11,326,441).
i. This number includes 7.5 minutes for each individual who calls with an average of 2.5 minutes to wait on the line/decide to call back and 5 minutes for the call itself.
j. The total number of breaches affecting 500 or more individuals for which OCR received reports in 2015.
k. The total number of breaches affecting fewer than 500 individuals for which OCR received reports in 2015.
l. The number of entities who use and disclose PHI for research purposes.

New or Previously Unquantified Ongoing Burdens of Compliance, Annualized Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours

m. As in the Department's previous submission, it assumes that half of the approximately 200,000,000 individuals insured by covered health plans will receive the plan's NPP by paper mail, and half will receive the NPP by electronic mail.
n. The Department estimates that each year covered health care providers will have first-time visits with 613 million individuals, to whom the providers must give an NPP.
o. This represents 1 minute and fifteen seconds (75/3,600) to disseminate the NPP and eliminates the 1 minute and 45 seconds previously allocated for obtaining the signed patient acknowledgement.
p. The Department doubled the estimated number of requests for confidential communications or restrictions on disclosures per year due to the combined effect of changes to the minimum necessary standard and the information blocking provisions of the ONC Cures Act Final Rule.
q. The Department has increased our estimate of the number of requests from individuals for copies of their PHI that covered entities annually provide to them directly to 1,230,000.
r. This represents an estimated average of 1 minute per request which is not chargeable as a fee to the individual.
s. The Department estimates that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their PHI.
t. The figures in this column are averages based on a range. Small entities may require fewer hours to conduct certain compliance activities, particularly with respect to Security Rule requirements, while large entities may spend more hours than those provided here due to their size and complexity.
u. This represents a previously unacknowledged annual burden of 18 hours per covered entity for making minimum necessary evaluations for purposes of treatment, payment, and health care operations uses and disclosures, reduced by an estimated 4 burden hours annually per covered entity (or 3,097,324 total) as a result of the proposed changes to the minimum necessary standard combined with proposed changes to the definition of health care operations.
v. 1% of an estimated 613 million new patient encounters annually.
w. 15% of 615,000 annual access requests to direct electronic copies of ePHI to health plans and providers as third parties under the right of access.
x. This represents 3.5 minutes for a medical assistant to obtain the needed information and submit it for the individual.
y.This represents one-fourth of the estimated 615,000 annual requests under the right of access for copies of ePHI directed to health plans and health care providers as third parties and reflects only the labor burden for such requests for ePHI to be sent via other than an internet-based method (e.g., on electronic media and mailed to the recipient).
z. This represents one-fourth of the estimated 615,000 annual requests for copies of ePHI directed to third parties and reflects only uncompensated the labor burden for requests for ePHI to be sent via other than an internet-based method (e.g., on electronic media and mailed to the recipient).
aa. 3% of an estimated 2.46 million annual access requests for copies of PHI.
bb. 1% of an estimated 2.46 million annual access requests for copies of PHI.

New One-time Burdens of Compliance

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.520	Notice of Privacy Practices for	774,331	1	774,331	0.1666667[a]	129,055

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	Protected Health Information—Post updated notice online					
164.525	Notice of Fees for Copies of PHI—Post fee schedule online	774,331	1	774,331	.16666667	129,055
164.530	Administrative Requirements—Training Minimum necessary, 164.514	774,331	1	774,331	1	774,331
164.530	Administrative Requirements—Training— Right of access, 164.525, and fee estimates, 164.525—Updated training content	774,331	1	774,331	2.5	1,935,828
164.530	Administrative Requirements—Training—Access—Workforce member time in training, 164.524	774,331	1	774,331	0.116666667	90,339
164.530	Administrative Requirements—Training—Disclosing PHI under164.510; uses and disclosures to prevent harm, 164.512	768,169	1	768,169	0.6666667	512,113
164.530	Administrative Requirements—Training—Disclosures for Uniformed Services, & disclosures to Telecommunications Relay Services for treatment, payment and health care operations, 164.512	774,331	1	774,331	0.25	193,583
164.530	Administrative Requirements—Training—Notice of privacy practices, changes	774,331	1	774,331	0.0833333	64,528

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	in content & right to discuss privacy practices, 164.520					
164.530	Administrative Requirements —Training —Verification of identity, 164.514	38,717[b]	1	38,717	0.1666667	6,453
164.530	Administrative Requirements —Policies & Procedures— Individual care coordination and case management , 164.501 & 164.502, minimum necessary, 164.514, and social services agencies for care coordination, 164.506	774,331	1	774,331	1.25	967,914
164.530	Administrative Requirements—Policies & Procedures— Right of access, 164.524, & fee estimates, 164.525	774,331	1	774,331	3	2,322,993
164.530	Administrative Requirements—Policies & Procedures— Disclosing PHI under 164.510; uses and disclosures to prevent harm, 164.512(j)	768,169[c]	1	768,169	1	768,169
164.530	Administrative Requirements—Policies & Procedures— Revising the Notice of Privacy Practices, 164.520	774,331	1	774,331	1	774,331
164.530	Administrative Requirements —Policies & Procedures— Disclosures for Uniformed Services & Telecommuni-	774,331	1	774,331	0.16666667[d]	129,055

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	cations Relay Services, 164.512					
164.530	Administrative Requirements—Polices & Procedures—Identity verification changes, 164.514	38,717[e]	1	38,717	0.5	19,358
TOTAL				10,131,413		**8,817,103[f]**

a. The figures in this column are averages based on a range. Small entities may require fewer hours to conduct certain compliance activities, particularly with respect to Security Rule requirements, while large entities may spend more hours than those provided here due to their size and complexity.
b. This represents 5% of all covered entities.
c. This represents all health care providers.
d. This equates to 10 minutes.
e. This represents 5 percent of all covered entities.
f. Total may not add up due to rounding.

List of Subjects

45 CFR Part 160

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health professions, Health records, Hospitals, Investigations, Medicaid, Medical research, Medicare, Penalties, Privacy, Reporting and record keeping requirements, Security.

45 CFR Part 164

Administrative practice and procedure, Computer technology, Drug abuse, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health professions, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements, Security.

Proposed Rule

For the reasons stated in the preamble, the Department of Health and Human Services proposes to amend 45 CFR Subtitle A, Subchapter C, Parts 160 and 164 as set forth below:

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 160 is revised to read as follows:

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); 5 U.S.C. 552; secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279 (42 U.S.C. 17921, 17931-17954); and sec. 1104 of Pub. L. 111-148, 124 Stat. 146-154.

2. Amend § 160.103, by adding new paragraph (4)(v) to the definition of "Business associate" to read as follows:

§ 160.103 Definitions

* * * * *

Business associate * * *

(4) * * *

(v) A provider of Telecommunications Relay Service, as defined in 47 U.S.C. § 225(a)(3), with respect to enabling communications through services regulated under 47 CFR Part 64.

* * * * *

PART 164—SECURITY AND PRIVACY

3. The authority citation for part 164 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279 (42 U.S.C. 17921, 17931-17954).

4. Amend § 164.501 by:

a. Adding in alphabetical order a definition for "Electronic health record";
b. Revising paragraph (1) of the definition of "Health care operations"; and
c. Adding in alphabetical order a definition for "Personal health application".

The additions and revision read as follows:

§ 164.501 Definitions.

* * * * *

Electronic health record means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and their staff. Such clinicians shall include, but are not limited to, health care providers that have direct treatment relationships with individuals as defined at § 164.501, such as physicians, nurses, pharmacists, and other allied health professionals. For purposes of this paragraph, "health-related information on an individual" covers the same

scope of information as the term *individually identifiable health information* as defined at § 160.103.

* * *

Health care operations * * *

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

* * * * *

Personal health application means an electronic application used by an individual to access health information about that individual, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.

* * * * *

5. Amend § 164.502 by:

a. Revising paragraph (a)(4)(ii) and (a)(5)(ii)(B)(*2*)(*vi*)
b. Revising paragraph (b)(2)(i);
c. Adding paragraph (b)(2)(vii);
d. Revising paragraph (g)(3)(ii)(C); and
e. Adding new paragraph (k).

The revisions read as follows:

§ 164.502 Uses and disclosures of protected health information: General Rules.

(a) * * *

(4) * * *

(ii) To the covered entity or, when specified in the business associate agreement, to the individual or the individual's designee, as necessary to satisfy a covered entity's obligations with respect to §§ 164.524(c)(2)(ii) or 164.524(d)(1).

(5) * * *

(ii) * * *

(B) * * *

(*2*) * * *

(*vi*) To an individual, or a third party designated by the individual, when requested under §§ 164.524 or 164.528.

* * *

(b) * * *

(2) * * *

(i) Disclosures to or requests by a health care provider for treatment, including for care coordination and case management activities with respect to an individual;

* * *

(vii) Disclosures to or requests by a health plan for care coordination and case management activities with respect to an individual.

* * * * *

(g) * * *

(3) * * *

(ii) * * *

(C) Where the parent, guardian, or other person acting *in loco parentis,* is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under state or other law, including case law, a covered entity may provide access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with state or other applicable law, provided that such decision must be made by a licensed health care professional, based on a good faith belief that providing access is in the best interests of the individual.

* * * * *

(k) Standard: Good Faith – Presumption of Compliance. When using or disclosing protected health information as provided in §§ 164.502(g)(3)(ii)(C); 164.510(a)(3)(i)(B); 164.510(b)(2)(iii); 164.510(b)(3); and 164.514(h)(2)(iv), a covered entity is presumed to have complied with the good faith requirement, absent evidence that the covered entity acted in bad faith.

* * * * *

6. Amend § 164.506, by adding new paragraph (c)(6) to read as follows:

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

* * * * *

(c) * * *

(6) A covered entity may disclose an individual's protected health information to a social services agency, community-based organization, home and community based services provider, or similar third party that provides health or human services to specific individuals for individual-level care coordination and case management activities (whether such activities constitute treatment or health care operations as those terms are defined in § 164.501) with respect to that individual.

* * * * *

7. Amend § 164.510 by revising paragraphs (a)(3)(i)(B), (b)(2)(iii), and (b)(3) to read as follows.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

* * * * *

(a) * * *

(3) * * *

(i) * * *

(B) In the individual's best interests based on a good faith belief of the covered health care provider.

* * * * *

(b) * * *

(2) * * *

(iii) Reasonably infers from the circumstances, based on a good faith belief, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, based on a good faith belief that the disclosure is in the best interests of the individual, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or that is needed for notification purposes. A covered entity may make reasonable inferences of the individual's best interests in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

* * * * *

8. Amend § 164.512 by:

a. Revising paragraph (j)(1)(i)(A);
b. Adding paragraphs (j)(5) through (6);

c. Revising the heading for paragraph (k)(1);
d. Revising paragraphs (k)(1)(i) introductory text, (k)(1)(i)(A), and (k)(1)(ii); and
e. Adding paragraph (m).

The revisions and additions read as follows**:**

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

* * * * *

(j) * * *

(1) * * *

(i) (A) Is necessary to prevent a serious and reasonably foreseeable harm, or lessen a serious and reasonably foreseeable threat, to the health or safety of a person or the public; and

* * *

(5) "Reasonably foreseeable" means that an ordinary person could conclude that a threat to health or safety exists and that harm to health or safety is reasonably likely to occur if a use or disclosure is not made, based on facts and circumstances known at the time of the disclosure.

(6) When a covered health care provider (or a member of the workforce of the covered health care provider) that has specialized training, expertise, or experience in assessing an individual's risk to health or safety—such as a licensed mental or behavioral health professional—determines that it is appropriate to use or disclose protected health information under paragraph (j)(1)(i)(A) of this section, such determination will be entitled to heightened deference if the determination is related to facts and circumstances about which the covered entity (or a member of its workforce) has such training, expertise, or experience.

* * * * *

(k) * * *

(1) *Uniformed Services and veterans activities—*

(i) *Uniformed Services personnel.* A covered entity may use and disclose the protected health information of individuals who are Uniformed Services personnel for activities deemed necessary by appropriate Uniformed Services command authorities to assure the proper execution of the Uniformed Services mission, if the appropriate Uniformed Services authority has published by notice in the FEDERAL REGISTER the following information:

(A) Appropriate Uniformed Services command authorities; and

* * * * *

(ii) Separation or discharge from Uniformed Service. A covered entity that is a component of the Departments of Defense, Homeland Security, Commerce, or Health and Human Services may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Uniformed Services upon the separation or discharge of the individual from Uniformed Service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

* * * * *

(m) *Standard: Disclosures to Telecommunications Relay Service.* A covered entity may disclose protected health information to a Telecommunications Relay Service Communications Assistant, as defined at 47 CFR 64.601(a)(10), as necessary to conduct covered functions.

* * * * *

9. Amend § 164.514 by:

a. Revising paragraph (h)(2)(iv); and
b. Adding paragraph (h)(2)(v).

The revision and addition read as follows:

§ 164.514 Other requirements related to uses and disclosures of protected health information.

* * * * *

(h) * * *

(2) * * *

(iv) *Exercise of good faith.* The verification requirements of this paragraph are met if the covered entity acts on a good faith belief in making a use or disclosure in accordance with § 164.510 or making a disclosure in accordance with § 164.512(j).

(v) *Exercise of individual rights.* A covered entity may not impose unreasonable verification measures on an individual that would impede the individual from exercising a right under this part. An unreasonable measure is one that causes an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable for the covered entity. Practicability considerations include a covered entity's technical capabilities, its obligations to protect the privacy of protected health information under § 164.530(c), the security of electronic protected health information under § 164.306, and the costs of implementing measures that are more convenient for individuals. Examples of unreasonable measures include requiring an individual to provide proof of identity in person when a method for remote verification is practicable for the covered entity and more convenient for the individual, or requiring an individual to obtain notarization of the individual's signature on a written request to exercise the individual right.

10. Amend § 164.520 by:

a. Revising paragraphs (b)(1)(i) and (b)(1)(iv)(C);

b. Adding new paragraph (b)(1)(iv)(G);
c. Revising paragraph (b)(1)(vii);
d. Adding new paragraph (b)(2)(iii);
e. Removing paragraph (c)(2)(ii);
f. Redesignating paragraph (c)(2)(iii) and (iv) paragraphs (c)(2)(ii) and (iii);
g. Revising paragraph (c)(3)(iii); and
h. Revising paragraph (e).

The revisions and additions read as follows:

§ 164.520 Notice of privacy practices for protected health information.

* * * * *

(b) * * *

(1) * * *

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed:

NOTICE OF PRIVACY PRACTICES OF [NAME OF COVERED ENTITY, AFFILIATED COVERED ENTITIES, OR ORGANIZED HEALTH CARE ARRANGEMENT, AS APPLICABLE]
THIS NOTICE DESCRIBES:

- HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED
- YOUR RIGHTS WITH RESPECT TO YOUR MEDICAL INFORMATION
- HOW TO EXERCISE YOUR RIGHT TO GET COPIES OF YOUR RECORDS AT LIMITED COST OR, IN SOME CASES, FREE OF CHARGE
- HOW TO FILE A COMPLAINT CONCERNING A VIOLATION OF THE PRIVACY, OR SECURITY OF YOUR MEDICAL INFORMATION, OR OF YOUR RIGHTS CONCERNING YOUR INFORMATION, INCLUDING YOUR RIGHT TO INSPECT OR GET COPIES OF YOUR RECORDS UNDER HIPAA.

YOU HAVE A RIGHT TO A COPY OF THIS NOTICE (IN PAPER OR ELECTRONIC FORM) AND TO DISCUSS IT WITH [ENTER NAME OR TITLE AT [PHONE AND EMAIL] IF YOU HAVE ANY QUESTIONS.

* * * * *

(iv) * * *

(C) The right of access to inspect and obtain a copy of protected health information at limited cost or, in some cases, free of charge; and the right to direct a covered health

care provider to transmit an electronic copy of protected health information in an electronic health record to a third party, as provided by § 164.524;

* * * * *

(G) The right to discuss the notice with a designated contact person identified by the covered entity pursuant to § 164.520(b)(vii);

* * * * *

(vii) *Contact.* The notice must contain the name or title and telephone number and email for a designated person who is available to provide further information and answer questions about the covered entity's privacy practices, as required by § 164.530(a)(1)(ii).

* * * * *

(2) * * *

(iii) A covered entity may provide in its notice information about how an individual who seeks to direct protected health information to a third party, when the protected health information is not in an electronic health record and/or is in a non-electronic format, can instead obtain a copy of protected health information directly under § 164.524 and send the copy to the third party themselves, or request the covered entity to send a copy of protected health information to a third party using a valid authorization under § 164.508.

* * * * *

(c) * * *

(2) * * *

(ii) If the covered entity health care provider maintains a physical service delivery site:

* * * * *

(3) * * *

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

* * * * *

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity.

* * * * *

11. Amend § 164.524 by:

a. Redesignating paragraphs (a)(1) introductory text and (a)(1)(i) and (ii) as paragraphs (a)(1)(i) and (a)(1)(i)(A) and (B), respectively;

b. Adding new paragraph (a)(1)(ii);

c. Revising paragraph (a)(2) introductory text;

d. Revising paragraph (a)(3) introductory text;

e. Removing paragraph (a)(4);

f. Redesignating paragraph (b)(1) as paragraph (b)(1)(i);

g. Designating the second sentence of newly redesignated paragraph (b)(1)(i) as paragraph (b)(1)(ii) and revising newly designated paragraph (b)(1)(ii);

h. Revising paragraph (b)(2)(i) introductory text;

i. In paragraph (b)(2)(i)(B), removing "paragraph (d)" and adding in its place "paragraph (e)";

j. In paragraph (b)(2)(ii), removing "30 days" and adding in its place "15 calendar days";

k. In paragraph (b)(2)(ii)(A), removing the word "and" at the end;

l. In paragraph (b)(2)(ii)(B), removing the period at the end and adding in its place "; and";

m. Adding paragraph (b)(2)(ii)(C) and (b)(2)(iii)

n. Redesignating paragraphs (c)(2)(iii) introductory text and (c)(2)(iii)(A) and (B) as paragraphs (c)(2)(iv)(A) introductory text and (c)(2)(iv)(A)(*1*) and (*2*);

o. Adding paragraphs (c)(2)(iii) and (c)(2)(iv)(B);

p. Revising paragraphs (c)(3) and (4);

q. Redesignating paragraphs (d) and (e) paragraphs (e) and (f), respectively;

r. Revising newly redesignated paragraph (e);

s. Adding a new paragraph (d);

t. Further redesignating newly redesiganted paragraph (f)(2) as paragraph (f)(3); and

u. Adding a new paragraph (f)(2).

The revisions and additions read as follows:

§ 164.524 Access of individuals to protected health information.

(a) * * * *Standard: Access to protected health information—*

(1) *Right of access.* (i) Except as otherwise provided in paragraphs (a)(2) or (3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(A) Psychotherapy notes; and

(B) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(ii) An individual's right to inspect protected health information about the individual in a designated record set includes the right to view, take notes, take photographs, and use other personal resources to capture the information, except that a covered entity is not required to allow an individual to connect a personal device to the covered entity's information systems and may impose requirements to ensure that an

individual records only protected health information to which the individual has a right of access.

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access under paragraph (a)(1) of this section, without providing the individual an opportunity for review, in the following circumstances.

* * * * *

(3) *Reviewable grounds for denial*. A covered entity may deny an individual access under paragraph (a)(1) of this section, provided that the individual is given a right to have such denials reviewed, as required by paragraph (e)(4) of this section, in the following circumstances:

* * * * *

(b) * * *

(1) *Individual's request for access.*

(i) The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set.

(ii) The covered entity may require an individual to make a request for access in writing (in electronic or paper form), provided that it informs the individual of such a requirement and does not impose unreasonable measures that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity. For example, requiring individuals to complete a standard form containing only the information the covered entity needs to process the request is a reasonable measure because it does not cause an individual to expend unnecessary effort or expense. In contrast, examples of unreasonable measures include requiring an individual to do any of the following when a measure that is less burdensome for the individual is practicable for the entity: fill out a request form with extensive information that is not necessary to fulfill the request; obtain notarization of the individual's signature on a request form; or submit a written request only in paper form, only in person at the entity's facility, or only through the covered entity's online portal.

(2) * * *

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access as soon as practicable, but no later than 15 calendar days after receipt of the request as follows.

* * * * *

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (e) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this

section, as applicable, the covered entity may extend the time for such actions by no more than 15 calendar days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request;

(B) The covered entity may have only one such extension of time for action on a request for access; and

(C) The covered entity has implemented a policy to prioritize urgent or otherwise high priority requests (especially those relating to the health and safety of the individual or another person), so as to limit the use of a 15 calendar-day extension for such requests.

(iii) Where another federal or state law requires a covered entity to provide an individual with access to the protected health information requested in less than 15 calendar days, that shorter time period is deemed practicable under paragraph (b)(2)(i) of this section.

* * * * *

(c) * * *

(2) * * *

(iii) Where another federal or state law applicable to the covered entity requires the provision of access in a particular electronic form and format, the protected health information is deemed readily producible in such form and format under paragraphs (c)(2)(i) and (ii) of this section.

(iv)(A) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information, or may provide an explanation of the protected health information to which access has been provided, if:

(*1*) The individual agrees in advance to such a summary or explanation; and

(*2*) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(B) The covered entity must inform any individual to whom it offers to provide a summary in lieu of a copy of protected health information that the individual retains the right to obtain a copy of the requested protected health information if the individual does not agree to receive such summary. This requirement does not apply if a covered entity is offering to provide a summary in lieu of a copy of protected health information because the covered entity is denying an individual's request for a copy; however, the covered entity still must follow the denial procedures under § 164.524(e).

(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect

or obtain a copy of the protected health information, or, at the individual's request, mailing or electronically transmitting the copy of the protected health information to the individual, including by e-mail, or to or through the individual's personal health application (if a copy is readily producible to or through such application). When protected health information is readily available at the point of care in conjunction with a health care appointment, a covered health care provider is not permitted to delay the right to inspect. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access; however, such discussion shall not extend the time allowed for the covered entity to provide access.

(4) *Fees.* (i) If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(A) Labor for copying the protected health information requested by the individual, whether in non-electronic (*e.g.,* paper, film) or electronic form;

(B) Supplies for creating a non-electronic copy;

(C) Postage, when the individual has requested that a non-electronic copy, or the summary or explanation, be mailed; and

(D) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(ii) A covered entity may not impose a fee when:

(A) an individual inspects the protected health information about the individual, as described at (a)(1)(ii) of this section, or

(B) an individual accesses electronic protected health information maintained by or on behalf of the covered entity using an internet-based method such as a personal health application.

* * * * *

(d) Standard: Right to direct the transmission of certain protected health information in an electronic format to a third party--(1) An individual has a right of access to direct a covered health care provider to transmit an electronic copy of protected health information in an electronic health record directly to another person designated by the individual (a "third party"). The covered health care provider must provide access under this paragraph when the individual's request to exercise the right of access is clear, conspicuous, and specific, which may be orally or in writing (including electronically), except for:

(i) Psychotherapy notes; and

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(2) *Unreviewable grounds for denial*. A covered entity may deny an individual's request to exercise the right of access to direct a covered health care provider to transmit an electronic copy of protected health information in an electronic health record directly to a third party under paragraph (d)(1) of this section, without providing an opportunity for review, in the following circumstances:

(i) The protected health information is excepted from the right of access by paragraph (d)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to exercise of the right of access, if transmitting such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's ability to exercise of the right of access may be temporarily suspended by a covered health care provider in the course of research that includes treatment for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's request to exercise the right of access may be denied if the protected health information is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, and if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's request to exercise the right of access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and providing the copy to the third party would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial of a request to direct an electronic copy of protected health information in an electronic health record.* A covered entity may deny an individual's request under paragraph (d)(1) of this section, provided that the individual is given a right to have such denials reviewed, as required by paragraph (e)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to endanger the life or physical safety of the individual or another person; or

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to cause substantial harm to such other person.

(4) *Implementation specification: Summary or explanation prepared by covered health care provider.* (i) A covered health care provider may transmit, to a third party designated by an individual, a summary of requested protected health information in an electronic health record, in lieu of transmitting a copy of the protected health information,

or may transmit an explanation of the requested protected health information in an electronic health record in addition to such protected health information, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered health care provider for such summary or explanation.

(ii) A covered health care provider must inform any individual to whom it offers to transmit a summary in lieu of a copy of protected health information that the individual retains the right to direct an electronic copy of the requested protected health information in an EHR if the individual does not agree to receive such summary. This requirement does not apply if a covered entity is offering to provide a summary in lieu of a copy of protected health information because the covered entity is denying an individual's request for a copy; however, the covered entity still must follow the denial procedures under § 164.524(e).

(5) *Implementation specification: Timely action by the covered entity.* (i) Except as provided in paragraph (d)(5)(ii) of this section, a covered health care provider is required to provide the copy requested under paragraph (d)(1) of this section as soon as practicable but no later than 15 calendar days after receipt of the individual's request.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (d) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (e)(2) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (d)(5)(i)(A) or (B) of this section within the time required by paragraph (d)(5)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 15 calendar days, provided that:

(A) The covered entity, within the time limit set by paragraph (d)(5)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request.

(C) The covered entity has implemented a policy to prioritize urgent or otherwise high priority requests (especially those relating to the health and safety of the individual or another person), so as to limit the use of a 15 calendar-day extension for such requests.

(iii) Where another federal or state law requires a covered entity to provide an individual with an electronic copy of the protected health information in an electronic health record in less than 15 calendar days, that shorter time period is deemed practicable under paragraph (d)(5)(i) of this section.

(6) *Fees.* A covered health care provider may impose a reasonable, cost-based fee for an access request to direct an electronic copy of protected health information in an electronic health record to a third party, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual in electronic form; and

(ii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as provided in paragraph (d)(4) of this section.

(7) *Right to direct covered health care providers or plans to submit an access request*.

(i) An individual has a right of access to direct a covered health care provider or health plan ("Requester-Recipient") to submit to a covered health care provider ("Discloser") a request for an electronic copy of the individual's protected health information in an electronic health record maintained by or on behalf of the Discloser.

(ii) A Requester-Recipient must submit to the Discloser a request made by the individual, orally or in writing (including electronically), and that is clear, conspicuous, and specific, if the individual is:

A. a current or prospective new patient of the Requester-Recipient health care provider, or

B. a current enrolled member (or dependent) of the Requester-Recipient health plan.

(iii) The Requester-Recipient must submit the access request to the identified Discloser as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and any information needed to submit the request. An extension is not available for submitting the request. The Discloser must respond to the access request within the time limits in paragraph (d)(5) of this section.

(e) *Implementation specifications: Denial of access.* If a covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

* * *

(2) *Denial*. The covered entity must provide a timely, written denial to the individual. The denial must be in plain language and contain:

* * *

(ii) If applicable, a statement of the individual's review rights under paragraph (e)(4)(i) of this section, including a description of how the individual may exercise such review rights;

* * *

(3) *Other responsibility*. If the covered entity (or its business associate on the covered entity's behalf) does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested protected health information is maintained, the covered entity must inform the individual where to direct the request for access.

* * * * *

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraphs (a)(3) or (d)(3) of this section:

(i) The individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny access. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (e)(4(i) of this section.

(ii) If the individual has requested a review of a denial under paragraph (e)(4)(i) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) or (d)(3) of this section, whichever is applicable, of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(f) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals under paragraph (a) of this section;

(2) The electronic health records that are subject to the right of access to direct the transmission of an electronic copy of protected health information in an electronic health record under paragraph (d) of this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

12. Add § 164.525 to subpart E to read as follows:

§ 164.525 ***Notice of Access and Authorization Fees*****.**

(a) If a covered entity imposes fees allowed under §§ 164.524(c)(4), 164.524(d)(6) or 164.502(a)(5)(ii)(A) and 164.508(a)(4), the covered entity must provide advance notice of such fees as follows.

(1) The covered entity must post a fee schedule on its website, if it has one, and make the fee schedule available to individuals at the point of service and upon request. The fee schedule must specify:

(i) All types of access to protected health information available free of charge; and

(ii) Standard fees for:

(A) Copies of protected health information provided to individuals under § 164.524(a), with respect to all readily producible electronic and non-electronic forms and formats for such copies;

(B) Copies of protected health information in an electronic health record and directed to third parties designated by the individual under § 164.524(d), with respect to any available electronic forms and formats for such copies; and

(C) Copies of protected health information sent to third parties with the individual's valid authorization under § 164.508, with respect to any available forms and formats for such copies.

(2) Upon request, the covered entity must provide an individualized estimate of the approximate fee that may be imposed for providing a copy of the requested protected health information for any type of request covered by the fee schedule required by paragraph (1) of this section.

(3) Upon request, the covered entity must provide an individual with an itemized list of the specific charges for labor, supplies, and postage, if applicable, that constitute the total fee charged for any type of request covered by the fee schedule required by paragraph (1) of this section.

(b) A request under paragraph (a)(2) or (3) of this section shall not automatically extend the time allowed for the covered entity to provide copies of protected health information under 164.524.

* * * * *

Alex M. Azar II,

Secretary,

Department of Health and Human Services.

[FR Doc. 2020-27157 Filed: 1/19/2021 8:45 am; Publication Date: 1/21/2021]