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 Kev 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.

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