

MAILING OF SENSITIVE PERSONAL INFORMATION

- 1. REASON FOR ISSUE:** To revise policy requirements for the Department of Veterans Affairs (VA) for the protection of sensitive personal information (SPI) of Veterans and VA beneficiaries, their dependents, and VA employees, that is sent using mailing services.
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This directive alters the policy for the protection of mail containing SPI being sent between VA facilities, and to its business partners. This Directive sets forth the measures to be implemented in order to provide adequate protection for mail that contains SPI.
- 3. RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (OI&T) (005R), Office of Information Security (005R1), Office of Privacy and Records Management (005R1A), is responsible for the material contained in this directive.
- 4. RELATED DIRECTIVE:** VA Directive 6340, Mail Management.
- 5. RESCISSION:** VA Directive 6609, Mailing of Personally-Identifiable and Sensitive Information, dated November 9, 2007.

Certified By:

**BY DIRECTION OF THE SECRETARY
OF VETERANS AFFAIRS**

/s/
Roger W. Baker
Assistant Secretary for
Information and Technology

/s/
Roger W. Baker
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

MAILING OF SENSITIVE PERSONAL INFORMATION

1. PURPOSE AND SCOPE

a. This directive supplements existing Department of Veterans Affairs (VA) Directive 6340, Mail Management, by ensuring the protection of the sensitive personal information (SPI) of individuals, including Veterans, dependents, and VA employees. This policy is effective immediately, and is applicable Department-wide to all employees, trainees, contractors, appointees, and volunteers (VA personnel).

b. The awareness of VA personnel of their individual responsibilities and roles for the protection of SPI is the most essential element of protecting this information, which is vital to the fulfillment of VA's mission. Therefore, it is essential that rules be established for the mailing of SPI, and that these rules be communicated to all VA personnel.

2. POLICY

Mail containing information under VA control must be shipped via the most secure, economical, and effective means practicable. VA requires the protection of SPI during the mailing process. As such, special procedures must be used for its protection. Mail, including both hardcopy and electronic media, that is lost, sent to the wrong recipient, or stolen can result in identity theft. Identity theft may result in personal hardship to individuals, including Veterans, dependents, and VA personnel. In order to ensure the adequate protection of mailing both within and from VA, the following procedures will be implemented Department-wide:

a. Risk Analysis: Pursuant to the results of a risk analysis, a sender may provide additional security protections for categories of mail based upon its format and content. The risk analysis should be performed in consultation with the appropriate Privacy Officer, and if the mailing is in electronic form, the appropriate Information Security Officer should be included. If the risk analysis dictates, the media may be shipped via a delivery service that exceeds the minimum security requirements set forth in this Directive. The cost of any associated and additional services and will be the responsibility of the sender. If the purchase of containers is identified as a necessary security solution, all responsibilities associated with the custody of these containers will be the sender's responsibility.

b. Organizations that mail SPI should evaluate the business necessity of mailing the SPI and only transmit the minimum amount of Personally-Identifiable Information necessary to fulfill the purpose of the mailing.

c. Physical Integrity of Mail Packaging: Any person sending or redirecting mail must ensure that it is secured before placing it into the mail system.

(1) Envelopes, parcels, packaging or boxes containing SPI must be secured in a manner that prevents unauthorized access, tampering, or accidental loss of contents.

(2) Window envelopes must show the recipients' names and addresses, but no other information. Social security numbers, claim file numbers, dates of birth or other SPI, must not be viewable through a window envelope.

(3) Mailing labels must only display the amount of personal information necessary for the mail to reach the addressee.

(4) If a facility uses mass production letters with mail merge and the letters are run through a machine, the letters containing SPI must be sealed prior to delivering them to the Post Office or other shipping service, such as United Parcel Service (UPS) or Federal Express (FedEx).

d. Use of Secure Delivery and Package Tracking: Original documents, as defined in Paragraph 5b of this policy, must be sent via a secure delivery service that tracks mail from pick-up to delivery. Examples of services that provide this type of online tracking system are FedEx InSight, UPS Ground, and United States Postal Service (USPS) Priority Mail.

(1) Veterans' documents may be sent via untracked mail only if they are copies, not originals, due to the possibility of loss or misplacement.

(2) Outgoing mail that contains SPI and is sent to Veterans, dependants, business partners (e.g., Veteran Service Organizations and health insurance plans) or other members of the public will be shipped using the USPS **unless the package contains original documents** or VA agrees to a request from the Veteran, beneficiary, business partner, or other member of the public to use a tracked delivery service. In accordance with 38 C.F.R. § 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. However, if the originating office determines that the sensitivity of the mail demands it, the office may use a tracked delivery service for the mailing of copies. The originating office will bear the additional cost of using this shipping method.

e. Notice Sheets: Every individual article or grouping of mail, however sent, that contains SPI that is sent from VA to any VA personnel must be accompanied by a notice sheet containing language that explains that there are penalties for violations of the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. (See Appendix A). These notice sheets must be inserted as coversheets to the document.

(1) A notice sheet does not need to be used when sending mail if the information is being mailed to the individual to whom the information pertains or there is a signed

authorization from the individual to whom the information pertains for the release of the information to the recipient.

(2) Any disclosure of information protected by 38 U.S.C. § 7332 pursuant to the individual's written consent must be accompanied by the following statement, in accordance with 38 C.F.R. § 1.476:

"This information has been disclosed to you from records protected by Federal confidentiality rules (38 CFR Part 1). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 38 CFR Part 1. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient or patient with sickle cell anemia or HIV infection."

(3) The notice sheet must also be inserted into internal/interoffice mail envelopes (i.e., Optional Form 65Cs or "holey joes") that contain documents containing SPI.

f. Notification with Untracked Mail: If a tracking service is not used for bulk mailings containing non-original documents with SPI sent within and between VA entities (e.g., from a VA entity to a business partner or vice versa), the originating office must alert the receiving office that a package with SPI is on its way and the receiving office must inform the sending office of the package's arrival.

g. Internal Special Attention Mail: For all bulk mailings internal to VA that contain original documents with SPI (e.g., claim files), a stamp or label denoting that special attention is needed must be used. These stamps or labels must be placed inside the larger package but on the outside of any internal package, envelope or groupings of documents. This is done in order to facilitate delivery to the correct recipient. All stamps or labels must provide space for the name of the sender and his or her routing symbol, and the recipient's name and routing symbol (see Appendix B, Special Attention Mail). The sender must fill-in the information on the attention stamp or label. The sending office is responsible for the cost and for providing all special attention stamps or labels.

h. Mail Containing Electronic Media: Electronic media (e.g., CDs) that contains SPI must be encrypted and password protected in accordance with the current requirements of VA Handbook 6500, Information Security Program, with respect to storage of VA information on portable storage devices and shipped via a secure delivery service that tracks the mail from pick-up to delivery.

i. Exceptions: Encryption is not required to mail electronic media (e.g. CD or DVD) for the following:

(1) Mailing records containing the SPI of a single individual to:

(a) That person (e.g. the Veteran's, beneficiary's, dependant's, or employee's own information) or to that person's legal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written waiver of the individual. Such information may be mailed via USPS regular mail unless tracked delivery service is requested and paid for by the recipient.

(b) A business partner such as a health plan or insurance company, pursuant to a documented risk assessment. The risk assessment should be performed in consultation with the appropriate Information Security Officer.

(c) A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding.

(d) Congress, law enforcement agencies, and other governmental entities.

(2) Mailing of electronic records containing SPI to a person or entity that does not have capability to decrypt it:

Such media must be password-protected, and the password must be transmitted separately from the electronic media containing the SPI (e.g., by telephone, email, or separate mailing). These media must be shipped via a secure delivery service that tracks the mail from pick-up to delivery. If these items are shipped in bulk, the delivery service must use the equivalent of a hard cover, locking container. This locking container service is available from certain shipping companies.

j. Incoming Mail: All incoming mail containing SPI will be appropriately safeguarded during all phases of the delivery process. Mail known to contain SPI must not be left in unsecured or unattended areas.

k. Off Duty Hours Shipments: All facilities are responsible for ensuring the security of deliveries received during off duty hours. This includes deliveries made during the late evening, and on holidays or weekends.

l. Privacy Incidents: Where SPI is divulged to someone other than the addressee, it is a privacy incident unless the person to whom it is divulged would ordinarily open mail in order to ensure that it is properly routed for action. In accordance with VA policy, all privacy incidents must be reported to the supervisor and Privacy Officer of the individual who makes the discovery.

m. Alternative Transmission: Electronic transmission of documents should be explored as an alternative to mailing wherever possible in order to provide maximum security and to reduce the cost of the transmission of information. All electronic transmissions must be sent within the confines of existing VA privacy and information security policies.

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

- a. Promulgating appropriate procedures or policies in support of this Directive;
- b. Conducting risk assessments to evaluate the risks associated with the mailing of documents containing SPI and adjusting internal policies and practices accordingly;
- c. Communicating this policy to all employees in their organizations and implementing policies and processes within their organizations to comply with the requirements of this policy; and
- d. Ensuring that measures are adopted to assure the confidentiality of SPI found in both internal and external mailings, and putting measures into place to prevent the divulgement of SPI to any person who does not have a need to know that information for the performance of his or her official duties in support of the mission of VA and for the purpose for which the records were originally created.
- e. Determining methods for adding postal fees and other fees charged when VA agrees to provide to Veteran, beneficiary, business partner, or other member of the public with copies of VA records using certified or registered mail, airmail, or special delivery mail.

4. REFERENCES

- a. 38 CFR Part 75, Information Security Matters
- b. 38 U.S.C. §§ 5701, 7332
- c. Freedom of Information Act, 5 U.S.C. § 552
- d. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, 45 C.F.R. Parts 160 and 164.
- e. Office of Management and Budget (OMB) Memo M-06-15, Safeguarding Personally Identifiable Information
- f. OMB Memo M-06-16, Protection of Sensitive Agency Information
- g. Privacy Act of 1974, 5 U.S.C § 552a
- h. VA Directive 6340, Mail Management.
- i. VA Directive 6502, VA Enterprise Privacy Program
- j. VA Handbook 6300.1, Records Management Procedures.

- k. VA Handbook 6500, Information Security Program
- l. VA Handbook 6500.6, Contract Security
- m. VBA IRM Handbook 8.02.01.HB1, Retiring Inactive Claims (XC) Folders for Deceased Veterans.

5. DEFINITIONS

a. **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 insurance plans, and health care providers). A business associate under the HIPAA Privacy Rule is a type of business partner.

b. **Original Document** – The best evidence of the contents of a document is the original of that document. For purposes of this directive, the term refers to the originals of documents used for evidentiary purposes which, if lost or destroyed, would be difficult or impossible to replace. Examples include service, medical or personnel records, marriage certificates, birth certificates, passports, and diplomas. A VA claims folder is an original document, even if it only contains copies.

c. **Personally-Identifiable Information (PII)** – For purpose of this Privacy Service Directive, PII is considered to be the same as VA Sensitive Information/Data. PII is any information about an individual that can reasonably be used to identify that individual that is maintained by VA, 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, telephone number, driver's license number, credit card number, photograph, finger prints, biometric records, etc., including any other personal information which is linked or linkable to an individual.

d. **Privacy Incident** - For purposes of this Handbook, a privacy incident is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for any other than an authorized purpose, have access or potential access to SPI in any usable form, whether physical or electronic. This term encompasses both suspected and confirmed incidents involving SPI.

e. **Sensitive Personal Information** – The term means any information about the individual maintained by an agency, including the following:

(1) Education, financial transactions, medical history, and criminal or employment history; or

(2) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records.

NOTICE!!!

- 1. Access to these records is limited to: AUTHORIZED PERSONS ONLY.**

- 2. Information may not be disclosed from this file unless permitted by all applicable legal authorities, which may include the Privacy Act; 38 U.S.C. §§ 5701, 5705, 7332; the Health Insurance Portability and Accountability Act; and regulations implementing those provisions, at 38 C.F.R. §§ 1.460 – 1.599 and 45 C.F.R. Parts 160 and 164.**

- 3. Anyone who discloses information in violation of the above provisions may subject to civil and criminal penalties.**

(This notice should cover any exposed text inside of the envelope or package.)

SPECIAL ATTENTION MAIL

Sender _____

Sender's Routing Symbol _____

To be opened only by _____

Recipient's Office _____

Recipient's Routing Symbol _____