Department of Veterans Affairs

Enterprise Data Strategy:

A Vision for the Future

January 2021

Forward

The Department of Veterans Affairs (VA) has one of the most inspiring missions in all of Government. To fulfill that mission and deliver the promise to America's Veterans, VA is implementing a series of unprecedented reforms that have put Veterans at the center of everything we do.

VA is implementing a unified electronic health record that will give clinicians from VA, the Department of Defense (DoD), and community providers a full picture of Veterans' medical history and enable faster, smarter connections between military service and health outcomes. VA is also adopting a new healthcare logistics system for acquiring medical and surgical supplies and a new integrated financial and acquisition management system to improve operational efficiency, productivity, and flexibility.

To keep the trust of our Veterans, VA must continue to innovate, upgrade and transform itself into a world-class customer focused organization. Data plays a key role in this transformation, and it is necessary to ensure that data management and analytic capabilities are aligned across the department. VA's Data Strategy is a crucial step toward building an integrated data analytics capability with greater efficiency and improved data integrity, consistency and sharing.

This strategy builds upon innovations such as the Million Veteran Program, My Health*e*Vet, and VA Informatics and Computing Infrastructure. It aligns with ongoing initiatives including, the Foundations for Evidence-Based Policymaking Act of 2018 and the Federal Data Strategy. Finally, the strategy empowers VA leaders at all levels of the organization to take bold steps to enhance the Veterans' experience, outcomes, and lifetime impact using authoritative data, trusted analytics, and a unified, comprehensive view of Veterans' needs across the enterprise.

VA employees have the honor of fulfilling our noble mission and delivering the quality health care and benefits Veterans have earned and deserve. By harnessing data as a strategic asset, VA will continue the necessary transformations to meet the needs of our Nation's Veterans, their loved ones and caregivers today and for years to come.

TABLE OF CONTENTS

TABLE OF TABLES

Context: Data as a Strategic Asset

The Department of Veterans Affairs (VA) is the largest integrated healthcare delivery network in the United States and is one of the largest beneficiary-delivery enterprises in the country. Data about Veterans, including health services and outcomes, service-connected disability payments, tuition coverage, and more is irreplaceable and essential. While VA has made progress in its data management, information sharing and analytics infrastructure, the underlying platforms remain fragmented and isolated. This strategy describes specific ways that VA could more effectively and efficiently provide superior services, experiences, and outcomes to Veterans, their families, caregivers, and survivors.

Legislation, policy, and VA mission-related goals and challenges are driving VA to re-envision its approach to better govern, manage, integrate, and extract the value of its vast holdings (Appendix C). The needs of Veterans, their families, caregivers and survivors require that VA's approach to data management must become more integrated and mature across the entire enterprise.

To this end, the Office of Enterprise Integration (OEI), in coordination with the VA's Data Governance Council (DGC), published VA's first-ever Data Management Directive, which establishes VA policy and defines roles and responsibilities for data governance and management throughout the Department. The Directive mandates that all data will be inventoried, cataloged, and systematically available for responsible sharing consistent with VA's I CARE core values, law and policy, VA Data Guiding Principles (Appendix D), and VA's Ethical Principles for Access to and Use of Veteran Data (Appendix E). The Directive emphasizes data protection, privacy and confidentiality; aligns with the appropriate standards and architectures; and ensures visibility of its quality and permitted uses. This strategy builds on the Directive and sets the vision for VA to leverage data as a strategic asset.

VA makes substantial, ongoing investments in its data, information sharing and analytics infrastructure, as well as operational investments in people, processes and technology. The DGC estimates approximately 10,000 individuals across VA have substantial participation in data management and data analytics – including generation, curation, access, reporting, and analysis. While there is some integration at the individual project, program or VA sub-component level, at the enterprise level integration is nascent. The top challenges include identifying and using authoritative data sources; poor data quality; difficulty linking data across isolated stovepipes; variations in processes, reporting, and decision support indicators; immature data management and governance; and fragmentation in tools, platform integration, technology, and process implementation.

VA is also pursuing several significant transformation initiatives with substantial data management and governance implications, including but not limited to Electronic Health Record Modernization (EHRM), Defense Medical Logistics Standard Support (DMLSS) and Financial Management Business Transformation (FMBT). Taken together, VA annual investments in people, process and technologies as they relate to data, information sharing, and analytics are substantial. Operational drivers and technology enablers, combined with statutory, strategic and policy coverage, make this the time to accelerate VA's transformation into a data-driven, learning enterprise and increase delivery of value to Veterans, their families, caregivers, and survivors.

Managing VA's data and analytics mission requires modernizing and aligning VA's people, processes, organization and technology investments. Using a federated governance structure, OEI will work in close collaboration with the Office of Information and Technology (OIT), the enterprise-wide DGC and partner organizations across VA to advance the VA Data Strategy and ensure its implementation.

VISION: Strengthening VA as a Learning Enterprise

VA exists to serve the Nation's Veterans, their families, caregivers and survivors. In 2020, VA's Veteran Population Projections have identified about 19.5 million[1] living Veterans geographically dispersed across the Nation. Our Veterans are diverse, have strong representation from racial and ethnic minorities, constitute an increasing number of women, and have a preference towards rural living compared to non-Veterans. In addition to our Veterans and their families, VA provides select services to active duty, National Guard, and Reserve members. To properly support all its customers, VA must have structured data, unstructured data and context to understand:

1. Veterans' journey, starting with recruitment as a Servicemember,
2. The cumulative lifetime impact on Veterans, their families and caregivers, and
3. Veterans' experiences across all encounters with VA.

The vision articulated by this strategy cements VA as a learning organization that manages its data well and leverages data and rigorous analytics to support VA leaders and employees at all levels in making data-driven policies and decisions to improve VA's services and value to all Veterans.

Managing VA's data as a strategic asset across its lifecycle, via the framework set in this strategy, is the necessary precondition to further strengthen VA's delivery of services and benefits to the Nation's Veterans, their families, caregivers and survivors

[1] Data comes from VA's authoritative clearinghouse, the National Center for Veterans Analysis and Statistics.

across their lifetime journeys. This ensures VA is always working towards improving Veteran experiences and health-quality outcomes and is achieving robust lifetime impact – health span, economic improvement, and dignity as measured by social connectedness. Much of VA's data are administrative, i.e., collected when Veterans apply for and receive benefits or services; received from the Department of Defense (DoD) or other partners; or developed while supporting employees or managing government resources to achieve VA's mission. Governing these vast data holdings starts with understanding, identifying and managing individual authoritative data for use in specific encounters; continues with ensuring the data are standardized and interoperable; progresses to establishing appropriate policy and secure mechanisms for effective data sharing; and culminates with testing them using key initiatives as a business case, such as suicide prevention. Finally, VA must proactively use data in business, programmatic and Veteran analytics to build clear, data-driven justifications supporting decision making, planning, budgeting and legislative proposals, and to drive continuous operational and programmatic improvements.

VA's commitment to operating a learning organization will require a new relationship with, and culture about, the use of managed and integrated, high quality data. This is complex because in addition to the human and organizational change-management aspects, it involves the creation, enhancement and orchestration of data across a complex information technology environment. It will require breaking down data stovepipes and adopting new federated governance and management frameworks.

Choice is key to Veterans – thus it is paramount that VA understands and proactively engages Servicemembers, Veterans, their families and caregivers using integrated VA (and community care) data and information reflecting a comprehensive and contextual understanding of VA's customers. That understanding must span the journey for Servicemembers and Veterans, keeping commitment to learning and lifetime impact as a core principle at both the individual and population level. Achieving this vision requires VA to redouble focus on managing VA's data as a strategic asset.

The Approach to Change: Federation

This strategy is grounded on the premise that data management, information sharing, and analytics are integral aspects of, and accelerators for, providing the best experiences and outcomes to Veterans, their families, caregivers and survivors. The approach to change is to **partner** with operational leaders across VA on VA priority transformation initiatives anchored in VA's Quadrennial Strategic Plan. Data management, information sharing, and analytics aspects or challenges of these initiatives are **priority objectives** in the data strategy. Taken together, these data-related priority objectives substantially span the data and analytics complexities discussed above, and broadly serve VA leadership across the Department every day to provide the best services to Veterans and their supporters.

The identified **priority objectives**, particularly capability and capacity planning for data-related aspects, are organized around a set of **goals** and sub-goals, subsequently described. Across the priority objectives, this decomposition, grouping like with like to gain unity of effort and economies of scale, will then be prioritized and captured in the implementation roadmap. The VA DGC serves as an integrated governance structure below the VA Operations Board (or Deputy Secretary-governance level). Its purpose is to organize the matrix between priority objectives and goals and to ensure that work is objectively measured, performance based, and effectively coordinated across the enterprise. The data governance structures and management processes developed and overseen by the DGC are key to solidifying enterprise support of data as a strategic asset at all levels across the Department.

The approach is a governed, managed **federation** of data initiatives at all organizational levels, led by designated and responsible **priority-objective champions**. Operational leaders in the Administrations and Staff Offices own their initiatives and specific implementation plans to achieve their operational objectives. Capacity and capability building under the strategic goals is federated across the missions, business initiatives, mission support, and operations; from supporting VA's data and analytics workforce from a strategic human capital perspective, to improving and streamlining data policy, information sharing processes, and analytic tradecraft and collaboration.

Under the DGC, and with the concurrence of the VA Operations Board, priority objective champions are responsible and accountable for catalyzing change by building, funding, coordinating, aligning, maintaining, and reporting on their implementation plans and efforts. The Chief Data Officer (CDO) in OEI is accountable for ensuring transparency to support required collaboration and collective accountability. In close collaboration with the DGC, the CDO will ensure unity of effort towards building and implementing data policies and directives that support efficient and effective implementation of initiatives. This approach ensures discussion and alignment of enterprise priorities and ensures coherence and cohesion of efforts within the federated model.

The work of the Department is further organized via the assignment of goals or sub-goals to senior leaders who serve in the role of **goal champions**. Progress and challenges will be reported to the VA Operations Board. The CDO will work with priority objective and goal champions, within DGC mechanisms, to document progress, opportunities, and challenges and make written recommendations on a quarterly basis.

Goals

The VA Data Strategy goals cascade from the Federal Data Strategy 2020 Action Plan requirements, the Federal Data Strategy, and the policy and responsibilities outlined in the VA Data Management Directive. They are also firmly anchored in the Data

Management Body of Knowledge (DMBoK). The five goals are to advance data stewardship, analytics, technology, workforce, and governance.

This strategy supports the Department of Veterans Affairs 2018 -2024 Strategic Plan Goal 4, which states " VA will transform business operations by modernizing systems and allocating resources more efficiently to be competitive and to provide world-class customer service to Veterans and VA employees". Although this strategy supports many of the objectives under Goal 4, it directly supports Objective 4.4, which states "VA will institutionalize data supported and performance focused decision making that improve the quality of outcomes".

These goals are intended to endure and, thus, do not refer to specific technologies, systems, or datasets. The goals apply to all forms of data collected or held by VA, including clinical, business and operational, geospatial, demographic and socioeconomic, health and genetic data. These goals will be incrementally fulfilled through and support the priority initiatives outlined in the next section of the strategy. Progress against individual goals and sub-goals are expected to support measurable increases in VA enterprise data-related maturity. Under the DGC, maturity and capability models, self-diagnostics, along with guidance and handbooks, are published and identified via corresponding goals and sub-goals. The use of DGC-supported maturity model is based on industry standards and best practices in assessing data management maturity, like the Capability Maturity Model Integration - Data Management Maturity (CMMI DMM) and coordinated with other VA maturity model efforts. This allows programs and offices across VA to self-assess their maturity, integrate actions to improve and measure progress as they mature and onboard into enterprise-wide efforts.

The following tables enumerate each goal, the targeted outcome, and sub-goals.

Goal 1: Stewardship

Table 1: VA Data Strategy Goal 1 - Stewardship

Goal 1 Stewardship - Provide quality and trusted authoritative data, metadata, and metrics to the enterprise, administered and governed by the DGC, in order to accelerate the use, quality and interoperability of VA data assets.
Goal 1 Targeted Outcome – Authoritative, high quality, and accessible data that provides trusted insights into critical problems, and that, in turn, drives better informed, data-driven decisions across the Department, from Veteran services and operations to enterprise investment planning and continuous modernization.
Sub-Goals
1.1 | Identify responsible individuals, delineate their roles, and strengthen the cadre of Business and Technical Data Stewards to collaboratively manage data across its lifecycle to ensure its suitable for business use.
1.2 | Ensure the establishment and implementation of data curation (identification, retrieval, meta-tagging, standardization, federation, security and access control, audit)

policies and their application, including geospatial data and Paperwork Reduction Act requirements, to facilitate interoperability, linking, and dynamic purpose-driven aggregation.
1.3 | Create a comprehensive inventory of data assets and designate the authoritative sources for both operations and analytics that are trusted, timely, and secure.
1.4 | Provide Transparency into Data Quality, Provenance, permitted uses, and fitness for use as measured by transparent metrics and in accordance with VA Data Management Requirements and the DGC.

Goal 2: Analytics

Table 2: VA Data Strategy Goal 2 - Analytics

Goal 2 Analytics - Empower the enterprise with integrated scalable analytics for evidence-based decision-making and policymaking.
Goal 2 Targeted Outcome - Data driven methods and analytical approaches are used to develop justification and support decision making to enhance VA services and benefit provisioning, inform policy making, facilitate program evaluation, and promote positive results for Veterans, their families, and other stakeholders.
Sub-Goals
2.1 | Invest and advance core enabling capabilities for securing and handling all types of data and analytics based on harmonized end-user reporting, key analytic questions, evidence based policymaking and decision-making requirements including setting forth the guidelines/standards for quality assessments and documentation to accompany a report.
2.2 | Create and maintain a federated analytics ecosystem supported by a robust infrastructure with seamless ability to integrate data for Veteran analytics and business intelligence that is accessible to customers when, where and how it's needed.
2.3 | Provide a robust, scalable environment for model development and intelligence gathering that incorporates customer feedback, enhances digital experiences, and supports data interventions to gain insights into customer and employee behaviors to design training and tools, and tools for evidence-based policy making.
2.4 | Increase trust in analytics, including artificial intelligence and predictive analytics, through scientific rigor and transparency of analytic rules and reproducible criteria via dynamic key performance indicators.

Goal 3: Technology

Table 3: VA Data Strategy Goal 3 - Technology

Goal 3 Technology - Create a secure infrastructure for business data architecture, data management, information sharing, and data analytics.
Goal 3 Targeted Outcome – Composable enterprise information (business and data) architecture and data infrastructure that enables information access, manipulation, and re-combination in order to create new insights and perspectives on operational effectiveness and anticipates future business opportunities.
Sub-Goals
3.1 | Develop and maintain an adaptable business, security, privacy controls, and infrastructure architecture platforms and tools that enable effective data management, information sharing, data integration, and analytics to ensure synchronization and data integrity.
3.2 | Enable self-service through a discoverable registry for data services and analytics that allows quick and secure data access and integration of data across products, projects, initiatives, and lifecycles.
3.3 | Further develop a technical architecture to enable the discovery of datasets, including through Application Programming Interface (APIs), and a secure living data catalog identifying data categories with corresponding standards to facilitate interoperability.
3.4 | Establish and manage the necessary information technology processes, procedures, and controls to support data stewards during implementation of Authoritative Data Sources and for decommissioning redundant systems.
3.5 | Leverage economies of scale and process automation in technology acquisition to gather insights in investments, efficiencies, and budget performance via metrics and dashboards.
3.6 | Enable a secure infrastructure that supports data management, secure information sharing, interoperability while protecting Personally Identifiable Information (PII), across the VA.

Goal 4: People

Table 4: VA Data Strategy Goal 4 - People

Goal 4 People - Foster a federated and distributed data-centric workforce.
Goal 4 Targeted Outcome - VA cultivates a data-savvy 21st century workforce that ethically and effectively uses and protects data to maximize delivery of world-class Veteran services.
Sub-Goals
4.1 | Define and develop a data-centric culture with clear roles, responsibilities, skillsets, and incentives for learning, recruitment, and retention.
4.2 | Capture, preserve, transfer, and build upon institutional knowledge and educate knowledge workers to improve their productivity; ensuring the correct interpretation and use of data to better serve Veterans.
4.3 | Educate and grow workforce capabilities to increase expertise in data management and analytics for the creation of better evidence in support of policy and decision making.
4.4 | Develop data-centric and subject-specific communities of practice that drive efficiency through collaboration and informal information exchanges.

Goal 5: Governance

Table 5: VA Data Strategy Goal 5 - Governance

Goal 5 Governance - Strengthen collaborative, federated, and accountable governance towards leveraging data and analytics to drive decision-making
Goal 5 Targeted Outcome - Established oversight and guidelines lead to strong partnerships, data integration, data protection, and data analytics that produce relevant, timely, and interactive products for effective use.
Sub-Goals
5.1 | Strengthen collaborative, enterprise-wide governance and decision rights and accountability to ensure trusted and accountable data sharing, reporting, and analytics while adhering to security and privacy controls through the DGC.
5.2 | Develop and leverage appropriate protocols for securely sharing data and analysis in compliance with all federal policies and guidance within VA, with the Department of Defense, and other external partners, leveraging active feedback loops for process improvements to establish VA as a learning organization.
5.3 | Enhance and extend an enterprise architecture optimized across the data lifecycle for information sharing and analysis.
5.4 | Establish consistent policies, automated tools, and procedures to manage data, an enterprise-level master inventory of data, analytic models, and logic for intelligence gathering and decision making.

Priority Objectives

This strategy will aggressively continue priority initiatives. Many – though not all – already have identified senior operational leaders, teams, and resources. The key characteristics of the priority objectives are that they are: 1) supporting clearly defined and compelling opportunities (including performance metrics and concomitant barriers); 2) requiring implementation of data governance policies, information sharing process (as validated and certified by the DGC); and 3) improving analytic tradecraft with clearly articulated (and therefore addressable) gaps.

The list of priority objectives will evolve over time, based on VA leadership intent and VA Operations Board governance. The CDO – jointly with appropriate champions and in consultation with the DGC – will report progress and outcomes to the VA Operations Board. Reporting metrics include priority (rank order of importance and resource intensity), sponsoring sub-organizations (ownership and accountability), and leadership support.

As described earlier, this strategy focuses on collective action against the data-related challenges and opportunities within these priority objectives via a federated, matrixed implementation approach.

1. **Authoritative Data Sources.** Advance the identification, management, and use of authoritative data sources for the Servicemember and Veterans Journey, including developing a joint DoD-VA Data and Analytics Vision and Strategy.
2. **Electronic Health Record (EHR) Modernization.** Advance and support EHR modernization data management and sharing to improve clinical operations and analytics, and enhance the clinician and Veteran experience and Veteran outcomes; including data syndication to ensure VA control over VA data, enterprise-wide data management and analytics, aligning and integrating EHR fully into the implementation of this strategy.
3. **Statistical and Predictive Analytics.** Use authoritative data and analytics throughout VA and partnered with DoD to support greater actionable insight and decision making to serve Servicemembers and Veterans, and their families, caregivers, and survivors, through alignment and improvement of longitudinal, lifetime analytics and greater data integration and leverage of existing federal and non-federal data.
4. **Federated Data and Analytics Mission Management.** Support operational leaders, researchers and front-line staff across VA to incrementally improve the federated data and analytics mission including investments in people, processes, platforms, tools, and capabilities via established budgeting, planning, programming, and execution management and governance processes.
5. **Common Operating Platform (COP) for Data Management and Decision Support.** Deliver a common operating platform to further strengthen decision making by improving the quality of data available and analytics capability for decision making at all levels in VA. Leadership in VHA and the field will have

access to integrated data and actionable leading indicators in support of operational, mission support, and planning decisions like those needed during the current Coronavirus Disease (COVID)-19 pandemic response, modernization of our medical supply chain, and sustained continuous improvement thereafter.

6. **Strengthen Policy, Processes, and Tradecraft for Data, Information Sharing, and Analytic Collaboration.** Streamline and mature data policy, information sharing process, and analytic tradecraft and collaboration to remove barriers and pursue opportunities. Ensure continued support for safeguarding Veteran information and privacy, minimizing collection burden, and improving management of our data as a strategic asset across its lifecycle. Establish systemic improvements to support the mental health and suicide prevention research and operational priorities as an entry point.
7. **Spatial Data Infrastructure.** Support the implementation of the Geospatial Data Act requirements, Federal Geographic Data Committee guidance, and the National Spatial Data Infrastructure strategic plan across VA to understand and define spatial data infrastructure in the VA and to incrementally acquire, process, distribute, use, maintain and preserve spatial data in support of VA's mission.
8. **Community Care Data Improvements.** Data is available to Veterans to make meaningful choices about their care, benefits, and services and to the providers inside and outside of VA, including data on access and quality, to ensure seamless transitions and continuity of care between VA and the community.
9. **Financial Management Systems Transformation.** Use analytics to provide financial insight across VA legacy systems and informed management decisions by incorporating standardized business processes and data standardization for data integrity, and compliance with federal policies and guidance to maintain a clean audit.
10. **Veterans Experience Data Sharing.** The Veterans Experience Office (VEO) leads the implementation of Customer Experience (CX) at VA (38 C.F.R §§ 0.600-0.603) and is responsible for core CX Capabilities of data, tools, and technology (VA Directive 0010), to improve the experiences of Veterans, their families, caregivers, and survivors through various channels and modalities. Establish secure and appropriate mechanisms to provide curated and qualitative customer insight data around the Veteran Experience for use by executives and program offices.
11. **Human Resources Management.** Advance human resources management by developing human capital data, assets, and capabilities that enable evidence-based human resources and manpower management for the enterprise with an objective of supporting the recruiting and retention of necessary data management talent who will implement this Strategy.
12. **Memorial Benefits Data Management.** National Cemetery Administration (NCA) will implement the Memorial Benefits Management System (MBMS) to replace the Burial Operations Support System Enterprise (BOSS-E) platform, the memorial legacy applications, with a more cohesive, compliant, and comprehensive memorials enterprise initiative that seamlessly integrates with VA's authoritative data systems. MBMS will streamline NCA's management and operation of the national cemeteries, benefits eligibility determinations for pre-

need and time of need, and the provisioning of memorial benefits including headstones, markers, medallions and Presidential Memorial Certificates.

13. **Veterans Benefits Portfolio Enhancements.** VBA will drive toward application modernization resulting in greater availability of standard platforms, common data sharing, and a standardized software delivery approach. A suite of strategies will drive VBA's core modernization efforts: leveraging more functionalities into the Veterans Benefit Management System, increasing use of Cloud-based commercial products, enhancing currently integrated systems, standardizing record sharing between federal agencies, and replacing or retiring as many legacy systems as possible.

The Way Forward

The work in front of us comprises three key transformations:

1. Authentic, authoritative, and auditable data based on an enterprise-wide framework of secure primary sources;
2. Federated capability to manage, exchange, and process data to improve clinical care services, benefits delivery, daily operations, resource management and research enterprises; and
3. Much greater transparency and accountability regarding data-centric investments and the people responsible for implementing these processes.

Transparency will enable VA leadership to ensure sustainability of efforts and align future investments with the vision, goals, and objectives of this strategy. Making progress towards the vision of managing data as a strategic asset to support and strengthen VA as a learning enterprise requires VA leaders and experts to organize for change, address organizational and cultural barriers, and work together to strengthen further enterprise integration as a managed federation. Together, VA will advance the management of its data as a strategic asset, solidify VA as a learning enterprise, using our vast holdings of data to improve service delivery, outcomes, and impact for the Nation’s Veterans, their families, caregivers, and survivors.

The heart of this strategy is a network of priority objective and goal/sub-goal champions, each an empowered leader within their sub-organizations owning aspects of the strategy and coordinating with each other with guidance and support from the DGC and with the oversight of the VA Operations Board. The DGC Executive Secretariat, via existing and to-be-established DGC working groups, will develop a concept of operations (CONOPS) to support the development, alignment, and synchronized implementation of work plans authored by the teams supporting the champions.

We anticipate this work can leverage some existing management and governance pathways, and will require some new ones, in order to achieve transparency and collective accountability. The CONOPS will define templates, reporting requirements, clear roles and responsibilities, performance metrics and measures, and a dashboard of workflows to provide basic automation support for cross-cutting alignment, feedback, and progress tracking against associated metrics.

The next step is development, coordination, and initial baselining of the implementation roadmap for this strategy. The roadmap will reflect and summarize critical dependencies, linkages, and milestones. The CDO, in close consultation with the DGC, will bring goal and objective champions together to review progress and assess performance, collectively identify opportunities to improve collaboration, review priorities, identify and remove barriers, and accelerate efforts. Collaboration and collective accountability towards accelerating progress and enterprise maturity will be supported via the quarterly assessment and reporting cadence. The emphasis on federated leadership, with named-accountable parties is key to aligning efforts toward a common outcome while keeping the work aligned to mission imperatives across VA.

APPENDIX A. Acronyms

The following lists relevant acronyms.

Acronym	Definition
API	Application Programming Interfaces
BOSS-E	Burial Operations Support System Enterprise
CDO	Chief Data Officer
CDTO	Chief Data Technology Officer
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
CONOPS	Concept of Operations
COP	Common Operating Platform
COVID	Coronavirus
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
CX	Customer Experience
DGC	Data Governance Council
DMBoK	Data Management Body of Knowledge
DMLSS	Defense Medical Logistics Standard Support
DMM	Data Management Maturity
DoD	Department of Defense
EHR	Electronic Health Records
EHRM	Electronic Health Records Migration
FMBT	Financial Management Business Transformation
IA	Information Architecture
LEP	Limited English Proficiency
M	Million
MBMS	Memorial Benefits Management System
NCA	National Cemetery Administration
OEI	Office of Enterprise Integration
OIT	Office of Information and Technology
PII	Personally Identifiable Information
VA	U.S. Department of Veterans Affairs
VACO	VA Central Office
VBA	Veterans Benefit Administration
VEO	Veterans Experience Office
VHA	Veterans Health Administration

Appendix B. DEFINITIONS

All definitions below are taken from the VA Data Management Directive 0900.

a. **Accessible.** Users and applications post data to a shared space. Posting data implies that (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the enterprise and (2) the data is stored such that users and applications in the enterprise can access it. Data assets are made available to any user or application except when limited by law, mandates, policies, or Directives.

b. **Authoritative Data Source.** A source of data or information designated as an official source of data that is recognized, trusted, timely, secure, and used within VA's information environment in support of VA business processes. Administrations and Staff Offices nominate these sources within domains for which they are the stewards. OIT develops and maintains technology solutions (e.g., services) that use these sources.

c. **Authorized User.** A person who is granted access to information resources based upon clearance, need-to-know, organization security policy, and federal security and privacy laws. [Source: VA Directive 6518, 02/20/2015].

d. **Data.** An elementary description of things, events, activities, and transactions that are recorded, classified, and stored, but not organized to convey any specific meaning. Data items can be numeric, alphabetic, figures, sounds, or images. A database consists of stored data items organized for retrieval or in line processing.

e. **Data Analytics**. Linking and processing authoritative data across data assets to gain trusted insight, create evidence, report on operations, or assess performance.

f. **Data Asset.** A collection of data elements or sets that may be grouped together and represents a work product generated by a VA employee or VA-affiliated entity.

g. **Data Quality.** A measure of the condition of data based on factors such as accuracy, completeness, consistency, and reliability.

h. **Data Governance.** The exercise of authority, control, and shared decision-making planning, monitoring, management and enforcement over data assets.

i. **Data Lifecyle.** The stages through which data passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

j. **Data Management**. The set of disciplines and techniques used to process, store and organize data.

k. **Data Stewardship.** The formal, specifically assigned and entrusted accountability for business (non-technical) responsibilities ensuring effective control and use of data and information assets implemented by formally assigning and entrusting its responsibilities to data stewards. A data steward is a person that fulfills the data stewardship role.

l. **Information**. Any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. Information usually but not always has associated meta-data, or data that helps to characterize and provide context.

m. **Information Architecture (IA).** The structural design of common and shared data and information. Information architecture includes design of the data environment requirements that enable legislative and regulatory compliance and business analytics. IA supports the determination of what, how, and where information will be collected, stored, processed, transmitted, presented, and used in support of mission and business operations, reporting, compliance, and analytics. IA informs the data strategy, implementation of standards, semantic interoperability, and user interface design in support of VA's business processes.

n. **Information Environment**. The aggregate of the information created and used by an organization, the information architecture of the organization (models, authoritative and redundant data stores and flows), and the governance framework, policies, and standards that ensure information is managed.

o. **Information Resources.** Includes both government information and information technology.

p. **Interoperability**. The ability of a system to securely exchange information with, and use information from, other systems without special effort by the user.

q. **Safeguarding.** Safeguarding relates to the measures used to deter, detect, and prevent against the loss, misuse, theft, unauthorized access, unauthorized modification, unauthorized disclosure, or unauthorized use of classified, controlled unclassified information (CUI), and other unclassified information of a sensitive nature, and the protections afforded to information systems/networks on which such information resides. Safeguarding encompasses - but is not limited to - counterintelligence, information assurance, information security, operational, administrative, personnel, and physical security, as well as privacy, civil rights, and civil liberties protections.

r. **Strategic Asset**. An asset that is required by an entity for it to maintain its ability to achieve future outcomes.

s. **VA Customers**. US service members, Veterans, and their beneficiaries and representatives and employees.

t. **Visible**. Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, nonintelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset.

Appendix C. Laws, Mandates, Policies, Directives

Laws, Mandates, Policies, Directives/URL	Data Requirements
Chief Financial Officer Act of 1990 (Public Law 101–576) Link - https://www.gao.gov/special.pubs/af12194.pdf	Requires that financial data is prepared with uniformity and is responsive to the financial information needs of agency management.
Digital Accountability and Transparency Act of 2014 known as Data Act (31 U.S.C. 6101) Link: https://www.congress.gov/113/plaws/publ101/PLAW-113publ101.pdf	Expands the Federal Funding Accountability and Transparency Act of 2006 (31 U.S.C. 6101 note) by requiring the disclosure of direct federal agency expenditures and the linkages of Federal contract, loan, and grant spending information to programs of Federal agencies. Standardizes the financial data elements, establishes Government-wide data standards for financial data to improve data quality; requires Inspector General to submit to Congress and make publicly available a report assessing the completeness, timeliness, quality, and accuracy of the agency's data; and recommends the establishment of a data analysis center or the expansion of an existing service to provide data, analytic tools, and data management techniques.
Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act) Link: https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf	Requires CFO Act Agencies to develop an evidence-building plan every four years as part of their strategic plans. The plan identifies questions relevant to programs, policies, and regulations and includes a list of the data the agency intends to collect, use, acquire or collect, and a list of challenges to accessing relevant data. The Open Data Act section codified into policy previous open data requirements including the designation of a point of contact within the agency; the development and implementation of a process to evaluate and improve the timeliness, completeness, consistency, accuracy, usefulness, and availability of open government data assets; the identification of priority data assets; the publication on the website of the agency of information on the usage of such assets by non-Government users; the hosting challenges, competitions, events, or other initiatives designed to create additional value from public data assets of the agency. It also requires agencies to create a

Laws, Mandates, Policies, Directives/URL	Data Requirements
	comprehensive data inventory that accounts for all data assets created by, collected by, and under the control or direction of, or maintained by the Agency. It also set forth the roles and responsibilities of the Evaluation Officer, Chief Data Officer and the Chief Statistical Official.
Geospatial Data Act of 2018 or GDA (P.L. 115-254) Link: https://www.fgdc.gov/gda/geospatial-data-act-of-2018.pdf	Establishes the Federal Geographic Data Committee to: lead the development and management of a National Spatial Data Infrastructure strategic plan and geospatial data policy; designate National Geospatial Data Asset data themes and oversee the coordinated management of the National Geospatial Data Asset data themes; establish and maintain geospatial data standards; periodically review and determine the extent to which covered agencies comply with geospatial data standards; ensure that the GeoPlatform operates in accordance with section 758; directs and facilitates national implementation of the system of National Geospatial Data Asset data themes; and requirements relating to geospatial data technology development, transfer, and exchange. Requires Agencies to issue an annual report.
Circular A-130-Management of Federal Information Resources (November 8, 2019) Link-https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf	The Memorandum directs an inventory of all agency information resources; an enterprise-wide data inventory that accounts for data used in the agency's information systems; that open data standards are used when implementing IT systems; data and information needs are met through agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives; require agencies to Implement data-level protection and access controls to ensure the security of and access to Federal information; and requires agencies to evaluate the sensitivity of each individual data element that is PII, as well as all of the data elements together. Further direction to ensure the physical and information system security of confidential information and the Federal information is managed consistent with applicable records retention and disposition requirements.
OMB M-19-23: Phase 1 Implementation of the Foundations for Evidence-	The Memorandum directs set forth the requirements for selection and appointment of Chief Data Officer, Evaluation Officer, and Statistical Official and clarifies

Laws, Mandates, Policies, Directives/URL	Data Requirements
Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance Link: https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf	and expands on their roles and responsibilities within the agencies. Clarifies governance; establishing the learning agendas as the priority for managing data as a strategic asset to support the agency in meeting its mission and, answering the priority questions laid out in the agency Learning Agenda.
OMB- M19-18- Federal Data Strategy - A Framework for Consistency Link: https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf	The Memorandum provides a common set of data principles and best practices in implementing data innovations that drive more value for the public. The Strategy complements statutory requirements and 0MB information policy and guidance, and incorporates relevant changes proposed by agency and public comments received in response to M-19-01. It sets forth three components to guide Federal data management and use: a mission statement; principles that serve as motivational guidelines in the areas of Ethical Governance, Conscious Design, and Learning Culture and practices that guide agencies in leveraging the value of data by Building a Culture that Values Data and Promotes Public Use; Governing, Managing, and Protecting Data; and Promoting Efficient and Appropriate Data Use.
OMB M-19-15 Improving Implementation of the Information Quality Act (April 24, 2019) Link: https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf	The Memorandum reinforces, clarify, and interpret agency responsibilities under the Information Quality Act (IQA) by expanding the OMB issued Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility and Integrity of Information Disseminated by Federal Agencies. The updated requirements are peer review of Influential Scientific Information; public access to government information (Open Data) requirements to re-use of existing agency program data. Includes increased transparency about statistical methodologies including Models and Machine Learning; prioritized access to data used in the analysis and consideration for protecting data.
OMB M-19 03: Strengthening the Cybersecurity of Federal Agencies by enhancing	This document sets guidance for High value assets by requiring agencies to: • Establish data-driven prioritizations • Update technology architectures

Laws, Mandates, Policies, Directives/URL	Data Requirements
the High Value Asset Program (December 10, 2018) Link: https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf	High value assets reporting frequency, including the method for collection and data elements required.
NIST Special Publication (SP) 800-37, Rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 20, 2018. Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf	This document sets forth the requirements for gathering the following information for understanding the data lifecycle and conducting system's risk assessments based on the following inputs: agency's missions, business functions, and mission/business processes the system will support; system stakeholder information; authorization boundary information; information about other systems that interact with the system (e.g., information exchange/connection agreements); system design documentation; system element information; list of system information types. The outputs should be documentation of the data lifecycle in the system, such as a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Such documentation includes, for example, data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries.
OMB M-11-02- Sharing Data While Protecting Privacy (November 3, 2010) Link: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-02.pdf	The Memorandum directs agencies to find solutions that allow data sharing in a manner that complies with applicable privacy laws, regulations, and polices. Agencies are encouraged to share high-value data for purposes of supporting important Administration initiatives, informing public policy decisions, and improving program implementation including: (1) identifying high-value data that would promote effective and efficient decision-making; (2) identifying high-value data and data sharing methodologies that would promote more efficient delivery of benefits with lower error rates; (3) developing effective approaches for properly sharing data with other Federal entities (4) ensuring the use of common data standards to promote greater interoperability across systems and improving sharing of data as part of IT modernization initiatives; and (5) following Enterprise Architecture guidance and principles consistent with appropriate OMB guidance and best

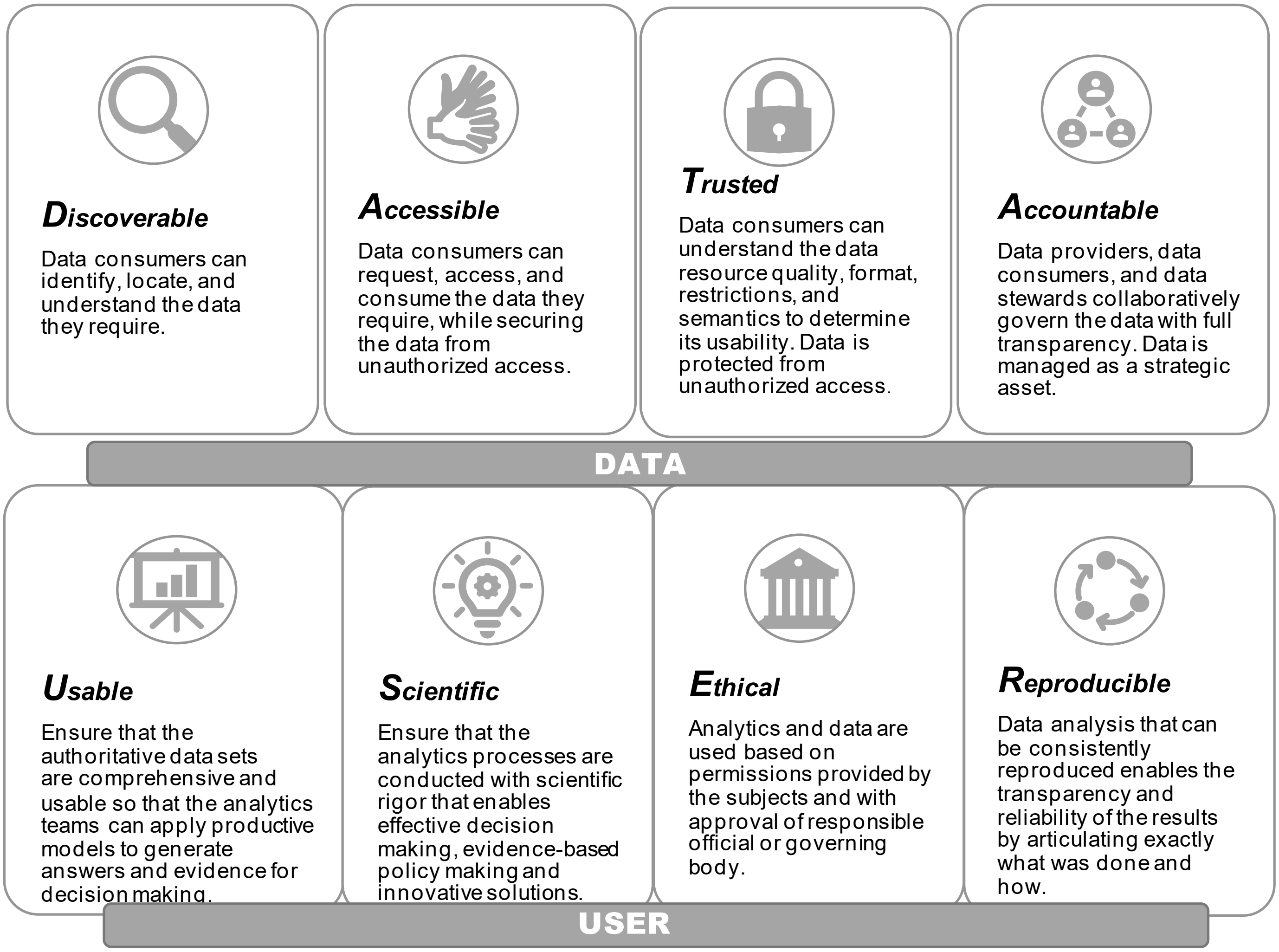
Laws, Mandates, Policies, Directives/URL	Data Requirements
	practices for new and on-going systems development and implementation.
NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Rev, 1, Vol. 1 and 2, August 1, 2008. Volume: 1 Link: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf	The Volume 1 set forth the requirement that during the review of impact level assessment the information security officers, mission owners; and Information Owners should review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing and the adjustment the impact levels as necessary based on the following considerations: Confidentiality, integrity, and availability factors; situational and operational drivers (timing, lifecycle, etc.); legal or statutory reasons; and document all adjustments to the impact levels and provide the rationale or justification for the adjustments. Assessment of data during aggregation need to consider that the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of an account number with the identity of an individual and/or institution). The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system security objective impact levels may need to be adjusted to a higher level than would be indicated by the security impact levels associated with any individual information type.
NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Rev, 1, Vol. 1 and 2, August 1, 2008. Volume 2 Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf	The Volume 2 set forth the following requirements. • Data Impact determination -the confidentiality impact assigned the data and system is that of the highest impact information type collected. • The availability impact level is based on the specific mission and the data supporting that mission. The integrity impact level is based on the specific mission and the data supporting that mission.
Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and	This document sets forth the standards and guidelines tasked to NIST by Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA). This publication addressed the standards to categorize all information and information

Laws, Mandates, Policies, Directives/URL	Data Requirements
Information Systems, February 1, 2004. Link: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf	systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.
VA Directive-0900- VA Enterprise Data Management Directive (December 8, 2020) Link: https://www.va.gov/vapubs//viewPublication.asp?Pub_ID=1218&FType=2	Establishes the requirements for the lifecycle management of data as a strategic asset in the Department and sets forth the overarching structure for enterprise data management within VA. Set forth the responsibilities for data management for the Chief Data Officer (CDO), Chief Information Officer and Data Governance Council (DGC) among others. Requires that all data is managed in compliance with data quality and security requirements; is available for responsible sharing; when authoritative data is identified, it is the responsibility of the data steward, data owner, and/or system owner to nominate the authoritative data source (ADS) for consideration to the DGC following the requirements for ADS identification and selection; requires data to be available via application programming interfaces (APIs) and the use of authoritative data and recognizes that VA customers individually and collectively, have an ongoing interest in their data and its management, quality, sharing, safeguarding, and use by VA.
VA Directive 6500, VA Cybersecurity Program (January 24, 2019) Link: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1003&FType=2	Sets forth the Security requirements for systems and data. Requires to tailor the rigor of the risk assessments to accommodate resource constraints and the availability of detailed risk factor information (e.g., threat data); requires data to be protected and manage consistent with the assessed risk including: the management of information, records, and data throughout the information life cycle consistent with VA's risk strategy to protect the confidentiality, integrity, and availability of information; protection of moderate and high impact information at rest and during transmission unless encrypting such information is technically infeasible or would demonstrably affect the ability of VA to carry out its missions; establishing a Data Management Board and developing and implementing guidelines supporting data modeling, quality, integrity, and de-identification needs of PII/PHI across the information life cycle; establishing a

Laws, Mandates, Policies, Directives/URL	Data Requirements
	Data Integrity Board to oversee organizational Computer Matching Agreements.
VA Directive 6051 – Department of Veterans Affairs (VA) Enterprise Architecture (April 8, 2016) Link: https://www.va.gov/DIGITALSTRATEGY/docs/VA_Directive_6051.pdf	Defines VA's Enterprise Architecture (EA) and requires that all VA IT systems must comply with the EA; VA officials will support the EA with a complete inventory of agency information resources, including personnel, equipment, and applications and data devoted to information resources management and information technology, at an appropriate level of detail.
VA Directive 6404 – VA Systems Inventory (February 23, 2016) Link: https://www.va.gov/digitalstrategy/docs/VADirective6404_VASystemsInventory.pdf	Establishes VASI as the authoritative data source (ADS) for VA IT Systems; VASI will deliver an integrated view of System information including data residing in other enterprise repositories; and all data stores and associated data schemas associated with systems registered in VASI shall be registered in the VA Enterprise Architecture (VA EA)

Appendix D. VA Data Guiding Principles

Complementing the data vision and mission are a set of eight guiding principles. These principles help frame the strategy that serves as a guide for how the VA must effectively manage and govern data as a strategic asset to enable timely, evidence-based decision making that will result in improvements to service delivery to our Veterans. Four of them (D - Discoverable, A-Accessible, T-Trusted, and A-Accountable) provide the guiding principles for "DATA" management, while the other four (U-Usable, S-Scientific, E-Ethical, and R-Reproducible) focus on the "USER" of data and analytics. These principles build upon the FAIR Guiding Principles[2] for scientific data management and stewardship. Both internal and VA stakeholders will have easier access to VA data, and analytics will apply greater scientific rigor, without compromising data security and privacy.



Discoverable

Data consumers can identify, locate, and understand the data they require.

Accessible

Data consumers can request, access, and consume the data they require, while securing the data from unauthorized access.

Trusted

Data consumers can understand the data resource quality, format, restrictions, and semantics to determine its usability. Data is protected from unauthorized access.

Accountable

Data providers, data consumers, and data stewards collaboratively govern the data with full transparency. Data is managed as a strategic asset.

DATA

Usable

Ensure that the authoritative data sets are comprehensive and usable so that the analytics teams can apply productive models to generate answers and evidence for decision making.

Scientific

Ensure that the analytics processes are conducted with scientific rigor that enables effective decision making, evidence-based policy making and innovative solutions.

Ethical

Analytics and data are used based on permissions provided by the subjects and with approval of responsible official or governing body.

Reproducible

Data analysis that can be consistently reproduced enables the transparency and reliability of the results by articulating exactly what was done and how.

USER

[2] Source: https://www.nature.com/articles/sdata201618

GUIDING PRINCIPLES

1 | Data is ***Discoverable***

Veterans, their families, and department stakeholders rely upon data that can be rapidly identified and located in a seamless and efficient manner. Available data will be discoverable, consistent, and comprehensive across the enterprise and to consumers by means of a robust data inventory and metadata repository.

2 | Data is ***Accessible***

Data needs to be available in a timely manner to approved users or applications except when limited by policy, regulation, or security. Users and mission partners with the appropriate level of authorization and justifiable need for the data will have timely access to data, leading to informed decisions and actions. When data access is denied, the VA will provide justification.

3 | Data is ***Trusted***

Trusted data is a critical resource and essential to accurate and insightful decision-making. Maintaining data integrity, lineage, and provenance ensures users can trust the data they discover and receive. VA programs will publish the quality, format, and semantics of their data, along with the appropriate metrics and compliance standards for the subject systems and users.

4 | Data is ***Accountable***

Ensuring the integrity of this critical asset, and as outlined in the Enterprise Data Management Directive, data stewards will be responsible for managing data as a strategic asset throughout the data lifecycle and in compliance with all applicable policies and regulatory obligations. Together, the data providers, users, and stewards will work collaboratively to effectively govern data, ensuring full transparency and oversight.

5 | Data and Analytics are ***Usable***

Usable and relevant data is integral to generating repeatable models and analytics that can be leveraged throughout the organization. The VA must be able to produce comprehensive datasets to drive analytical, evidence-based decision-making in support of operations and services. All data within a system will be stored independently to promote usability across multiple stakeholders.

6 | Data Analytics Derived from Sound ***Scientific*** Methodologies

Analytical processes will be conducted with scientific rigor; generating data and evidence grounded in trusted data collection, cleansing, modeling, observations, experimentation, and simulation methods. Analytical teams will adhere to established best practices and policies, employing only authorized tools, methods, and analytical approaches. Relevant analytic methods and results are to be fully documented and vetted by designated entities.

7 | Data and Analytics are Used ***Ethically***

It is critical that the VA Ethical Principles for Access to and Use of Veteran Data developed by VA are meticulously adhered to and applied across all applicable data and subsequent information created using that data. The VA will use data in ways that are consistent with the intentions and understanding of their customers and stakeholders and, to the extent possible, will execute mechanisms for tracking the context of collection, methods of consent, and chain of responsibility.

8 | Data and Analytics are ***Reproducible***

By articulating exactly what was done and how, data analysis can be consistently reproduced which enables the transparency and reliability of the results. Across the organization, data stewards, including data analysts, operational researchers, actuarial specialists, mathematicians or statisticians, and data scientists, will publish, distribute and ensure the reproducibility of their results through standardization methods, precise analysis, and automation. Users will be able to trace and verify the analytic processes of the results; thereby providing the necessary linkages between conclusions and analysis as required by the Policy for Information Quality in VA (Handbook 009).

Appendix E. VA Ethical Principles for Access to and Use of Veteran Data

Veterans trust the Department of Veterans Affairs (VA) to promote and respect their privacy, confidentiality, and autonomy in the services we provide and support. We embody this trust when we adhere to VA's **I CARE** core values of **I**ntegrity, **C**ommitment, **A**dvocacy, **R**espect, and **E**xcellence. Consistent with these values, VA must promote and assure responsible practices whenever Veteran data is accessed or used. Veteran data is, and should be, accessed and used for many purposes which are developing at an unparallel pace. The regulatory and policy framework that governs data access and use sets important standards about what is required with respect to data access and use but does not always provide definitive guidance about how VA should manage access or use of Veteran data when regulation and policy permit organizational discretion. The following principles establish an overarching ethical framework for all individuals, groups, or entities inside and outside VA to apply when managing data access or use or accessing and/or using Veteran data. All parties who oversee access and use of Veteran data, or who access and use Veteran data themselves, must carefully consider and apply this principle-based ethical framework in the context of the specific clinical, technical, fiscal, regulatory, professional, industry, and other standards for each specific data access and/or use. Consistent application of this framework will ensure the integrity and trustworthiness that Veterans and other stakeholders expect and deserve when Veteran data is accessed and/or used.

Principle 1: For the good of Veterans, their families, caregivers and survivors
Veteran data is personal and sensitive. Use of Veteran data must have the primary goal of supporting and improving overall Veteran health and wellness, and the delivery of benefits and services to Veterans at large.

Principle 2: Equity
Proper use of Veteran data must help to ensure equity so that no Veteran population is disproportionally excluded from the benefits of, or burdened by the risks of, data use because of race, color, religion, national origin, Limited English Proficiency (LEP), age, sex (including gender identity and transgender status), sexual orientation, pregnancy, marital and parental status, disability, or genetic information.

Principle 3: Meaningful choice
Sharing of Veteran data – by VA or non-VA parties – when regulation and policy permit organizational discretion (for example, for purposes other than treatment, payment, health care operations, or meeting legal requirements), should be based on the Veteran's meaningful choice to permit sharing their information for that specific purpose. Timely, clear, relevant, concise, complete, and comprehensible information must be provided to the Veteran to serve as a basis for their free and informed choice. A Veteran's preference to change their mind about sharing or not sharing their information should be facilitated, with the understanding that information that has already been shared may not be able to be retrieved or retracted. A Veteran's choice(s) about data sharing must not be the basis to deny care or benefits to which they are otherwise

entitled.

Principle 4: Transparency

Access to and exchange of Veteran data should be transparent and consistent, and in accordance with all applicable standards. For VHA, this includes practices described in VHA's Notice of Privacy Practices. Data should only be sent or accessed for approved and/or specified purposes; there should be no un-specified use, or re-use of Veteran data without approval. Release of Veteran data for purposes other than those which were originally approved or specified requires a separate approval and commitment of all parties to follow these principles. Failure to assure such protections is a breach of Veteran trust and confidentiality.

Principle 5: Principled de-identification

Parties who receive de-identified Veteran data must not attempt to re-identify the data in any manner without prior authorization. VA considers unauthorized re-identification a breach of Veteran trust and confidentiality.

Principle 6: Reciprocal obligation for Veteran data use

Financial or other gain from innovation that used Veteran data creates a moral and tangible obligation of reciprocity to share this gain with Veterans, or Veterans organizations and causes. For example, parties could fulfill this obligation by giving back to the Veteran community through support of Veteran causes or organizations, by facilitating Veteran access to innovations to which Veteran data contributed, or, at a minimum, by publicly recognizing Veteran contributions to the gain or innovation. Veteran data must not be sold.

Principle 7: Obligation to ensure data security, quality, integrity

All parties who send, receive, or use Veteran data must assure data security, quality, and integrity; that is, that the data remains secure, accurate, complete, and representative of the data quality, meaning, and integrity when it was received or accessed from VA. Access to data should be limited to the minimum amount needed to accomplish the stated purpose, and should be terminated when no longer required; data not necessary to accomplish the purpose for which it was obtained should not be retained longer than legally required. Transparency about breaches in data security, quality, or integrity, is also essential to promote trust and minimize impacts to Veterans.

Principle 8: Veteran access to their own information

Veterans must have user-friendly access to their own information.

Principle 9: Veteran right to request amendment to their own information

Veterans must be able to exercise their right to request amendments to their information if they feel it is untimely, inaccurate, incomplete, or not relevant.