Department of Veterans Affairs
Washington, DC 20420

VA Directive 6609
Transmittal Sheet
November 9, 2007

MAILING OF PERSONALLY IDENTIFIABLE AND SENSITIVE INFORMATION

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, beneficiaries**,** and employees transmitted through the mail.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: Numerous measures are being implemented to increase the security and protection of mail.

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: VA Directive 6340, Mail Management.

5. RESCISSION: None.

Certified By:

/S/
Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

/S/
Robert T. Howard
Assistant Secretary for
Information and Technology

Distribution: Electronic

MAILING OF PERSONALLY IDENTIFIABLE AND SENSITIVE INFORMATION

1. PURPOSE AND SCOPE

a. This directive supplements existing Department of Veterans Affairs (VA) mail policy to ensure the protection of the Personally Identifiable Information (PII) of all individuals, including veterans, dependents and employees. This policy is effective immediately, and applicable department-wide to all employees, contractors, and volunteers.

b. 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 (social security numbers, service numbers, pay stubs) the same as they would like theirs to be treated.

2. POLICY

a. All mail under the jurisdiction of the VA will be handled by the most secure economical and effective means. VA must especially protect personal information that is mailed. Extraordinary procedures must be used. Sensitive information that is lost, or mail that is sent to the wrong recipient, or tapes that are stolen can result in actual or potential identity theft and personal hardship to veterans. In order to meet this goal, effective immediately the following procedures will be implemented agency wide:

(1) Mail being sent to veterans, dependents, and employees does not require that it be sent via a secured delivery service or other secured delivery service unless the program office sending the mail makes a determination that the criticality of the mail demands it. This directive also covers other sensitive Department data that requires protection.

(2) Mail within the VA that contains documents , such as claims folders, must always be sent via a secure delivery service that tracks mail from pick-up to delivery. Notification procedures by both the originating and receiving office must also be employed. For mail (field station to field station or field station to business partner and vice versa) the originating office should alert the receiving office that a package with PII is on its way. Generally, it is preferable to mail copies of veterans' documents because of the possibility of loss or misplacement of the originals.

(3) All outgoing bulk or batch mail, between VA locations, or VA business partner (field station to field station or field station to business associate and vice versa) traditional mail (printed copy) which contains PII must be shipped via a secure delivery service that tracks mail from pick-up to delivery. Notification procedures by both the shipper and receiver must also be employed. An example of a service which provides this type of online tracking system is FedEX InSight. Field station to field station or field station to business associate and vice versa) shipments, the originating office should

alert the receiving office that a package with PII is on its way. An example of this is the USPS "Registered Mail" service.

NOTE: Mail that contains the PII of a single veteran generally does not require tracked shipping unless it contains the original documents.

(4**)** All outgoing (field station to field station or field stations to business associate and vice versa) magnetic, optical, and electronic tapes containing bulk or batch PII must be shipped using the equivalent of a hard-cover, locking container via a secure delivery service that tracks the device from pick-up to delivery. An example is the UPS "Turtle". For added protection, the hard-cover container may be placed in an unmarked shipping box. Based on a case-by-case risk assessment, shipments of this PII may be shipped by a more secure delivery service. An example is the FedEx "White Glove" service. The cost and custody of these containers and service will be the responsibility of the data owner.

(5) All outgoing mail or shipments between VA and the Federal Records Centers of hard copy original records containing PII must be shipped via a shipping or delivery service that tracks mail from pick-up to delivery. In addition, the packaging or boxes containing the records must be physically secured in an appropriate manner, e.g., double shrink-wrapped, that prevents inappropriate tampering or accidental loss of contents. Reference VA Handbook 6300.1, Records Management Procedures, Chapter Records Disposition Program.

(6) All outgoing mail to veterans, beneficiaries, outside business partners (e.g., Veteran Service Organizations and Health Plans or other members of the public, whether hard copy or electronic media such as CDs, which contains PII will continue to be shipped using the U.S. Postal Service unless the veteran, beneficiaries, outside business partners, or other members of the public requests mailing through a secure delivery service. In accordance with 38 CFR § 1.526 (j) a copy of the VA record requested to be transmitted by certified or registered mail, airmail, or special delivery mail will result in the postal fees being added to the other fees charged for providing such copies.

(7) Contractual agreements for contract mail staff must include Privacy Act clauses found in the Federal Acquisition Regulations (FAR): 52-224-1, Privacy Act Notification and 52.224.2, Privacy Act.

(8) Every article of mail which between VA locations or VA business associates which contains PII will be accompanied by a warning sheet that will be placed inside the package or envelope. The warning sheet will contain language that covers the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and associated criminal and civil penalties and or fines. A warning sheet shall not be used when sending mail to the veteran, beneficiary, outside business partner or other members of the public. See Figure 1.

(9) All incoming mail received and internal mail containing PII received and distributed within VA sites or facilities will be appropriately safeguarded and protected during all phases of the delivery process. Mail containing PII should not be left in unsecured or unattended areas.

(10) Special attention envelopes will be utilized for all internal mailings containing PII or other sensitive information dependent upon volume. Warning sheets will be inserted into these envelopes as cover sheets. See Figure 2. Organization originating offices are responsible for obtaining the special attention envelopes.

(11) All data tapes, CD's and backup tapes containing PII or other sensitive information must be shipped utilizing a delivery system that provides real time tracking from originator to addressee. Notification procedures by the originating office and receiving office must also be employed. Delivery will not be permitted on weekends or holidays unless the addressee can guarantee availability to receive the package on the weekend or holiday.

(12) All incidents and violations of PII must be reported by mail handlers to their Supervisors and appropriate Privacy officers in accordance with VA Handbook 6502, Enterprise Privacy Program

(13) Window envelopes/labels may reveal individual's names and addresses, but no other information. Social security numbers, claim numbers, date of birth or other sensitive PII, must not be revealed or viewable through a window envelope.

(14) Special care must be exercised to ensure that mail which arrives open is protected and that the mail is not sent or delivered to the wrong address.

(15) All additional costs associated with the requirements listed above will be borne by the sending office.

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 implementing processes within their organizations to comply with the requirements of this policy.

b. 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.

c. 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. DEFINITIONS

a. **Business Associate** – A business associate is an individual, entity, company, or organization who on behalf of VHA, as a HIPAA covered entity, performs or assists in the performance of functions or activities involving the use or disclosure of protected health information (PHI) or provides certain services to VHA and the provision of those services involves the disclosure of PHI by VHA.

b. **Business Partner** – A business partner is a non-contracted or non-VA individual, entity, company or organization who VA communicates with in the course of doing business (e.g., Veteran Service Organizations, health plans, and care providers).

c. **PII** - Information about an individual, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, etc. including any other personal information which is linked or linkable to an individual.

b. **Sensitive Information** - VA sensitive information is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance; confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

NOTE: Information that has been de-identified in accordance with the HIPAA Privacy Rule or is required to be released under the Freedom of Information Act is not sensitive information.

5. REFERENCES

a. VA Directive and Handbook 6340, Mail Management.

b. VA Handbook 6300.1, Records Management Procedures.

c. VBA IRM Handbook 8.02.01.HB1, Retiring Inactive Claims (XC) Folders for Deceased Veterans.

d. Freedom of Information Act, 5 U.S.C. 552

e. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164.

NOTICE!!!

1. Access to these records is limited to:

AUTHORIZED PERSONS ONLY.

2. Information may not be disclosed from this file unless permitted pursuant to 38 CFR 1.500 – 1.599.

3. These records may not be altered or destroyed except as authorized by 38 CFR 1.579.

4. The Privacy Act contains provisions for criminal penalties for knowingly and willfully disclosing information from this file unless properly authorized to do so. The HIPAA contains similar provisions.

(This notice should be placed inside of the envelope or package)

Figure 1

SPECIAL ATTENTION MAIL

To be opened only by _____

Office_____

Office Organizational Code _____

Figure 2