

Department of
Veterans Affairs

Memorandum

Date JUN 12 2006
From Deputy Under Secretary for Health for Operations & Management (10N)
Chief Research and Development Officer (12)
Subj Research Responsibilities for Protecting Sensitive Information
To VA Research Community

1. All of us have the responsibility for protecting the information entrusted to us by America's veterans. VA research can only accomplish its mission of improving the health of veterans through innovative advances in health care if we maintain the trust of those we serve by adhering to the highest standards of safeguarding sensitive data.

2. In addition to completing the annual General Privacy Training and VA Cyber Security Awareness Training for 2006 by June 30, researchers are expected to be familiar with and abide by existing policies, procedures, and directives regarding the protection of human subjects in research and the use and disclosure of individually-identifiable information. If you are not familiar with these policies, we urge you to carefully study VHA Handbook 1200.5, *Requirements for the Protection of Human Subjects in Research* (http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=418) and VHA Handbook 1605.1, *Privacy and Release of Information* (http://www1.va.gov/VHAPUBLICATIONS/ViewPublication.asp?pub_ID=1423), as well as the most recent policies and directives concerning data security, including:

- (1) VA IT Directive 06-2, **Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations** (see attachment). *This directive emphasizes the requirement to protect confidential and Privacy Act-protected information while transporting it to alternative work locations, such as, universities and other research federal agency sites.*
- (2) VA Directive 6504, **Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities** (see [http://www.va.gov/pubs/directives/Information-Resources-Management-\(IRM\)/6504dir06.doc](http://www.va.gov/pubs/directives/Information-Resources-Management-(IRM)/6504dir06.doc)). *This directive restricts the use of VA data stored in non-electronic form outside the regular work site, prohibits the use of non-VA owned equipment (including laptops) to access the VA intranet remotely or to process VA Protected Information (VAPI) except as specifically provided by the directive, and requires all employees to only use computers and electronic storage media configured to conform with all VA security and configuration policies to store, transport, transmit, use and access VAPI. Please note that VAPI information stored on both VA and non-VA equipment must be encrypted using VA approved encryption software.*

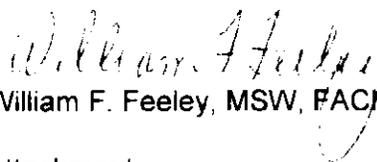
3. We urge you to immediately review all your removable and transportable storage media, including, flash drives, CD-ROMs, and laptops, to remove or otherwise secure sensitive information as specified by the above directives. Please contact your local facility Information Security Officer (ISO) for guidance on securing and encrypting sensitive data, sanitizing media, and other questions about securing information.

Researcher Responsibilities for Protecting Sensitive Information

4. VA and VHA policies are likely to change over time. It is important for you to stay abreast of these changes and incorporate them into your data practices as required.

5. Please note that adherence to applicable VA and VHA policies pertaining to research is continually monitored by the Office of Research Oversight. Failure to comply may result in sanctions to individual investigators and the local research program, including loss of eligibility for VA research funding and other disciplinary action. In addition, violations of HIPAA and the Privacy Act may result in civil and criminal penalties.

6. We appreciate your commitment to America's veterans and to following the necessary safeguards to promote data security.


William F. Feeley, MSW, FACHE


Joel Kupersmith, MD

Attachment

**Department of
Veterans Affairs**

Memorandum

Date **JUN 6 2006**

From Secretary (00)

Subj VA IT Directive 06-2, *Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations*

To Under Secretaries, Assistant Secretaries, and Other Key Officials

1. The Department of Veterans Affairs (VA) is committed to protecting the personal data of all individuals, including veterans, dependents and employees. Those protections extend to all data formats and media, including electronic, paper, and oral information.

2. Due to business imperatives and management efficiencies, VA employees are sometimes permitted to transport confidential and Privacy Act-protected information about individuals to alternative work locations. You must emphasize to these employees that the loss of confidential and Privacy Act-protected data can result in substantial harm to individuals, including the veterans we serve. This directive addresses procedures to be followed for safeguarding information removed from VA premises to alternative locations, and reminds employees that supervisory permission is necessary to do so.

3. Employees who are authorized to remove confidential and Privacy Act-protected data from the Department are required to take all precautions to safeguard that data until it is returned.

4. Employees authorized to remove electronic data must consult with their supervisors and Information Security Officers (ISOs) to ensure that the data is properly encrypted and password-protected in accordance with VA policy.

5. Failure to comply with VA policy and regulations pertaining to cybersecurity and safeguarding confidential and Privacy Act-protected data may violate Federal law. Some of these laws carry civil and criminal penalties.

6. A number of VA directives exist to instruct employees on the proper handling of confidential and Privacy Act-protected data. These include VA Handbook 5011/5, Chapter 4, (Alternative Workplace Arrangements), Security Guideline for Single-User Remote Access, Revision 3.0, VA Directive and Handbook 6210, "Automated Information Security Procedures," and VA Directive and Handbook 6502, "Privacy Policy." If employees do not have written authorization to specifically remove confidential and Privacy Act-protected data from VA's premises, they must refrain from doing so.

Page 2.

VA IT Directive 06-2, Safeguarding Confidential and Privacy Act-Protected Data
At Alternative Work Locations

7. In the event that an employee loses confidential or Privacy Act-protected data, the employee must report the loss immediately to the facility or staff office ISO and privacy officer, and to the employee's immediate supervisor. Senior management should be informed immediately by the supervisor, who will further inform those in the chain of command.

8. All VA senior management officials are directed to ensure that employees under their supervision fully comply with this mandate immediately.



R. James Nicholson