Veterans'
Information
Security

SAFEGUARDING VETERANS' PERSONAL INFORMATION

A Top Priority for VA

VA has placed the highest priority on protecting Veterans' privacy and safeguarding their personal information. Information used for research purposes is handled according to strict federal and VA-specific regulations and guidelines.

Veterans Health Administration
Research Development
Improving Veterans' Lives www.research.va.gov

DISCOVERY INNOVATION ADVANCEMENT

Veterans'
Information
Security

Safeguarding Veterans' Perso

Why is information essential to VA Research?

VA Research is dedicated to improving Veterans' lives through innovation and discovery. To conduct studies that may ultimately lead to advancements in Veterans' health care, VA researchers must have access to general data on VA care and services, as well as data on Veterans' health care utilization and outcomes. It is important to note, however, that researchers have access only to information that is considered vital to their study—as determined by an Institutional Review Board (IRB). An IRB is a board made up of researchers, non-researchers, and experts outside of VA. Protecting personal information is essential because its loss or unauthorized use can lead to serious consequences for Veterans and disruptions in VA's operations.

> "To honor the confidence placed in us by the Veterans we serve, we must steadfastly protect the personal information with which we are entrusted—information without which our research would be impossible."

Joel Kupersmith, MD

Chief Research and Development Officer
Department of Veterans Affairs

How does VA Research protect Veterans' information from unauthorized access?

To protect Veterans' personal information on which VA research relies, extensive policies and procedures are in place. Main elements of the security program can be categorized as:
(1) **Managerial**—includes establishment and continual examination and upgrading of information security policies and directives;
(2) **Technical**—includes upgrading of software and equipment to prevent unauthorized access to sensitive data; and
(3) **Operational**—includes establishment of enhanced training programs to educate employees about their information security responsibilities.

Management

Adopting Effective Policies and Procedures

Upgraded information security procedures include a requirement that VA health studies' lead researchers and other staff certify that all projects comply with current requirements for the use, storage, and security of research information. Also, reviews are conducted to identify VA employees who require access to sensitive data; these employees undergo appropriate background checks, depending on their responsibilities and the level of access they require.

VA also works with other federal and commercial entities that have Veterans' information for business reasons to ensure they have appropriate safeguards in place to protect sensitive data.

nal Information—A Top Priority for VA

Technical

Securing Computers and Related Technologies

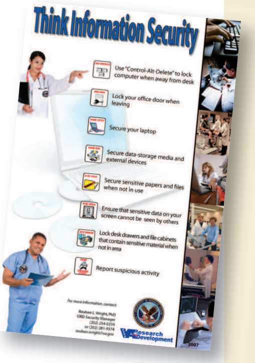
Like most organizations today, VA relies heavily on computer systems and telecommunications networks to achieve its mission. VA researchers, in particular, have benefited from advances in computer technology. They can access the information stored in VA's state-of-the-art electronic health record system, with proper safeguards in place, and conduct large-scale studies that contribute greatly to Veterans' health care.

For sensitive information accessed on-site, as well as data retrieval from remote locations, security requirements are in place to prevent unauthorized access. For example, laptop computers throughout VA have data encryption programs installed, and all sensitive data on mobile computers or portable storage devices such as thumb drives must be encrypted so that unauthorized users are unable to decipher the information.

Operational

Emphasizing Personal Responsibility

To ensure current policies and procedures protect sensitive information, VA Research places great emphasis on personal vigilance and individual responsibility among its employees. All employees receive training on privacy and security of sensitive data, and education campaigns are continuously undertaken to remind employees of their all-important responsibilities in this area.



Think Information Security

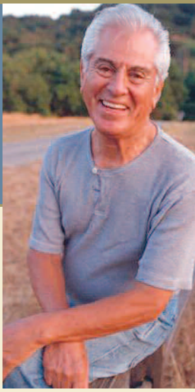
- Use "Control-Alt-Delete" to lock computer when away from desk
- Lock your office door when leaving
- Secure your laptop
- Secure data-storage media and external devices
- Secure sensitive papers and files when not in use
- Ensure that sensitive data on your screen cannot be seen by others
- Lock desk drawers and file cabinets that contain sensitive material when not in area
- Report suspicious activity

For more information, contact:

Reuben L. Wright, PhD
ORD Security Manager
(202) 254-0259
or (202) 281-9374
reuben.wright@va.gov

VA Research & Development

2007



Laws That Protect Personal Information

VA is required to comply with a number of federal laws that protect personal information. Below are three of the most important statutes that govern how VA and other federal agencies handle health care and other personal information.

Privacy Act of 1974

Federal agencies must establish safeguards to ensure the security and confidentiality of statistical records. A person's information must be protected against anticipated threats that could cause him or her substantial harm, embarrassment, inconvenience, or unfairness.

E-Government Act of 2002

Agencies must conduct "privacy impact assessments" that include descriptions of how certain types of personal information will be secured. Under a part of this Act known as the Federal Information Security Management Act (FISMA), agencies must develop and implement cost-effective programs to protect information from unauthorized access and use.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Under this Act, agencies are required to adopt standards for the electronic exchange, privacy, and security of health information—primarily a mandate to the Department of Health and Human Services but also applicable, in part, to VA and other federal agencies.

A Message to Our Veterans

In carrying out our mission of health care discovery and innovation, we as Veterans Affairs (VA) administrators and researchers are entrusted with Veterans' personal information that is vital to our work. We handle this information, which plays such a crucial role in research to improve Veterans' health care, very carefully to keep it secure and to prevent unauthorized access. VA Research is committed to being a leader in the area of information security, putting the safekeeping of Veterans' information first.

This brochure discusses steps that VA Research has taken to adopt, as well as enforce, policies and procedures to ensure the protection of sensitive data.

Joel Kupersmith, MD
Chief Research and Development Officer
Department of Veterans Affairs

Veterans Health Administration
Research & Development
Improving Veterans' Lives www.research.va.gov

For questions or additional copies contact:

R&D Communications (12)
103 South Gay Street, Ste. 517
Baltimore, MD 21202
(410) 962-1800 x223
research.publications@va.gov

200912

Veterans Health Administration
Research Development
Improving Veterans' Lives www.research.va.gov

DISCOVERY INNOVATION ADVANCEMENT