Department of Veterans Affairs
Washington, DC 20420

VA Directive 6600
Transmittal Sheet
February 26, 2007

RESPONSIBILITY OF EMPLOYEES AND OTHERS SUPPORTING VA IN PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

1. REASON FOR ISSUE: To issue policy requirements for the Department of Veterans Affairs (VA) on protecting personally identifiable and sensitive information on veterans, their family members, and employees.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: Numerous measures are being implemented to increase the security of sensitive data.

3. RESPONSIBLE OFFICE: The Office of Information and Technology (OI&T), 810 Vermont Avenue, NW, Washington, DC 20420, is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None.

5. RESCISSION: None.

Certified By:

Robert T. Howard
Assistant Secretary for
Information and Technology

R. James Nicholson
Secretary

Distribution: Electronic

RESPONSIBILITY OF EMPLOYEES AND OTHERS SUPPORTING VA IN PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

1. PURPOSE AND SCOPE

a. This directive establishes Department of Veterans Affairs (VA) policy toward protecting the personal data of all individuals, including veterans, dependents and employees. This policy extends the protections stated to all data formats and media, including electronic, paper and oral information.

b. VA must ensure that an information security program is in effect to ensure that sensitive data, primarily PII, is neither mismanaged nor used for any unauthorized purpose. Veterans, their families and employees have a right to expect that VA employees, and those who support VA, will take all necessary precautions to safeguard their personal information.

c. The essential aspect of protecting sensitive information is the awareness and individual responsibility of our employees. It is required that all VA employees treat the sensitive information of others the same as they would like theirs to be treated. To that extent, the VA has enacted the following key activities:

(1) Encrypted Government owned laptops

(2) Expanded the use of Public Key Infrastructure (PKI)

(3) Intensified Cyber Security and Privacy Training

(4) Initiated annual Computer Security Awareness Week

(5) Increased communications with employees

(6) Enhanced tracking and monitoring of reported incidents

(7) Created an Incident Resolution Core Team (IRCT)

(8) Enhanced oversight and accountability of all data

(9) Implemented the DS-ASC (Data Security – Assessment and Strengthening of Controls) Program

2. POLICY

a. VA must achieve the ***Gold Standard*** in data security. In order to meet this goal, VA will thoroughly examine every aspect of the VA information security program to

ensure that sensitive data, primarily PII, is neither mismanaged nor used for any unauthorized purpose.

b. VA must emphasize the importance of continuing its vigilance and strong focus on protecting the personal and sensitive data of veterans, their family members, and employees. To this effort, VA will continue to reinforce the actions already taken and implement others that will further enhance VA's posture in the protection of sensitive information. There must be heightened and constant awareness of our responsibilities regarding the protection of sensitive data.

3. RESPONSIBILITIES. All Under Secretaries, Assistant Secretaries, and Other Key Officials are responsible for the following:

a. Communicating this policy to all employees in their organizations and evaluating the security and privacy awareness activities of each organization in order to set clear expectations for compliance with security and privacy requirements and to allocate adequate resources to accomplish such compliance.

b. Developing mechanisms for communicating, on an ongoing basis, each workforce member's role and responsibilities specific to data security and privacy policies and practices that will enhance our security and privacy culture.

4. DEFINITION

Gold Standard for Data Security – system-wide strategies that promote data security awareness among all employees, and a change in the culture and capability in all VA facilities and remote locations (as defined in VA Strategic Plan FY 2006-2011).

5. REFERENCES

a. 40 U.S.C. Section 11101, Definitions

b. 44 U.S.C. Section 3544

c. VA Directive and Handbook 6210, Automated Information Security Procedures

d. VA Directive and Handbook 6502, Privacy Policy

e. VA Strategic Plan FY 2006-2011