Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6509
Transmittal Sheet
July 30, 2015

DUTIES OF PRIVACY OFFICERS

1. REASON FOR ISSUE: This directive assigns responsibilities to Department of Veterans Affairs (VA) Privacy Officers to ensure the protection of Personal Identifiable Information (PII), Protected Health Information (PHI), and Sensitive Personal Information (SPI) collected by VA.

PII and PHI are subsets of SPI. The term SPI will be used throughout the policy.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive:

a. Establishes a framework for general duties shared by Privacy Officers and categorizes specific responsibilities for organizational level- Privacy Officers;

b. Adds the newly established requirements of VA Directive 6508, Implementation of Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA), to the general duties of VA Privacy Officers; and

c. Institutes new responsibilities for Information Security Officers, Data Owners, System Managers/System Owners, Program Managers, and Project Managers to oversee and coordinate with Privacy Officers to ensure that privacy related laws, regulations, Office of Management and Budget (OMB) guidance, and VA policies and procedures are followed.

3. RESPONSIBLE OFFICE: Office of the Assistant Secretary for Information and Technology (005), Office of Information Security (005R), Office of Privacy and Records Management (005R1).

4. RELATED HANDBOOK: VA Directive 6502, VA Enterprise Privacy Program; VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment; Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment.

5. RESCISSION: Duties of Privacy Officers, August 13, 2009.

CERTIFIED BY:

/s/
LaVerne H. Council
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
LaVerne H. Council
Assistant Secretary for
Information and Technology

DUTIES OF PRIVACY OFFICERS

1. PURPOSE

a. The purpose of this directive is to define the roles of VA Privacy Officers through a hierarchical approach and to connect those roles with the objective of protecting VA's SPI. This methodology will enable Privacy Officers at all levels to accomplish their responsibilities in an efficient and effective manner. When executed, this policy will assist in fulfilling VA's promise to Veterans as well as their dependents and beneficiaries, to protect and properly safeguard their SPI.

b. This directive establishes general duties for Privacy Officers that encompass proactive measures limiting the collection of SPI to only that which is legally authorized; safeguard SPI to prevent unauthorized uses and disclosures; and mitigate the risk of harm when a privacy incident or breach of SPI occurs.

2. POLICY: In order to ensure privacy laws, regulations, OMB guidance, and VA policies and procedures are adhered to, VA will:

a. Ensure that every Administration, staff office, and facility has a designated Privacy Officer and notifies the VA Privacy Service (005R1A) of this designation, at least quarterly;

b. Support Privacy Officers in the performance of their official/designated duties by:

(1) Providing guidance, expectations, and requirements stipulated in this directive for all Privacy Officers;

(2) Requiring the Privacy Service to administer Privacy Officer Professionalization training and recommend additional privacy related training;

(3) Affording adequate resources for the fulfillment of their official duties as stipulated in this directive and in VA Directive 6502, VA Enterprise Privacy Program; and

(4) Communicating and enforcing privacy laws, regulations, OMB guidance, and VA policies and procedures to properly protect VA SPI. Specifically:

(a) Privacy Act, which information pertaining to individuals that is retrieved by his/her name or some other personal identifier, such as birthdate; and

(b) Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations ("HIPAA Rules"), which set the standards for using and disclosing PHI and protecting PHI with administrative, technical, and physical safeguards;

c. **Privacy Officer General Duties:**

These general duties are applicable to all Privacy Officers regardless of the hierarchal level of the Privacy Officer, i.e., Administration, Staff Office, or Facility:

(1) Fulfill the Privacy Officer General Duties and the specific responsibilities for each level of Privacy Officer as provided in the responsibilities section of this Directive;

(2) Establish and implement Administration, Staff Office, and Facility policies that implement this Directive;

(3) Provide input for the development of privacy policies and initiatives, and as executed provide feedback on their effectiveness;

(4) Understand and apply federal law, regulations, guidance, and VA policy related to privacy;

(5) Serve as advisor and primary contact for privacy for their respective Administrations, Staff Offices and Facilities;

(6) Administer privacy training and/or awareness programs within their realm of responsibility;

(7) Identify and report on Privacy Act System of Records (SORs); work with the appropriate parties to ensure that system or records notices (SORNs) are published for all SORs; and update SORNS in accordance to VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records;

(8) Collaborate with local Record Officers or Records Liaison Officers to implement processes to facilitate proper retention and disposal of records, especially those that contain SPI;

(9) Ensure that when the Department collects information from members of the public that notice is provided through Privacy Act statements informing them of:

(a) Authority: The legal authority for collecting information through statute, executive order, and/or regulation;

(b) Purpose: The purpose for collecting the information and the manner in which it will be used;

(c) Routine Uses: VA routine uses detail the categories of users and the purpose of such use; and

(d) Access: VA procedures whereby an individual, by written request, can gain access to any record pertaining to that individual contained in the system of records, and how an individual can contest its contents;

(10) Create and promote a proactive privacy environment within their organizations;

(11) Respond appropriately to all privacy complaints under their purview of responsibility as stipulated in Directive 6502, VA Enterprise Privacy Program;

(12) Report all actual or suspected privacy incidents into the designated data breach reporting system within one hour of discovery or notification;

(13) Complete all assigned PTAs and PIAs, in accordance with VA Directive 6508, as applicable::

(a) Collaborate with Project Managers, Program Managers, ISOs, System Owners, System Managers, Integrated Project Teams (IPTs) via the Project Management Accountability System (PMAS) and the Privacy Service, as appropriate, to complete and submit PTAs to the Privacy Service;

(b) Coordinate with ISOs and System Managers/System Owners to ensure that all data and associated risks are identified and documented in all PIA submissions, as appropriate; and

(c) Work with Project Managers, Program Managers, ISOs, System Managers/System Owners and the Privacy Service to ensure that PIAs for each system within their area of responsibility are completed and submitted to the Privacy Service; and

(14) Facilitate the inclusion of privacy language in contracts ensuring VA PII, PHI, and SPI is properly safeguarded pursuant to the requirements of privacy laws, regulations, OMB guidance, VA policy, and the Federal Acquisition Regulations.

d. **Accountability for Safeguarding SPI:**

In accordance with “Rules and Consequences” section of OMB memorandum, M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, VA established respective responsibilities and consequences relative to safeguarding SPI included in VA Handbook 5021/15, Employee/Management Relations, “Table of Penalties for Title 5 and Title 38 Employees.” The corrective measures are commensurate with level of responsibility and type of SPI involved. Additionally, applicable Privacy and Labor laws, regulations, case law, VA policies, and any relevant collective bargaining agreements are used alongside the “VA Table of Penalties for Title 5, Hybrid Title 38 and title 38 Employees” when determining employee disciplinary action.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs.** The Secretary has designated the Assistant Secretary for Information and Technology as the Department’s CIO, and the senior agency official for privacy (SAOP) responsible for the VA Information Security and Privacy Programs.

b. **AS/IT.** The AS/IT, as the VA CIO and SAOP, will:

(1) Establish an enterprise-wide Privacy Program and provide oversight and guidance related to the protection of throughout VA;

(2) Have overall responsibility and accountability for VA privacy issues and for ensuring VA's implementation of privacy protections, including compliance with federal laws, regulations and policies related to information privacy;

(3) Oversee, coordinate, and facilitate compliance efforts, including reviewing VA information privacy practices and procedures for relevance and completeness;

(4) Ensure that VA employees and contractors are provided appropriate privacy awareness training programs;

(5) Maintain a central policy-making role in VA's development and evaluation of legislative, regulatory, and other policy proposals implicating privacy issues;

(6) Designate the Deputy Assistant Secretary (DAS), Office of Information Security, as the principal Department official responsible for ensuring VA compliance with privacy law, regulations, policies, and standards;

(7) Require that adequate staff and funding resources are employed to properly fulfill all privacy-protection functions; and

(8) Lead in responding to information security and privacy breaches.

c. **Deputy Assistant Secretary (DAS), Information Security.** The DAS will:

(1) Direct all VA information protection and Enterprise-wide Privacy Program activities;

(2) Perform all privacy duties and responsibilities as designated by the AS/IT;

(3) Set the direction and strategy for the development and implementation of privacy policy, guidelines, and procedures to comply with federal law, regulation, guidance, and policy;

(4) Coordinate with the Assistant Secretary for Operations, Security and Preparedness on matters related to privacy;

(5) Define information protection and risk management activities as related to privacy and ensure Privacy Service and Enterprise Risk Management (ERM) will organize and conduct ongoing privacy compliance monitoring assessments in facilities and coordinate with Administration and facility Privacy Officers; and

(6) Set requirements for privacy awareness training programs.

d. **Director, Office of Privacy Records Management (OPRM).** The Director will:

(1) Perform all privacy duties and responsibilities as designated by the DAS, Information Security;

(2) Oversee the continual development, issuance, monitoring, and implementation of VA privacy policies and procedures to comply with federal law, regulations, guidance and VA Directives;

(3) Provide leadership and direction in collaboration with appropriate senior officials to ensure that all privacy issues are resolved in a timely and appropriate manner;

(4) Facilitate coordination to properly process PII and comply with the VA Fair Information Practice Principles;

(5) Oversee the administration of the process for receiving, documenting, tracking, investigating, and taking action on all privacy complaints of actual or suspected privacy incidents involving SPI in coordination and collaboration with AS/IT and the breach response team, when necessary;

(6) Oversee the coordination and maintenance of a privacy incident reporting and notification system, in accordance with applicable federal law, OMB guidance, and Department of Health and Human Services (HHS) requirements, and VA policy;

(7) Coordinate with the Director, Privacy Service, under the guidance of the AS/IT to establish policies and procedures on reporting, tracking, auditing, and resolving VA privacy complaints, violations, and data breaches within VA;

(8) Issue guidance concerning privacy reviews and the contents of reports generated as a result of the privacy reviews;

(9) Coordinate with AS/IT and DAS, Office of Information Security, in monitoring the development and delivery of a privacy training, awareness, and training program, consisting of both an orientation privacy training and on-going training and awareness campaigns, including role-based training on safeguarding SPI to all VA staff, volunteers, contractors, Business Associates (BAs), and other third parties, as appropriate;

(10) Oversee the development of security and privacy controls that ensure compliance with federal law, VA Fair Information Practice Principles and policy, including the necessary controls to ensure only those authorized to process the information to fulfill their assigned responsibilities at VA have access to SPI and that the other minimum necessary standards of the Privacy Act and the HIPAA Privacy Rule are met for the collection, use, and disclosure of SPI;

(11) Establish SORNs and complete PIAs for information technology (IT) systems that collect, maintain, use, or disseminate SPI;

(12) Perform all PIA duties and responsibilities as designated by the ASIT; and

(13) Ensure that PTA and PIA templates and instructions are made available to the Privacy Officers, System Managers and ISOs and that guidance and assistance is provided that meets OMB and VA requirements.

e. **Director, Privacy Service.** The Director will:

(1) Perform all privacy duties and responsibilities as designated by the Director, OPRM;

(2) Collaborate with the Administrations and Staff Offices as needed to communicate and implement the requirements set forth by this Directive;

(3) Develop, review, coordinate, and monitor VA privacy policy in conjunction with policy efforts by all VA Administrations and Staff Offices;

(4) Provide technical guidance to Under Secretaries and Assistant Secretaries regarding requirements for the protection of all SPI;

(5) Collaborate with VA entities responsible for the development of VA policy and guidance pertaining to responsibilities of Privacy Officers, including Privacy Officers ensuring compliance with the HIPAA Privacy and Security Rules, as applicable;

(6) Develop, facilitate, and monitor delivery of annual privacy awareness training and monitor on-going training and awareness campaigns on privacy;

(7) Provide VA policy and guidance on the development and implementation of periodic role-based privacy awareness training;

(8) Provide basic privacy training, resources, guidance, and assistance to all Privacy Officers;

(9) Provide resources and training related to the professionalization of Privacy Officers;

(10) Assist in the development, implementation, and maintenance of VA privacy policies and procedures in coordination with Privacy Officers and the Office of the General Counsel (OGC) to ensure adherence with federal law and other VA policies and procedures;

(11) Maintain an online directory of all employees who are designated as Privacy Officers;

(12) Establish VA policies, procedures, and guidance on the development, publication, and biennial review of SORNs;

(13) Require privacy reviews by Under Secretaries and Assistant Secretaries of all PII, PHI, and SPI for which they are responsible and a report on the privacy review to show how this data is used;

(14) Facilitate and prepare all required privacy-related reporting, to be approved and submitted by the AS/IT, DAS Office of Information Security and the Director, OPRM, as required by applicable law and VA policy and procedures;

(15) Establish VA policy and procedures on the tracking, auditing, and resolution of VA privacy violations and complaints to:

(a) Ensure that a VA system to track privacy complaints and reports of alleged, suspected, or actual breaches involving SPI, or alleged violations of applicable privacy laws and VA policies, is maintained;

(b) Maintain audit records and documentation provided by tracking system;

(c) Report to oversight agencies and VA management, as required by law and VA policy, on privacy violations and complaint resolution measures taken within VA; and

(d) Provide oversight and guidance to ensure VA compliance with applicable federal law as it relates to the tracking of privacy complaints or actual or suspected breaches involving SPI throughout VA.

(16) Chair a monthly Privacy Steering Committee Meeting, consisting of representatives of each Administration and Staff Office, to discuss privacy concerns and changes in the field of privacy and as the focal point for collaboration across the Department, and shall:

(a) Provide guidance of VA privacy initiatives within the scope of the Privacy Service; and

(b) Identify and facilitate privacy best practices for the protection of SPI.

(17) Establish Department-wide requirements and guidance on the development and completion of PTAs and PIAs as designated by the Director, OPRM by:

(a) Sustaining a PTA and PIA template for use when performing PTAs and PIAs on VA information systems in accordance with the E-Government Act and Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance;

(b) Ensuring that guidance and assistance is provided in compliance with the E-Government Act of 2002; prescribed NIST standards, and other VA policies;

(c) Approving PTAs for signature by the Administration/Facility Privacy Officers and System Owners;

(d) Approving PIAs for signature by the Administration/Facility Privacy Officers, Information Security Officers, and System Owners;

(e) Submitting completed PIAs to the CIO as appropriate;

(f) Publishing PIAs on the VA website; and

(g) Developing and promulgating privacy-related duties and responsibilities for all Privacy Officers.

f. **Director, Records Management Service**. The Director will:

(1) Perform all PIA related duties and responsibilities as designated by the Director of OPRM; and

(2) Review Information Collection Requests (ICR) to determine whether the information requested contains SPI that could potentially require a PIA; and

g. **Under Secretaries, Assistant Secretaries, and Other Key Officials.**

These officials will:

(1) Provide the resources necessary to establish designated Privacy Officers;

(2) Periodically reassess the necessity for additional Privacy Officers;

(3) Designate dedicated Administration-level Privacy Officers based on organizational needs and legal requirements and notifies the Privacy Service (005R1A) of this designation, at least quarterly;

(4) Oversee the development of administration specific policies necessary to implement the provisions of VA Directive 6502, VA Enterprise Privacy Program;

(5) Periodically review the skill sets, statuses, and effectiveness of all Privacy Officers in their organizations and assess the adequacy of current staffing levels at all VA facilities including, but not limited to: VA Medical Centers and VBA Regional Offices to ensure that at least one Privacy Officer is designated at each office under their purview, and that the VA Medical Centers' Privacy Officers comply with the Privacy Act, the HIPAA Privacy and Security Rules, and all other privacy related laws, ,regulations, OMB guidance, NIST standards, and VA policies;

(6) Monitor compliance with VA and Administration-level privacy policies and develop sanctions for noncompliance;

(7) Develop and implement plans to eliminate the collection and use of SSNs where the collection or use of SSNs is not required by law or mandated by the mission of the Department as set forth by the Secretary; and

(8) Ensure that all Privacy Officers reporting structure is aligned under the Office of the Facility or Program Office Director

h. **Office of General Counsel (OGC).** The OGC will be requested to:

(1) Interpret laws and directives applicable to VA privacy issues and responsibilities;

(2) Advise Administrations and Staff Offices on compliance with federal privacy law and VA policy; and,

(3) Provide legal advice and services on matters of privacy and related responsibilities.

i. **Program Directors/Facility Directors.** Program Directors/Facility Directors will:

(1) Designate in writing program/facility-level Privacy Officers and Alternate Privacy Officers based on organizational needs and legal requirements, and report this designation and any changes to the Privacy Service;

(2) Periodically reassess the necessity for additional Privacy Officers;

(3) Ensure compliance with established administration-level specific policies that adhere to the provisions codified in VA Directive 6502, VA Enterprise Privacy Program;

(4) Periodically review the skill sets, statuses, and effectiveness of all Privacy Officers in their organizations and prescribe to Under Secretaries, Assistant Secretaries, and Other Key Officials the adequacy of current staffing levels at all VA facilities;

(5) Ensure compliance to VA and Administration-level policies to eliminate the collection and use of SSNs where the collection or use of SSNs is not required by law or mandated by the mission of the Department as set forth by the Secretary; and

(6) Ensure that all Privacy Officers reporting structure is aligned under the Office of the Facility or Program Office Director.

j. **Information Security Officers (ISOs).** ISOs will:

(1) Include Privacy Officers as part of the IPT that safeguards VA sensitive information in meeting the legal and policy requirements of PTAs and PIAs;

(2) Collaborate with Records Management Officers and Privacy Officers to ensure the proper disposal of files and records;

(3) Work with Project Managers, Program Managers, System Managers, System Owners, Privacy Officers, and the Privacy Service to complete and finalize PTAs in a manner that will ensure approval by the VA Privacy Service;

(4) Coordinate with appropriate Privacy Officers and System Managers to ensure that all data and associated risks are identified and documented in all PIA submissions, as appropriate;

(5) Coordinate with the facility Privacy Officer for the assurance of reasonable safeguards as required by the Privacy Act, HIPAA Privacy and Security Rules, and other applicable statutes, regulations, and OMB guidance;

(6) Work with appropriate Privacy Officers, Program Mangers, Project Mangers, System Managers, System Owners, and the Privacy Service to ensure that the PIAs for each system within their area of responsibility is of a quality that will reasonably ensure its approval by the VA Privacy Service; and

(7) Coordinate with Staff Office and facility level Privacy Officers and Directors to ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals within their program areas and in the facilities to which they are designated or assigned.

k. **Data Owners**. Data Owners (DO) will:

(1) Work with the Privacy Officers, Program Managers, Project Managers, Information Security Officers, and System Managers/System Owners to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions;

(2) Collaborate with the System Owners to ensure that data are used and disclosed in accordance with the uses and disclosures set forth in the SORNs and other types of privacy notices, including a HIPAA Notices of Privacy Practices (NoPP), when applicable;

(3) Ensure that all PIAs for systems maintaining SPI are complete and accurate;

(4) Work with System Owners and the Privacy Service to establish Privacy Act statements for all collections of SPI; complete and approve PIAs before any collection of SPI begins; and publish requisite SORNs; and

(5) Use and disclose SPI in accordance with applicable law and assist individuals in exercising their rights with respect to their information.

l. **System Managers/System Owners.** System Managers/System Owners will:

(1) Assure that all proper measures are taken to safeguard and protect the integrity, availability, and confidentiality of SPI in accordance with federal security and privacy laws, policies, and guidance on all systems for which they are responsible;

(2) Work with Privacy Officers, Project Managers, ISOs, System Managers/System Owners, and the Privacy Service to complete and finalize PTAs and submit for VA Privacy Service approval;

(3) Work with appropriate Privacy Officers, Program Managers, Project Mangers, ISOs, System Managers, and the VA Privacy Service to ensure that the PIAs for each system within their area of responsibility; and

(4) Work with Data Owners and the Privacy Service to publish new SORNs in the *Federal Register* and update all SORNs as required by federal law, policies, and guidance.

m. **Program Managers.** Program Managers will:

(1) Work with Privacy Officers, Project Managers, ISOs, System Managers, System Owners, and the Privacy Service to complete and finalize PTAs in a manner that will ensure approval by the Privacy Service; and

(2) Work with appropriate Project Managers, ISOs, System Managers, System Owners, and the Privacy Service to ensure that the PIAs for each system within their area of responsibility is of a quality that will reasonably ensure its approval by the Privacy Service and that PIAs are updated as needed.

n. **Project Managers.** Project Managers will:

(1) Work with Privacy Officers, Program Managers, ISOs, System Managers, System Owners, and the Privacy Service to complete and finalize PTAs in a manner that will ensure approval by the VA Privacy Service; and

(2) Work with appropriate Program Managers, ISOs, System Managers, System Owners, and the Privacy Service to ensure that the PIAs for each system within their area of responsibility is of a quality that will reasonably ensure its approval by the Privacy Service and that PIAs are updated as needed.

o. **Administration Privacy Officers.** Administration Privacy Officers will:

(1) Implement the Privacy Program within their respective areas;

(2) Monitor and administer VA privacy training and awareness within their realms of responsibility by providing:

(a) General privacy and HIPAA privacy training, as appropriate; and

(b) VA National Rules of Behavior training.

(3) Provide instruction regarding responsibilities and requirements for implementation of the Privacy Program within field-based facilities, and report to the Privacy Service of this designation at least quarterly;

(4) Provide guidance to Facility-level Privacy Officers within their Administrations, as appropriate, in order to ensure that policies and practices at those Privacy Officers' facilities adhere to federal privacy laws and VA and Administration policies and procedures;

(5) As appropriate, coordinate with ISOs and System Managers to ensure that all data and associated risks are identified and documented in PTA and PIA submissions to the Privacy Service; and

(6) Work with the Privacy Service and VA Enterprise Risk Management (ERM) to ensure facility Privacy Officers are available to assist in compliance monitoring assessments.

p. **Staff Office Privacy Officers.** VA Staff Office Privacy Officers will:

(1) Deliver initial and annual privacy orientation and general privacy and VA National Rules of Behavior training to all employees, volunteers, medical and professional staff, contractors, and other third parties within their program areas, as appropriate;

(2) Coordinate with their ISOs and Staff Office Directors to ensure compliance with privacy practices and consistent application of sanctions for failure to comply with VA privacy policies for all Individuals within their program areas;

(3) Conduct walk-throughs of all areas of their assigned offices to ensure that privacy-related policies are being followed and provide guidance, as needed, to employees on proper procedures for the handling of SPI, at least quarterly;

(4) As appropriate, coordinate with ISOs and System Managers to ensure that all data and associated risks are identified and documented in PTA and PIA submissions to the Privacy Service; and

(5) Collaborate with the Privacy Service, Administration, and Facility-level Privacy Officers to ensure compliance with all VA privacy policy requirements.

q. **Facility-level Privacy Officers.** Facility-level Privacy Officers will:

(1) Coordinate with the Privacy Service, Administration-level, and Staff Office Privacy Offices to ensure that privacy laws, regulations, OMB guidance, and VA policies and procedures are adhered to;

(2) Coordinate and collaborate with the Privacy Service on Department-wide training, communications, reporting initiatives, and compliance requirements;

(3) Coordinate with the facility ISOs for the assurance of reasonable safeguards as required by the Privacy, HIPAA Privacy and Security Rules, other applicable statutes, regulations, and OMB guidance;

(4) Acquire the necessary knowledge and expertise in information privacy policies and procedures to develop effective and comprehensive privacy programs at their facilities that comply with the VA privacy program requirements;

(5) Deliver or ensure delivery of initial and annual privacy orientation and general privacy and VA National Rules of Behavior training to all facility employees, volunteers, contractors, and other third parties, as appropriate;

(6) Investigate all privacy related complaints and incidents and prepare reports and briefings for facility executive leadership

(7) As applicable to VHA Privacy Officers, provide HIPAA training to facility employees, volunteers, contractors and other third parties, as appropriate;

(8) Coordinate with the facility ISO, OGC and facility management to ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for individuals in the facilities to which they are designated or assigned;

(9) Maintain knowledge of federal privacy laws, regulations, guidance and VA policies to ensure implementation and compliance;

(10) Promote enterprise or Administration-sponsored activities designed to foster privacy awareness within the facilities;

(11) Conduct a walkthrough of all areas of the facility to ensure that privacy-related policies are being followed and provide guidance, as needed, to employees on proper procedures for the handling of SPI, annually;

(12) Work with facility personnel involved with any aspect of the collection, maintenance, protection, and disposal of SPI to ensure full compliance with records management and privacy laws, regulations, OMB guidance, VA policy and procedures; and

(13) Work with VA Privacy Service and VA Enterprise Risk Management (ERM) in conducting site visits to ensure privacy compliance monitoring assessments are completed in their respective facility.

4. REFERENCES.

The Enterprise-wide VA Privacy Program has its foundation in federal statutes, Executive Orders, OMB directives, and VA Directives, Handbooks and guidance including, but not limited to, the authorities described below.

a. E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899 (2002).

b. Electronic Communications Privacy Act of 1986, 18 U.S.C. Chapter 121 (October 21, 1986).

c. Electronic Records Management, 60 Fed. Reg. 44634 (1995).

d. Employee Suitability Determinations and Investigations, 5 CFR Parts 731, 732, and 736.

e. Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, codified at 42 U.S.C. § 2000ee-3.

f. Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.

h. Fraud and Related Activity in Connection with Access Devices and Computers, 18 U.S.C. §§ 1029-1030.

i. Freedom of Information Act (FOIA), 5 U.S.C. § 552; Release of Information from Department of Veterans Affairs Records Other Than Claimant Records, 38 CFR §§ 1.550-557.

j. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 123 Stat. 226 (2009).

k. Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191,110 Stat. 1936 (1996), 42 USC §§ 1320d-d-8; 264(3).

l. HIPAA Privacy and Security Rules, 45 C.F.R. Parts 160 and 164.

m. National Institute for Standards and Technology Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide, August 8, 2012.

n. National Institute for Standards and Technology Special Publication 800-88, Revision 1, Guidelines for Media Sanitization, December 2014.

o. National Institute for Standards and Technology Special Publication 800-53, Revision 4, Appendix J, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

p. National Institute for Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

q. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, November 28, 2000.

r. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, March 02, 2006.

s. OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

t. OMB M-05-08, Designation of Senior Agency Official for Privacy, February 11, 2005.

u. OMB M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006.

v. OMB M-06-16, Protection of Sensitive Agency Information, June 23, 2006.

w. OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.

x. Privacy Act of 1974, 5 U.S.C. § 552a.

y. VA Directive and Handbook 0710, Personnel Suitability and Security Program, June 4, 2010.

z. VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology, July 28, 2000.

aa. VA Directive 6102, Internet/Intranet Services, July 15, 2008.

bb. VA Directive 6103, VA Electronic Mail System, March 23, 1998.

cc. VA Directive 6221, Accessible Electronic Information Technology (EIT), December 9, 2005.

dd. VA Directive 6361, Ensuring Quality of Information Disseminated by VA, September 2, 2004.

ee. VA Directive 6500, Managing Information Security Risk: VA Information Security Program, September 20, 2012.

ff. VA Directive 6507, Reducing the Use of Social Security Numbers, November 20, 2008.

gg. VA Directive 6508, Privacy Impact Assessments, October 15, 2014.

hh. VA Directive 6511, Presentations Displaying Personally-Identifiable Information, January 7, 2011.

ii. VA Directive 6515, Use of Web-Based Collaboration Technologies, June 28, 2011.

jj. VA Directive 6600, Responsibility of Employees and Others Supporting VA in Protecting Personally-Identifiable Information (PII), February 26, 2007.

kk. VA Directive 6609, Mailing of Sensitive Personal Information, May 20, 2011.

ll. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, August 19, 2013.

mm. VA Handbook 5021/15, Employee/Management Relations, “Table of Penalties for Title 5 and Title 38 Employees”, July 19, 2013.

nn. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records, June 6, 2010.

oo. VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Addresses, July 31, 2008.

pp. VA Handbook 6300.7, Procedures for Computer Matching Programs, October 8, 2011.

qq. VA Handbook 6301, Procedures for Handling Electronic Mail Records, April 24, 1997.

rr. VA Handbook 6309, Collections of Information, January 12, 2010.

ss. VA Handbook 6361, Ensuring Quality of Information Disseminated by VA, September 2, 2004.

tt. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Program, March 10, 2015.

uu. VA Handbook 6500, Appendix E, VA Privacy Controls, March 10, 2015.

vv. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), January 6, 2012.

ww. VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle, March 22, 2010.

xx. VA Handbook 6500.6, Contract Security, March 12, 2010.

yy. VA Handbook 6502.1, Privacy Event Tracking, February 18, 2011.

zz. VA Handbook 6502.3, Webpage Privacy Policy, June 3, 2011.

aaa. VA Handbook 6502.4, Privacy Act Review, November 16, 2009.

bbb. VA Handbook 6508.1, Privacy Impact Assessment (PIA), November 16, 2010.

ccc. VA IT Directive Memorandum 06-4, Embossing Machines and Miscellaneous Storage Devices, September 7, 2006.

ddd. VA IT Directive Memorandum 06-5, Use of Personal Computing Equipment October 5, 2006.

eee. 38 U.S.C. § 5701, Confidential Nature of Claims; 38 CFR §§1.500-527, Release of Information from Department of Veterans Affairs Claimant Records.

fff. 38 U.S.C. § 5705, Confidentiality of Medical Assurance Records; 37 CFR §§ 17.500-.511, Confidentiality of Healthcare Quality Assurance Review Records.

ggg. 38 U.S.C. §§ 5721-5727, Information Security, 38 CFR §§ 75.111-118.

hhh. 38 U.S.C. § 7332, Confidentiality of Certain Medical Records; 38 CFR §§ 1.460- 496, Release of information from Department of Veterans Affairs Records Relating to Drug Abuse, Alcoholism or Alcohol Abuse, Infection with the Human Immunodeficiency Virus (HIV), or Sickle Cell Anemia.

5. DEFINITIONS

a. **Business Associate:** A Business Associate is a person or entity who, other than in the capacity of a member of the covered entity work force: (1) on behalf of a covered entity processes PHI for a function or activity regulated by the HIPAA Privacy Rule, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or (2) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity where the provision of services involve the disclosure of PHI from such covered entity or from another BA of such covered entity to the person.

b. **Designated Privacy Officer:** For purposes of this Directive, a Designated Privacy Officer is an individual who has been designated by his or her management as the official Privacy Officer for a VA facility.

c. **Personally-Identifiable Information (PII):** For purposes of this Directive PII is considered to be the equivalent of VA Sensitive Information/Data. PII is any information about an individual that can be used to distinguish or trace an individual's identity, alone, or when combined with other information which is linked or linkable to a specific individual, 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, training, financial transactions, medical history, and criminal or employment history, etc. PII is also known as Sensitive Personal Information (SPI).

d. **Privacy Event.** A Privacy Event is a confirmed instance in which information protected by the Privacy Act of 1974, the HIPAA Privacy Rule, or other confidentiality provisions such as 38 U.S.C. 5701, 5705, or 7332 may have been improperly disclosed or used, and includes the loss, theft, or any other unauthorized access, or any other access than that which is incidental to the scope of employment, to data containing SPI in electronic, printed, or any other format, and results in the potential compromise of the confidentiality or integrity of the data regardless of the manner in which the breach might have occurred.

e. **Privacy Hierarchy:** A Privacy Hierarchy is composed of Privacy Officers in VA Administrations, Staff Offices, and Facilities aligned according to increasing responsibilities and authority over privacy-related matters.

f. **Privacy Impact Assessment (PIA).** A Privacy Impact Assessment is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and

policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

g. **Privacy Incident.** 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.

h. **Protected Health Information (PHI).** PHI, for purposes of this VA Privacy Service directive, will be considered a subcategory of PII. This term applies only to individually-identifiable health information that is under the control of VHA, as VA's only Covered Entity under HIPAA, or one of its Business Associates, such as OIT. PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium. PHI excludes employment records held by an employer in its role as employer, records of a person deceased for more than 50 years, and some training records. PHI includes genetic information.

i. **Privacy Reviews.** Privacy Reviews are a comprehensive compliance evaluation of privacy related practices throughout an organization. This evaluation would include but not limited to the following:

(1) Conducting detailed risk assessments of new or altered systems of records to ensure appropriate administrative, technical, and physical safeguards are established to protect records in the system from unauthorized disclosure, alteration or access; and

(2) Assessing the management of physical, administrative, and technical safeguards in place to prevent unauthorized disclosure or alteration of personal information in the system.

j. **Privacy Threshold Analysis (PTA).** A Privacy Threshold Analysis is a required document that serves as the official determination of whether a Department program or system has privacy implications, and whether additional privacy compliance documentation is required [e.g., Privacy Impact Assessment (PIA) or System of Records Notice (SORN)]. The PTA is built into departmental processes for technology investments and security. PTAs expire and must be reviewed and recertified when the system undergoes a major change as defined in OMB M-03-22 or every three years.

k. **Staff Office:** For purposes of this Directive, Staff Office refers to any of the 14 offices in the VA hierarchy that support the operations of the Department, but are not part of VA's three Administrations.

l. **Sensitive Personal Information (SPI).** SPI, as defined by 38 U.S.C. 5727(19), is any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) 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. For purposes of this directive, the term SPI is interchangeable with the term PII.

m. **System of Records (SOR).** A SOR is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

n. **System of Records Notice (SORN).** A SORN is a formal notice to the public published in the *Federal Register* that an agency is maintaining information about individuals and identifies the purpose for which such information is collected, from whom and what type of PII is collected, how the PII is shared externally through routine uses, and how to access and correct any such information maintained by the Department.

o. **System Owner.** A System Owner is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The System Owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements, the decision of who has access to the information system (and with what types of privileges or access rights) and the assurance that system users and support personnel receive the requisite security training (e.g., instruction in VA National Rules of Behavior).

p**. VA Sensitive Information/Data.** VA Sensitive Information/Data 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 disclosures, alteration, or destruction of the information and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission and proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.