Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6509
Transmittal Sheet
August 13, 2009

DUTIES OF PRIVACY OFFICERS

I. REASON FOR ISSUE: This Directive issues policy requirements for the Department of Veterans Affairs (VA) Privacy Officers' duties in the fulfillment of their positions as Privacy Officers to ensure that Personally-Identifiable Information (PII) about Individuals collected by VA is limited to that which is legally authorized and necessary, and is maintained in a manner that precludes unwarranted intrusions upon Individual privacy.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive lays out the role of Privacy Officers in order to ensure that they are aware of their responsibilities in the execution of their duties at each organizational level. It also establishes responsibility for the oversight of Privacy Officers.

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

4. RELATED HANDBOOK: None.

5. RESCISSION: None.

CERTIFIED BY:

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

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

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

Distribution: Electronic Only

DUTIES OF PRIVACY OFFICERS

1. PURPOSE

a. The purpose of this Directive is to define the role of Department of Veterans Affairs (VA) Privacy Officers in the protection of VA's holdings of Personally-Identifiable Information (PII), issue policy requirements for Privacy Officers' duties and to assign responsibility for their oversight.

b. The core duty of a Privacy Officer at each organizational level is to take proactive measures to help ensure that PII collected by VA is limited to that which is legally authorized and necessary, and is maintained in a manner that precludes unwarranted intrusions upon individual privacy, thereby, minimizing privacy events. Additionally, it is the defensive duty of a Privacy Officer to assist in mitigating damage when PII is compromised.

c. This Directive is required because of the increased availability and aggregation of PII, coupled with the proliferation of electronic databases, the internet and intranets, has exposed individuals to possible identity theft and required agencies to enhance methods to establish appropriate administrative, technical and physical safeguards to protect against anticipated threats. This Directive places VA's Privacy Officers as the first responders to privacy events when PII entrusted to VA has been compromised that could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

2. POLICY

a. After individual users, Privacy Officers collectively function as VA's greatest mechanism for the protection of the vast amounts of PII held by VA. In order to ensure that VA's Privacy Officers are able to perform their duties in the most efficient and effective manner, VA shall:

(1) Ensure that every VA Administration has a full-time Privacy Officer and every VA Staff Office has a designated Privacy Officer;

(2) Ensure that every VA Facility has at least a designated Privacy Officer;

(3) Support Privacy Officers in the performance of their official duties by:

(a) Providing clear guidance as to the expectations and requirements for all Privacy Officers;

(b) Providing adequate resources for the fulfillment of their official duties; and

(c) Providing professional advancement opportunities to Privacy Officers;

(4) Create, communicate, and enforce a set of clear rules governing the use of PII; and

(5) Make every effort to inform the public about how VA collects, stores, and uses PII by issuing Privacy Act statements at the point of collection.

b. VA will ensure that all Privacy Officers are trained and are familiar with basic concepts in the Privacy Act regarding PII collected by VA that may be retrieved by the name of the Individual or by some identifying particular assigned to the Individual, which information may be maintained in a VA system of records. This training shall be sufficient to ensure that Privacy Officers are able to advise their organizational elements that when collecting information from individuals that may be stored in a system of records, VA shall:

(1) Advise each Individual of the authority for the information collection;

(2) Advise the principal purpose for which the information is intended to be used; and

(3) Advise the effects, if any, of not providing all or any parts of the requested information.

c. VA will ensure that Privacy Officers with assistance from appropriate contracting officers and responsible officials understand that all contracts in which any VA-owned PII maintained by Business Associates contain the appropriate security and privacy clauses as required by Federal Acquisition Regulations, VA policy and other appropriate Federal authorities in order to ensure that VA data are always maintained in accordance with Federal law and VA policy.

d. VA will ensure that policies and procedures are in place to encourage Staff Office, Program Office, and Facility-level Privacy Officers; Information Security Officers (ISOs); and the respective Chief Information Officers (CIOs) to work together as the information protection team to assure the protection of VA Sensitive Data, and the fulfillment of all legal and policy-based reporting obligations.

3. RESPONSIBILITIES

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

b. **The Assistant Secretary for Information and Technology (AS/IT).** The AS/IT for Information and Technology, as VA CIO, shall:

(1) Establish and maintain procedures consistent with privacy law, applicable Office of Management and Budget (OMB) Guidelines, Circulars, and privacy-related Directives;

(2) Designate the Deputy Assistant Secretary (DAS), Office of Information Protection and Risk Management as the principal Department official responsible for ensuring Department-wide compliance with this Directive;

(3) Designate the Associate Deputy Assistant Secretary (ADAS), Office of Privacy and Records Management as the principal Department official responsible for overseeing the implementation of this Directive;

(4) Work with Under Secretaries, Assistant Secretaries, and Other Key Officials to ensure that any privacy reviews for all PII for which they are responsible are carried out, and that they report how such data are maintained; and

(5) Work with VA Assistant Secretaries of the Staff Offices, the Under Secretary for Health, the Under Secretary for Benefits, and the Under Secretary for Memorial Affairs to ensure that the VA Privacy Program operates in a concerted and consistent manner.

c. **The Deputy Assistant Secretary (DAS), Office of Information Protection and Risk Management.** The DAS shall:

(1) Direct all VA information protection and privacy programs;

(2) Define information protection activities as related to privacy;

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

(4) Recommend for selection the ADAS, Office of Privacy and Records Management; and

(5) Collaborate with the Executive Director of Oversight and Compliance; DAS, IT Enterprise Strategy, Policy, Plans and Programs; DAS, IT Resource Management; DAS, Enterprise Development; DAS Enterprise Operations and Field Development; and the DAS for Human Resources Management, as needed, for the implementation of this Directive.

d. **The ADAS, Office of Privacy and Records Management.** The ADAS shall:

(1) Perform all privacy duties and responsibilities as designated by the DAS, Office of Information Protection and Risk Management;

(2) Serve as the senior executive for privacy for VA;

(3) Have overall responsibility for oversight of the Department-wide Privacy Program;

(4) Develop, issue, monitor and implement VA privacy policies and procedures in accordance with Federal law, regulations, guidance, and VA Directives;

(5) Recommend for selection a Director of the Privacy Service;

(6) Facilitate cooperation among all VA Administrations, Staff Offices, and Other Key Officials regarding VA's Privacy Program;

(7) Administer the process for receiving, documenting, tracking, investigating, and taking appropriate action, on all privacy complaints or actual or suspected privacy events involving PII, in coordination and collaboration with other offices serving similar functions and, when necessary, legal counsel;

(8) Update, on a continuous basis, policies regarding the maintenance of PII as legal requirements and other circumstances may dictate;

(9) Coordinate with the ADAS, Office of Risk Management and Incident Response to provide a privacy notification system, in accordance with applicable Federal law that pertains to all PII;

(10) Issue guidance concerning the conduct and use of privacy reviews, and the contents of reports generated as a result of the privacy reviews;

(11) Coordinate and monitor the delivery of privacy training, consisting of both an initial privacy orientation, and on-going education and awareness campaigns, to all VA employees, volunteers, medical and professional staff, contractors, and other third parties as appropriate; and

(12) Develop guidelines for acceptable restrictions for collection, use and disclosure of PII.

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

(1) Perform all privacy duties and responsibilities as designated by the ADAS, Office of Privacy and Records Management;

(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 privacy policy for VA in conjunction with policy efforts by all VA Administrations and Staff Offices;

(4) Provide technical guidance to Under Secretaries, Assistant Secretaries, and Other Key Officials regarding requirements for the protection of all PII;

(5) Provide basic privacy training, resources, guidance, and assistance to all field and Staff Office Privacy Officers;

(6) Provide Department-wide requirements for the development and implementation of periodic role-based privacy training;

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

(8) Provide development guidance and assist in the identification, implementation, and maintenance of VA privacy policies and procedures in coordination with Administration-level Privacy Officers, and the Office of the General Counsel (OGC);

(9) Oversee, direct, deliver, or ensure delivery of privacy training and initial orientation to employees, volunteers, medical staff, professional staff, contractors, Business Associates, and other appropriate third parties;

(10) Provide guidance to Privacy Officers in order to ensure that policies and practices adhere to those set forth by law and VA and Administration policies and procedures;

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

(12) Provide a means for Under Secretaries, Assistant Secretaries, and Other Key Officials to report how PII for which they are responsible is maintained;

(13) Provide all required privacy-related reporting, including recommendations to the ADAS, Office of Privacy and Records Management, and the CIO, as required by applicable law;

(14) Establish VA policy on the tracking and auditing of privacy breaches and complaints at VA by:

(a) Assigning, implementing, and managing a Department-wide system to track privacy complaints and reports of alleged, suspected, or actual breaches involving PII, or alleged violations of applicable privacy laws and policies;

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

(c) Reporting to oversight agencies and VA management on privacy violation complaint resolution measures taken within VA as required; and

(d) Providing oversight and guidance, and ensuring VA compliance with applicable Federal law relating to privacy complaints, or actual or suspected breaches involving PII throughout VA;

(15) Establish Department-wide requirements and guidance on the development and completion of Privacy Impact Assessments (PIA) by:

(a) Sustaining a PIA template for use when performing PIAs on VA information systems in accordance with OMB guidance; and

(b) Providing oversight and monitoring compliance with the legal and policy requirements of each PIA for each system; and

(16) Develop and promulgate privacy-related duties and responsibilities of all Privacy Officers.

f. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials shall:

(1) Provide adequate resources to Facilities and Staff Offices to establish Privacy Officer positions that will allow those Privacy Officers to perform their official duties;

(2) Provide at least one staff member to act as alternate Privacy Officer in the event that the Privacy Officer is absent or the Privacy Officer position is temporarily vacant;

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

(4) Ensure that all Facility-level Privacy Officers are provided the time and resources to work with the facility ISO and CIO to ensure that PIAs are complete and accurate;

(5) Develop and implement plans to eliminate the collection and use of Social Security Numbers (SSN) 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;

(6) Conduct a privacy review for all PII for which they are responsible, and report how such data is maintained to the Director, VA Privacy Service;

(7) Submit to the ADAS, Privacy and Records Management, quarterly reports on progress toward meeting Administrations' or Staff Offices' goals for the establishment of full-time Privacy Officers;

(8) Work with other Under Secretaries, Assistant Secretaries, and Other Key Officials to explore the creation of VA unique identifiers for Veterans and employees for use as an alternative to the SSN when there is not a compelling need, or use of the SSN is not required by law or mandated by the mission of the Department as set forth by the Secretary; and

(9) Ensure that all Privacy Officers are aware of their appropriate reporting structures within the privacy hierarchy for their organizations or facilities.

g. **Assistant Secretary for Human Resources and Administration (ASHRA).**

ASHRA shall work with the Office of General Counsel (OGC) and Under Secretaries to ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all Individuals in the Facility.

h. **Administration Privacy Officers.** Privacy Officers shall:

(1) Develop and implement Administration policies that promulgate this policy;

(2) Provide input to the Director, Privacy Service for the development of privacy policies and initiatives and, once these policies are implemented, provide feedback on their effectiveness;

(3) Implement the VA Privacy Program within their respective areas;

(4) Understand and apply Federal law, regulations, guidance, and VA Policy related to privacy;

(5) Serve as advisors on all aspects of privacy to their Administrations or program areas;

(6) Monitor and assist in the administration of VA privacy training and/or awareness programs within their realms of responsibility;

(7) Identify and report on Privacy Act Systems of Records (SOR), as appropriate;

(8) Assist with submission of PIAs, as appropriate;

(9) Coordinate with all system owner/managers to ensure that they understand the Privacy Act requirements and their related responsibilities throughout the system lifecycle;

(10) Collaborate with Records Management Officers and Information Security Officers (ISO) to ensure proper disposal of files and records;

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

(12) Determine the need for field-based Privacy Officers within their Administrations and provide instruction regarding responsibilities and requirements for implementation of the VA Privacy Program within field-based Facilities;

(13) Respond appropriately to any privacy complaints under their realms of responsibility;

(14) Identify SORs that are found within their realms of responsibility and work with the appropriate parties to ensure that System of Record Notices (SORNs) are published for all SORs identified within these areas and to update SORNs when appropriate;

(15) Enter all actual or suspected privacy events into the designated data breach reporting system within one hour of discovery;

(16) Provide at least quarterly to the Director, VA Privacy Service, a current list of all persons who have been designated as Privacy Officers within their Administration;

(17) 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 those set forth by law and VA and Administration policies and procedures; and

(18) Coordinate with appropriate ISOs and System Managers to ensure that all data and associated risks are identified and documented in all PIA submissions, as appropriate, and work with appropriate ISOs, System Managers, and the VA Privacy Service to ensure that the PIA(s) for each system within their area of responsibility is of a quality that will reasonably ensure its approval by the VA Privacy Service.

i. **Staff Office Privacy Officers.** VA Staff Office Privacy Officers shall:

(1) Develop and implement Staff Office policies that promulgate this policy;

(2) Provide input to Director, Privacy Service for the development of privacy policies and initiatives and, once these policies are implemented, provide feedback on their effectiveness;

(3) Provide input to the officials responsible for the development of privacy policies and initiatives related to the protection of PII within their program areas;

(4) Understand and apply Federal law, regulations, guidance, and VA Policy related to privacy;

(5) Understand and apply VA policy related to the activities of their respective offices;

(6) Deliver or ensure delivery of initial and annual privacy orientation and training to all employees, volunteers, medical and professional staff, contractors, Business Associates, and other third parties within their program areas, as appropriate;

(7) Serve as advisors on all aspects of privacy to their Staff Offices and/or program areas;

(8) Manage the VA privacy training and/or awareness programs within their realms of responsibility;

(9) Identify and report on SORs, as appropriate;

(10) Coordinate with all system owner/managers to ensure that they understand the Privacy Act requirements and their related responsibilities throughout the system lifecycle;

(11) Serve as the primary privacy contact within their respective program areas;

(12) Coordinate with HR, their ISOs, OGC and Staff Office 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;

(13) Collaborate with the Records Management Officers and the ISOs to ensure proper disposal of records;

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

(15) Determine the need for field-based Privacy Officers within their program areas and provide instruction regarding responsibilities and requirements for implementation of the VA Privacy Program within field-based Facilities;

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

(17) Respond appropriately to all privacy complaints;

(18) Enter all actual or suspected privacy events into the designated data breach reporting system within one hour of discovery, and if the event cannot be resolved, refer it to the next level of the privacy hierarchy within the Privacy Officer's organization, as soon as possible;

(19) Coordinate with appropriate ISOs and System Managers to ensure that all data and associated risks are identified and documented in all PIA submissions, and work with appropriate ISOs, System Managers, and the VA Privacy Service to ensure that the PIA(s) for

each system in their immediate areas of operation is of a quality that will reasonably ensure its approval by the VA Privacy Service;

(20) Work with Facility personnel involved with any aspect of release of PII to ensure full coordination and cooperation under the law, and VA policy and procedures;

(21) Provide guidance to Facility-level Privacy Officers within their Offices (if any), to help ensure compliance with all policy requirements; and

(22) Ensure that there is a mechanism within your office to adhering to all Business Associate Agreements (BAAs).

j. **Facility-level Privacy Officers.** Facility-level Privacy Officers shall:

(1) Coordinate and collaborate with their Administration-level or Staff Office Privacy Offices and Office of IT Oversight and Compliance (ITOC) assessment teams in order to ensure that policies and practices at their designated or assigned Facilities adhere to those set forth by law and VA and Administration policies and procedures;

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

(3) Acquire the necessary knowledge and expertise in information privacy, access, and release of information laws, policies and practices to develop effective and comprehensive Privacy Programs at their Facility;

(4) Implement the Administration or Staff Office privacy policies and procedures within the respective facilities to which they are designated or assigned;

(5) Provide input to respective facility or field-office leadership for the development of privacy policies and initiatives related to the protection of PII;

(6) Coordinate with the Facility CIOs to ensure that they understand the requirements of the Privacy Act and other applicable laws and regulations and their related responsibilities throughout the system lifecycle;

(7) Coordinate with Facility CIOs and ISOs to complete PIAs for all systems that operate or are under development at the facilities to which they are designated or assigned, as required by VA Handbook 6507;

(8) Deliver or ensure delivery of initial and annual privacy orientation and training to all Facility employees, volunteers, medical and professional staff, contractors, and other third parties, as appropriate;

(9) Serve as information privacy contact for their respective Facilities;

(10) Cooperate with the Office of the Inspector General (OIG); OGC; ITOC; Office of Human Resources (HR); Administration-level Offices, where applicable; and other legal and regulatory authorities in all compliance reviews or investigations;

(11) Coordinate with HR, 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 all Individuals in the Facilities to which they are designated or assigned;

(12) Maintain current knowledge of Federal privacy laws, regulations, guidance and VA policies to ensure organizational implementation and compliance, and maintain knowledge of accreditation standards in order to work with Facility management to ensure compliance therewith;

(13) Promote enterprise or Administration-sponsored activities designed to foster information privacy awareness within the Facilities to which they are designated or assigned;

(14) Respond to privacy events by following the formal process established for receiving, documenting, tracking, investigating, and taking action on these events, and if the event cannot be resolved, refer it to the next level of the privacy hierarchy within the Privacy Officers' facilities, as soon as possible;

(15) Enter all actual or suspected privacy events into the designated VA data breach reporting system within one hour of discovery;

(16) Complete appropriate notification/credit monitoring letters, as appropriate, and ensure that Facility Directors sign the letters;

(17) Conduct, at least quarterly, a walk-through of all areas of the facility to ensure that privacy-related policies are being followed and to provide guidance, as needed, to employees on proper procedures for the handling of PII;

(18) Work with Facility personnel involved with any aspect of release of PII to ensure full coordination and cooperation under the law, and VA policy and procedures; and

(19) Coordinate with local ISOs and System Managers to ensure that all data and associated risks are identified and documented in all PIA submissions, and work with their ISOs, System Managers, and the VA Privacy Service to ensure that the PIA(s) for each system in their immediate areas of operation is of a quality that will reasonably ensure its approval by the VA Privacy Service, as appropriate.

4. REFERENCES.

The VA Privacy Program has its foundation in Federal statutes, Executive Orders, Office of Management and Budget directives, and VA guidance including, but not limited to the authorities described below.

a. E-Government Act of 2002, Pub. L. 107-347, Section 208.

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

c. Employee Suitability Determinations and Investigations, 5 C.F.R. Parts 731, 732, and 736.

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

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

f. Freedom of Information Act (FOIA), 5 U.S.C. 552, 38 C.F.R. §§ 1.550-557.

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

h. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 C.F.R. Parts 160 and 164.

i. National Institute for Standards and Technology Special Publication 800-61, Computer Security Incident Handling Guide, December 1998.

j. National Institute for Standards and Technology Special Publication 800-88, Guidelines for Media Sanitization, September 2006.

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

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

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

n. Privacy Act of 1974, 5 U.S.C. 552a, 38 CFR §§ 1.575 – 1.584.

o. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56, Title II.

p. Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. 109-461, Section 902.

q. VA Directive 6066, Protected Health Information (PHI).

r. VA Directive 6221, Accessible Electronic Information Technology (EIT).

s. VA Directive 6361, Ensuring Quality of Information Disseminated by VA.

t. VA Directive 6371, Destruction of Temporary Paper Records.

u. VA Directive 6500, Information Security Program.

v. VA Directive 6502, VA Enterprise Privacy Program.

w. VA Directive 6507, Reducing the Use of Social Security Numbers.

x. VA Directive 6508, Privacy Impact Assessments.

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

z. VA Directive 6609, Mailing of Personally-Identifiable and Sensitive Information.

aa. VA Handbook 6300.5/1, Procedures for Establishing and Managing Privacy Act Systems of Records.

bb. VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Addresses.

cc. VA Handbook 6300.7/1, Procedures for Computer Matching Programs.

dd. VA Handbook 6301, Procedures for Handling Electronic Mail Records.

ee. VA Handbook 6310.2, Collections of Information Procedures.

ff. VA Handbook 6361, Ensuring Quality of Information Disseminated by VA.

gg. VA Handbook 6500, Information Security Program.

hh. VA Handbook 6500.2, Management of Security and Privacy Incidents.

ii. VA Handbook 6502.1, Privacy Violation Tracking System (PVTS).

jj. VA Handbook 6502.3, Web Page Privacy Policy.

kk. 38 U.S.C. 5701, Confidential Nature of Claims, 38 C.F.R. 1.500-527.

ll. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records, 37 C.F.R. 17.500-511.

mm. 38 U.S.C. 5721-5727, Information Security, 38 C.F.R. 75.111-118.

nn. 38 U.S.C. 7332, Confidentiality of Certain Medical Records, 38 C.F.R. 1.460- 496.

5. DEFINITIONS

a. **Business Associate:** For the purposes of this Directive, a Business Associate is defined as an entity, including any person, company, or organization that, on behalf of VHA, performs or assists in the performance of functions or activities involving the use or disclosure of PHI, or that provides certain services involving the disclosure of PHI by VHA.

b. **Designated Privacy Officer:** For purposes of this Directive, a Designated Privacy Officer is a 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 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, SSN, 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. PII is also known as Sensitive Personal Information (SPI).

d. **Privacy Event.** A Privacy Event is a confirmed instance in which information protected by HIPAA; the Privacy Act of 1974; or other confidentiality statutes such as 38 U.S.C. 5701, 5705, or 7332 may have been improperly disclosed, 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 confidentially or integrity of the data regardless of the manner in which the breach might have occurred.

e. **Privacy Hierarchy:** The organization of each Administration's or Staff Office's cadre of Privacy Officers according to increasing responsibilities and authority over privacy-related matters.

f. **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. For example, the Office of General Counsel, the Office of Human Resources and Administration, and the Office of Information and Technology are Staff Offices.

g. **VA Sensitive Information/ Data:** All Department data, on any storage media or in 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, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.