Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6502
Transmittal Sheet
May 5, 2008

VA ENTERPRISE PRIVACY PROGRAM

1. REASON FOR ISSUE: To update and reaffirm VA Directive 6502, the Department-wide program policy for the protection of privacy of veterans, their dependents and beneficiaries, as well as the privacy of all employees and contractors of the Department of Veterans Affairs (VA), and other individuals for whom personal records are created and maintained in accordance with Federal law. This directive clarifies policies, roles, and responsibilities for the VA Privacy Service, also known as the VA Enterprise Privacy Program, the program that oversees all VA-wide privacy programs.

VA applies leading privacy practices and adheres to data stewardship principles in managing data pertaining to all individuals on whom data is collected or maintained. These include the following:

a. Maintaining the confidentiality of Personally Identifiable Information (PII);

b. Limiting data access to PII to only individuals with a need for that information in order to perform their official duties; and

c. Minimizing the collection and maintenance of data to that necessary to perform the official functions of the Department.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive sets forth:

a. Policy for the Privacy Program. This policy requires VA-wide compliance with all applicable privacy laws, regulations, Executive Orders, and implementing policies, guidance, directives, and handbooks. This policy complies with Title 38 of the United States Code (U.S.C.) 5701, 5705, and 7332, and VA implementing regulations. Beyond Title 38, these policies are in accordance with Federal law, as embodied elsewhere in the U.S. Code, which bears directly on the privacy of personal data. The following list illustrates the various laws that contain privacy requirements and is not intended to be all-inclusive: Privacy Act, as amended (1974) (Pub. L. 93-579; Electronic Communications Privacy Act (1986) (Pub. L. 99-508); Health Insurance Portability and Accountability Act (HIPAA) (1996) (Pub. L. 104-191); USA PATRIOT Act (2001) (Pub. L. 107-56); and E-Government Act of 2002 (Pub. L.107-347). This policy applies to all future amendments and all new Federal privacy law to the extent possible;

b. Policies for the Privacy Program are also in compliance with related Federal regulations such as the Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), 45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule, 45 C.F.R. Parts 160 and 164, both published by the Department of

Health and Human Services (HHS). These policies also comply with Federal law related to the dissemination of Federal information, such as the Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Pub. L. 104-231;

c. Responsibilities for implementing and managing the Department-wide Privacy Program;

d. References related to the Privacy Program;

e. Major changes include the following:

(1) Change of directive title;

(2) Administrative updates;

(3) Guidance for the proper maintenance of personal information;

(4) Standards for access to, and disclosure of, records;

(5) Requirement for a Data Integrity Board;

(6) Requirement for the oversight of a privacy breach tracking tool;

(7) Change in title of the senior executive for privacy from ADAS, Office for Cyber and Information Security to ADAS, Office of Privacy and Records Management;

(8) Establishment of new duties for the ADAS, Office of Privacy and Records Management, the Director of the Privacy Service, and Under Secretaries, Assistant Secretaries, and Other Key Officials;

(9) Establishment of duties for VA employees, contractors, volunteers, interns, and business associates;

(10) Establishment of responsibilities for Privacy Officers;

(11) Provision of additional privacy program-related legislation and guidance; and

(12) Provision of definitions for terms added to this Directive.

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

4. RELATED HANDBOOKS: VA Handbook 6500, Information Security Program, VA Handbook 6502.1, Privacy Violation Tracking System (PVTS); VA Handbook 6502.2, Privacy Impact Assessments; VA Handbook 6502.3, Web Page Privacy Policy; and all

Handbooks to follow, including but not limited to the following topics: Maintenance of PII; Privacy Officer Roles and Duties; Privacy Reviews; Privacy Training; Processing of Privacy Act requests; Release of Information; Systems of Records; Procedures for Establishing Computer Matching Agreements; Information Governance Board; Privacy Act Officer Roles and Duties

5. RESCISSION: VA Directive 6502, Privacy Program, dated June 30, 2003.

CERTIFIED BY:

/S/

Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/S/

Robert T. Howard
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

VA ENTERPRISE PRIVACY PROGRAM

1. PURPOSE

a. This directive establishes the policies and responsibilities for the Department of Veterans Affairs (VA) Privacy Service, also known as the VA Enterprise Privacy Program, and establishes the VA Privacy Program.

b. The VA Privacy Program shall apply to all personal data (hereinafter referred to as “Personally Identifiable Information (PII)” that is collected, created, transmitted, used, processed, stored, or in the process of disposition (all hereinafter referred to as “maintained”, unless otherwise indicated) by, or for, VA regardless of the medium in which it is maintained.

Note: For purposes of this Privacy Service Directive, the term PII is interchangeable with the term “Sensitive Personal Information” (SPI), as defined in 38 U.S.C. § 5727 (19) and VA Handbook 6500. Nevertheless, PII and SPI are defined separately in the Definitions Section because SPI is a term unique to VA by statute while PII is the term used elsewhere in the Federal government and in the private privacy industry.

c. The mission of VA is to serve America's veterans and their families. In order to fulfill this mission, it is necessary for VA to collect and maintain PII about veterans, their dependents and their beneficiaries. In the exercise of its mission, VA is required to collect and maintain such data for others, such as VA employees, contractors, and volunteers. The mission of the VA Privacy Service, through the implementation of the Privacy Program, is to preserve and protect the privacy of PII gathered or created by VA in the course of performing official duties. The manner of this protection shall comply with requirements of all Federal statutes and regulations, Executive Orders, and Government and VA-wide policies, procedures, and guidance.

d. VA applies leading privacy practices and adheres to data stewardship principles in managing data pertaining to all individuals on whom PII is collected and maintained. These include the following:

(1) Maintaining the confidentiality of Personally Identifiable Information (PII);

(2) Ensuring appropriate levels of security for PII by limiting data access to individuals with a need for that information in order to perform official duties; and

(3) Minimizing the collection and maintenance of data to that which is necessary to perform the official functions of the Department.

e. The provisions of this directive apply to all VA components and pertain to all PII, maintained in any medium, including, but not limited to, hard copy, microform, and electronic format, and by information systems administered by, or otherwise under the authority or control of VA.

f. Terms not specifically defined within this Directive reflect their reasonable meaning within the context of the preservation and protection of PII.

2. POLICY

It is VA policy that:

a. **Privacy is a fundamental right.** The privacy of PII is a personal and fundamental right that shall be respected and protected in all VA functions, services, and facilities.

b. **A Privacy Program will be sustained.** VA shall implement a Department-wide Privacy Program through the conduct of a Privacy Service under the Assistant Secretary for Information and Technology.

c. **PII will be kept confidential.** In accordance with 5 U.S.C. 552a, 38 U.S.C. §§ 5701, 5705, and 7332, and other applicable Federal privacy laws and regulations, as appropriate, VA shall ensure that all PII that is maintained by, or for, VA in any medium, is kept confidential, except when disclosure is permitted or compelled under law.

d. **PII will be properly controlled.** All PII in the custody and control of VA shall be used and disclosed only as permitted or required by law.

e. **Contractor-controlled PII will be properly maintained.** VA shall ensure that all contracts in which any data containing VA-owned PII that is maintained by contractors will contain the appropriate clauses as may be required by Federal Acquisition Regulations and other Federal authorities in order to ensure that the VA data under the control of the contractor is maintained in accordance with Federal law and VA policy.

f. **Data will be protected.** The physical input and output products of VA information systems that contain privacy-protected data, such as disks, paper, flash drives or any other data storage device, shall be protected against misuse and unauthorized access, unauthorized disruption, unauthorized disclosure, or unauthorized modification or destruction. No technology utilized to collect, use, or disclose PII shall erode privacy protections afforded by Federal law or VA policy.

g. **PII will be kept secure.** Security plans shall be continually developed and security controls implemented on all networks and filing systems that maintain PII in any form. These controls shall be implemented, as required by law or policy, to protect the security and privacy of all operating or filing systems, application software, and data in VA information systems from accidental or malicious disclosure, alteration or destruction, and to provide assurances to the user of the quality, integrity, and confidentiality of PII maintained by VA. Technologies used to maintain PII will allow for continuous auditing of compliance with VA policy.

h. **Privacy and data breaches shall be reported.** VA personnel, contractors, and authorized users shall report all privacy complaints or actual or suspected breaches involving PII in a timely and complete manner, as required by applicable law, and VA regulations and policy to agents designated by the Privacy Service. VA shall resolve all such breaches with privacy implications in a timely fashion in accordance with applicable law and policy. For further guidance see VA Handbook 6502.1, Privacy Violation Tracking System (PVTS).

i. **A data breach service shall be sustained.** VA shall maintain a service for the tracking and reporting of suspected or actual breaches involving PII to the VA Security Operations Center (SOC), US-CERT, the VA Privacy Service, the appropriate Privacy Officer and any other pertinent entity. For further guidance see VA Handbook 6502.1, Privacy Violation Tracking System (PVTS) and the Formal Event Reporting and Evaluation Tool (FERET) guidebook.

j. **Privacy awareness training shall be provided.** VA shall provide annual privacy awareness to all levels of VA staff, contractors, volunteers, interns, and trainees, and provide role-based privacy training on an as-needed basis. Business Associates shall provide annual privacy awareness training to all levels of staff, all contractors, volunteers, interns and any other entity that will handle VA data.

k. **Privacy Reviews shall be conducted.** VA shall conduct privacy reviews as required by law, OMB guidance, and VA policy.

l. **Privacy Impact Assessments (PIA) shall be performed.** VA shall perform PIAs in compliance with Section 208 of the E-Government Act of 2002 (Pub. L. 107-347), and applicable Office of Management and Budget (OMB) guidance. See VA Handbook 6502.2, Privacy Impact Assessment, for further guidance.

m. **An Information Governance Board shall be sustained.** VA shall establish a multidisciplinary information governance body entrusted with establishing VA-wide data classification and data management strategies.

n. **PII will be properly maintained.** Personally Identifiable Information shall be maintained in a manner that will ensure:

(1) The PII is relevant and necessary to carry out a purpose prescribed by the Secretary or required by law, regulation or Executive Order;

(2) To the greatest extent practicable, the PII is collected directly from the individual to whom it pertains;

(3) When it is not possible to collect PII directly from the individual and that information is collected from third parties, it will be verified with the subject of the record to the greatest extent practicable before any negative action is taken;

(4) The individual from whom PII is obtained is informed why the information is being collected, the authority for the collection, whether or not providing the information is mandatory or voluntary, and the consequences of not providing the information requested;

(5) No record that describes how individuals exercise their rights guaranteed by the First Amendment of the U.S. Constitution will be kept, unless expressly authorized by statute or by the individual to whom the records pertain or is pertinent to and within the scope of an authorized law enforcement activity;

(6) The PII collected shall be timely, accurate, relevant, and complete for its intended use to the extent possible;

(7) Administrative, technical, and physical safeguards are in place to ensure the security of records containing PII. These safeguards must be appropriate to prevent the compromise or misuse of PII while being maintained by VA in any medium; and

(8) All PII will be disposed of at the end of the retention period as required by law or regulation.

o. **Records containing PII shall be disclosed only under limited circumstances**. Disclosure of records from a Privacy Act system of records pertaining to an individual shall be prohibited except with the consent/authorization of the individual to whom the records pertain or as authorized by the Act and other laws pertaining to the information. When disclosures are made, the individual shall be permitted to the extent authorized under the Privacy Act or other law pertaining to disclosure of the information, to receive an accounting of these disclosures from VA. PII contained in a Privacy Act system of records shall be handled in full compliance with fair information practices as defined in the Privacy Act.

Note: Information that is not maintained in a Privacy Act System of Records may still be considered PII, and may be prohibited from disclosure by law, regulation, or VA policy.

p. **Computer Matching Agreements shall comply with the law.** Computer matching programs between VA and Federal, state, or local governmental agencies shall be conducted in accordance with law and VA policy.

q. **A Data Integrity Board shall be sustained.** VA shall sustain a Data Integrity Board, consisting of senior officials and shall include ADAS, Office of Privacy and Records Management and the Inspector General or their designees. This Board will oversee and coordinate VA efforts to comply with the provisions of the Privacy Act and all other applicable law, and will oversee and approve all VA computer matching activities in accordance with the requirements of the Privacy Act; the Computer Matching and Privacy Protection Act of 1988; and the Office of Management and Budget (OMB) guidance.

r. **VA shall comply with current laws and regulations.** VA shall evaluate legislative and regulatory proposals involving the collection use, and disclosure of PII, and shall continually assess compliance with all applicable Federal privacy laws and regulations. All VA entities that maintain PII shall:

(1) Identify the PII for which they are responsible;

(2) Comply with all extant and future Federal privacy law, regulations, and guidance pertaining to that PII;

(3) Submit a Privacy Review to the Privacy Service documenting the procedures used to comply with Federal privacy law and regulations; and

(4) Submit annual privacy risk assessments as required by law or policy and conduct related ongoing compliance monitoring activities in coordination with other compliance and operational assessment functions.

s. **VA shall not impede the Inspector General's duties.** Nothing in this directive shall prevent or impede the VA Inspector General from performing duties pursuant to the Inspector General Act or other statutory authority.

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) who is the senior agency official responsible for the VA Information Security and Privacy Programs.

b. **The Assistant Secretary for Information and Technology (ASIT).** The ASIT, as the VA CIO, shall:

(1) Establish Department-wide requirements, and provide oversight and guidance related to the protection of PII throughout VA;

(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 privacy and records management law, policies, and standards;

(3) Approve the Director of the Privacy Service and the Director of Records Management, as the Secretary's designated senior agency official for the VA Privacy Program;

(4) Ensure that there are adequate staff and funding resources to properly fulfill all privacy-protection functions;

(5) Sustain a privacy training, education, and awareness program for all VA personnel and other authorized individuals involved in either the maintenance and management of PII, or the management, use, or operation of VA information systems containing PII;

(6) Develop and issue VA privacy directives, handbooks, and other Department-wide privacy publications, as appropriate; and

(7) Submit, as required by applicable law, all VA reviews of PII.

c. **The DAS, Office of Information Protection and Risk Management.** The DAS shall:

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

(2) Perform all privacy duties and responsibilities as designated by the Assistant Secretary of Information and Technology;

(3) Recommend for selection an Associate Deputy Assistant Secretary (ADAS), Office of Privacy and Records Management, as the principal Department official responsible for the VA Privacy Program;

(4) Set the direction and strategy for the development and implementation of privacy policy, standards, guidelines, and procedures to ensure ongoing maintenance of privacy in accordance with federal law and policy;

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

(6) Maintain relationships with VA Office of the Inspector General and VA Police and other governmental agencies when dealing with privacy issues;

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

(8) Set requirements for privacy education and awareness; and

(9) Ensure VA-wide implementation of Federal Information Security Management Act (FISMA) and OMB Circular A-130 compliance, related to confidentiality, for all VA applications and general support systems.

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 the Department of Veterans Affairs;

(3) Have overall responsibility for oversight of a 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) Advise the DAS, Office of Information Protection and Risk Management, VA Assistant Secretary of Information and Technology, Under Secretaries, Assistant Secretaries, and other key officials on privacy policy compliance; effective privacy practices and safeguards over VA information systems; and other matters relevant to protecting all PII, and all information systems containing PII;

(6) Recommend for selection a Director of the Privacy Service.

(7) Facilitate cooperation among all VA Administrations, staff offices, and other key officials regarding VA's Privacy Program;

(8) Develop program spending plans that consider the risk to the integrity and confidentiality of all PII, regardless of the medium on which it is found;

(9) Issue technical guidance and direction to the Deputy CIOs and Administration and Staff Office Privacy Officers regarding all aspects of implementing the VA privacy program;

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

(11) Coordinate with key officials to ensure proper maintenance of all data containing PII; and ensure that the data stewardship principles are followed;

(12) Coordinate with key officials to develop VA-wide, network-wide privacy policies and procedures in accordance with Federal law and regulations, and VA policy;

(13) Coordinate with Under Secretaries, Assistant Secretaries, and other key officials to establish a multidisciplinary information governance board to create VA-wide data classification and data management strategies;

(14) Coordinate with the senior official responsible for incident response and the senior official responsible for data security to ensure that incident response policies and procedures are in accordance with applicable Federal privacy laws and VA Directives;

(15) Coordinate with key officials to ensure that all contracts that allow PII to be accessed by, transferred to and maintained by third parties contain FAR clause 52.224.1;

(16) Devise privacy risk assessment policies and procedures and conduct ongoing compliance monitoring activities in coordination with other compliance and operational assessment functions within VA;

(17) Develop multiyear plans to improve privacy controls as part of VA cyber and information security;

(18) Collaborate with the ADAS, Office of Cyber Security to develop standards that ensure security controls provide proper protection of all PII at VA;

(19) Administer the process for receiving, documenting, tracking, investigating, and taking 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;

(20) Continually update policies regarding the maintenance of PII as legal requirements and other circumstances may dictate;

(21) 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;

(22) Issue guidance concerning the conduct and use of Privacy Reviews, and the contents of reports generated as a result of the Privacy Reviews;

(23) 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, business associates, alliances, and other third parties, as appropriate;

(24) Establish, along with management and operations, a mechanism to track access to PII, as required by law; and

(25) Develop access, audit, and reporting procedures to allow qualified individuals to receive access and to review information pertinent to their assigned duties or responsibilities at VA.

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) Develop, review, coordinate and monitor privacy policy for VA in conjunction with policy efforts by all VA Administrations and staff offices;

(3) Provide technical guidance to Under Secretaries, Assistant Secretaries, and other key officials regarding requirements for the protection of all PII;

(4) Coordinate with the VA Office of Oversight and Compliance to devise measures and methodologies to be utilized when auditing VA facilities for privacy compliance;

(5) Coordinate with the Director of Records Management, as needed, on matters concerning the Privacy Act;

(6) Establish Department-wide requirements, and monitor compliance with all Federal privacy law, regulations, guidance, and VA policy;

(7) Collaborate with entities responsible for the development of Department-wide requirements for the responsibilities of Privacy Officers and provide implementation guidance, as needed;

(8) Collaborate with pertinent parties in the development and implementation of Department-wide requirements and guidance regarding VA Rules of Behavior concerning the handling of PII;

(9) Develop and provide annual Department-wide general privacy awareness training and monitor compliance with this requirement;

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

(11) Publish an annual list of all employees who are designated as Privacy Officers;

(12) Require a Privacy Review, which is a review by Under Secretaries, Assistant Secretaries, other key officials, and information owners of all PII for which they are responsible, and how such data is maintained;

(13) Review, monitor, and maintain the Privacy Reviews which shall be used to determine compliance with applicable law in conjunction with the VA Office of Oversight and Compliance and the Office of General Counsel;

(14) Analyze the existing safeguards to ensure the confidentiality of all PII and provide recommendations for policy modifications, procedures and processes targeted at the protection of PII;

(15) 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;

(16) Examine new or pending legislation, in conjunction with the Office of General Counsel, to determine the actual or potential impact of such legislation on privacy policy and/or practice at VA;

(17) Establish VA policy on the tracking and auditing of VA privacy breaches and complaints 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;

(18) Establishing 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 Office of Management and Budget (OMB) guidance; and

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

(19) Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy breaches, implementation of the Privacy Act, internal controls, and other relevant matters; and

(20) Developing and promulgating privacy-related duties and responsibilities of all full-time Privacy Officers.

f. **The Director of Records Management**. The Director shall:

(1) Provide advice, assistance, and recommendations to the ADAS, Office of Privacy and Records Management regarding policies, procedures, and other requirements governing the Freedom of Information Act (FOIA), the Privacy Act, 38 U.S.C. 5701, 5702, 5705 and 7332, and their implementation;

(2) Coordinate with the Director of the Privacy Service, as needed, on matters concerning the Privacy Act; and

(3) Collaborate with the Director of the Privacy Service on improving VA safeguards for PII.

g. **ADAS, Office of Risk Management and Incident Response and the ADAS, Office of Cyber Security.** These offices are responsible for:

(1) Coordinating with the ADAS, Office of Privacy and Records Management when developing policies and methodologies regarding the response to data breaches; and

(2) Coordinating actions on privacy incidents, data breaches, and privacy violations.

h. **The Inspector General**. The Office of the Inspector General is responsible for:

(1) Conducting and supervising Privacy Program audits and providing follow-up regarding Privacy Program audit findings as deemed necessary by the Inspector General (IG); and

(2) Conducting or providing oversight for investigations concerning PII.

i. **The General Counsel**. This Office is responsible for:

(1) Interpreting laws, regulations, and directives applicable to VA privacy issues; and

(2) Rendering legal opinions on the compliance of each Administration or staff office policies with the Federal privacy law and regulations applicable to that Administration or office by:

(a) Providing reviews of each Privacy Review for compliance with applicable law; and

(b) Rendering legal advice and services regarding privacy issues to Under Secretaries, Assistant Secretaries, and Other Key Officials.

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

(1) Under Secretaries, Assistant Secretaries, and other key officials shall:

(a) Ensure that Department-wide privacy policies and procedures are implemented;

(b) Establish procedures and rules of conduct necessary to implement this Directive so as to ensure compliance with all federal privacy mandates;

(c) Appoint Privacy Officers in the following manner:

1. Under Secretaries shall appoint full-time, dedicated administration-level Privacy Officers; and

2. Assistant Secretaries and Other Key Officials shall appoint full-time Privacy Officers based upon organizational needs and legal requirements;

(d) Develop policies necessary to implement this Directive and prescribe the responsibilities and duties of the full-time Privacy Officers within their respective VA facilities;

(e) Safeguard and secure all PII maintained in VA information systems for which they are responsible, as well as those systems shared with, or operated by, other Federal agencies, contractors, or other outside organizations in coordination with the VA Privacy Service, and in accordance with Federal data security guidance;

(f) Work in close association with the Privacy Service to:

1. Develop, implement, sustain, and enforce a structured program to adequately secure all PII, and the systems and resources for which they are responsible; and

2. Propose such regulations, issue such policy or guidance, and enter into such agreements as necessary to implement this directive.

(g) Assign to program offices the requirement to develop and submit to the Privacy Service a Privacy Review of all PII for which they are responsible under applicable Federal law, and describe how program offices maintain PII;

(h) Ensure that all VA employees, volunteers, medical and professional staff, contractors, business associates, alliances, and other appropriate third parties under their respective jurisdictions act in compliance with the Department's privacy policies;

(i) Seek technical guidance and requirements for the protection of all PII from the Director, Privacy Service, for the development and approval of systems planning, design, acquisition, budgeting, and funding;

(j) Ensure that Privacy Officers report, in a timely manner, all actual or suspected breaches involving PII to a tracking service designated by the Privacy Service for audit purposes;

(k) Allocate sufficient funds, personnel, and management support to implement the provisions of this directive, and ensure compliance with Federal and VA privacy program requirements;

(l) Ensure that personnel within their respective organizations attend privacy orientation and training before they are granted access to any VA system of records, in accordance with applicable legal requirements and guidance, Office of Personnel Management regulations, and VA privacy policy; and that they complete privacy awareness and security training periodically thereafter;

(m) Ensure that all privacy-related reporting or notice requirements are met (e.g., privacy training numbers, privacy complaints, and System of Records information);

(n) Ensure that all alleged breaches of applicable Federal privacy law that, on their face, appear to constitute a criminal violation of law, are referred for investigation to the Office of the Inspector General;

(o) Ensure that non-compliance with these policies by VA personnel and other authorized individuals are addressed and remedied promptly including, if necessary, the initiation of penalties for non-compliance in accordance with applicable Federal law and VA personnel rules and regulations;

(p) Perform program reviews to assess the adequacy of privacy safeguards and identify weaknesses that would jeopardize the privacy and confidentiality of all PII of VA personnel, veterans, their dependents, or their beneficiaries; and all others on whom VA collects or maintains PII;

(q) Identify and report on all Privacy Act Systems of Records under his or her control or authority to the ADAS, Office of Privacy and Records Management;

(r) Ensure proper disposal of all files and records under his or her authority or control;

(s) Ensure that privacy considerations are addressed in all phases of the Systems Development Lifecycle;

(t) Comply with all Departmental policies, procedures, and guidance concerning privacy;

(u) Work with the ADAS, Office of Cyber Security, and the ADAS, Office of Privacy and Records Management, as needed, to determine and verify the security requirements and appropriate level of security controls for the information system or systems, under his or her authority or control, where PII is currently maintained;

(v) Determine who has access to systems containing PII, including types of privileges and access rights; and

(w) Provide a plan of action and milestones to the Assistant Secretary for Information and Technology, on at least a quarterly basis, detailing the status of actions being taken to correct any security compliance failure or policy violation that resulted in a breach of PII.

(2) Assistant Secretaries and other key officials shall:

(a) Review the status of all Privacy Officers in their organizations and assess the adequacy of currently staffing levels at major 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 major facility throughout VA; and

(b) Ensure a Privacy Officer is assigned within their respective areas based upon organizational needs and legal requirements.

k. **Administration and Staff Office Privacy Officers.** Privacy Officers shall:

(1) Develop and implement staff office polices 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) Implement the VA Privacy Program within their respective areas;

(4) Understand and apply Federal law, Regulations, and VA Directives related to privacy;

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

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

(7) Identify Privacy Act Systems of Records;

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

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

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

(11) 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;

(12) Respond to all privacy complaints; and

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

l. **System Owners.** System owners, as program managers for VA information systems, shall:

(1) Assure that all proper measures are taken to ensure confidentiality of PII on all systems for which they are responsible;

(2) Conduct PIAs on systems for which they are responsible, as necessary; and

(3) Work with information owners and Director of Records Management to publish initial System of Records Notices, and update all System of Records Notices as dictated by law or VA policy.

m. **Information Owners.** Information owners, as the owners of the information maintained on VA data systems, shall:

(1) Collaborate with the System Owners to ensure that data is being used according to uses set forth in the System of Records Notice; and

(2) Ensure that all PIAs for systems maintaining their data are complete and accurate.

n. **VA Employees, Contractors, Volunteers, and Business Associates:** As users of VA systems with potential access to veteran, employee, contractor, volunteer, intern, and business associate records, all VA employees, contractors, volunteers, interns, and business associates shall:

(1) Access records containing PII only when the information is needed to carry out their official duties;

(2) Disclose PII about veterans, employees or contractors volunteers, interns, and business associates only in accordance with applicable Federal privacy laws, regulations, and VA policies and procedures;

(3) Take privacy awareness training provided or approved by the Privacy Service on an annual basis;

(4) Take any role-specific privacy training provided or approved by the VA Privacy Service that is applicable to their official duties; and

(5) Report all actual or suspected breaches involving PII to their Privacy Officers within one hour of discovery.

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. Electronic Communications Privacy Act of 1986, as amended, Pub. L. 99-508, 100 Stat. 1848, 99th Cong. (October 21, 1986), codified at 18 U.S.C. 2510 et seq.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

p. 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.

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

s. VA Directive and Handbook 0710, Personnel Suitability and Security Program, September 10, 2004.

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

u. VA Directive 6102, Internet/Intranet Services, January 30, 2006.

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

w. VA Directive and Handbook 6210, Automated Information Systems Security, August 4, 2006.

x. VA Directive 6212, Security of External Electronic Connections, January 21, 2000.

y. VA Directive 6214, VA Information Technology Security Certification and Accreditation Program, March 15, 2002.

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

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

bb. VA Directive 6500, Information Security Program, August 4, 2006.

cc. VA Directive 6600, Protecting Personally Identifiable Information (PII), February 26, 2007.

dd. VA Handbook 6300.5; 6300.5/1, Procedures for Establishing and Managing Privacy Act Systems of Records, October 5, 2000.

ee. VA Handbook 6300.6; 6300.6/1, Procedures for Releasing Lists of Veterans' and Dependents' Addresses, January 12, 1998.

ff. VA Handbook 6300.7; 6300.7/1, Procedures for Computer Matching Programs, January 12, 1998.

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

hh. VA Handbook 6310.2, Collections of Information Procedures, December 1, 2001.

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

jj. VA Handbook 6500, Information Security Program, September 18, 2007.

kk. VA Handbook 6502.1, Privacy Violation Tracking System (PVTS), March 24, 2004.

ll. VA Handbook 6502.2, Privacy Impact Assessment, October 21, 2004.

mm. VA Handbook 6502.3, Web Page Privacy Policy, April 17, 2006.

nn. VA IT Directive 06-2, Safeguarding Confidential and Privacy Act Protected Data at Alternative Work Locations, June 6, 2006.

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

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

qq. VA IT Directive 06-6, Safeguarding Removable Media, September 29, 2006.

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

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

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

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

5. DEFINITIONS

a. **Data Breach.** The loss, theft, or any other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information in electronic, printed form, that results in the potential compromise of the confidentiality or integrity of the data.

b. **Data Steward.** An individual who manages and oversees the protection of PII. The Data Steward assures the protection of PII by acting as the conduit between information technology (IT) and operations in order to align the business needs with those of IT systems. This individual assures that the usability, accessibility, and quality of data is retained to the fullest allowable extent, while ensuring the confidentiality of PII.

c. **Individually Identifiable Health Information.** A subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That indentifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

d. **Information Owner.** An information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal. Information owner responsibilities extend to interconnected systems or groups of interconnected systems.

e. **Maintain.** To collect, create, use, process, store, disseminate, transmit, or dispose of PII.

f. **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.

g. Protected Health Information (PHI) For purposes of this Privacy Service Directive, PHI shall 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. PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium, and relates to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) past, present, or future payment for the provision of health care to an individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information.

h. **Plan of action and milestones**. A plan used as a basis for the quarterly reporting requirements of the Office of Management and Budget that includes the following information:

(1) A description of the security weakness;

(2) The identity of the office or organization responsible for resolving the weakness;

(3) An estimate of resources required to resolve the weakness by fiscal year;

(4) The scheduled completion date;

(5) Key milestones with estimated completion dates;

(6) Any changes to the original key milestone date;

(7) The source that identified the weakness; and

(8) The status of efforts to correct the weakness.

i. **Privacy Event.** An event with the potential to result in an actual or suspected Data Breach.

j. **Record.** Any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual.

k. **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.

l. **Sensitive Personal Information (SPI).** Defined in VA Handbook 6500 as any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (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 Personally Identifiable Information (PII).

m. **System of Records.** 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 Owner.** 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, and is also responsible for deciding who has access to the information system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

VA Fair Information Principles

1. The Principle of Openness. When VA collects personal data from an individual, VA will inform him or her of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the *Federal Register* and posted on the VA Systems of Records Notices Government Printing Office (GPO) Compilation website, available at: http://www.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf

2. The Principle of Individual Participation. Unless VA has claimed an exemption from the Privacy Act, everyone will be granted access to his or her records, upon request; to the extent permitted by law, and provided a list of disclosures made outside VA; and provided the opportunity to make corrections to his or her file if it is shown to be in error.

3. The Principle of Limited Collection. VA will collect only those personal data elements required to fulfill an official function or mission grounded in law. Those collections will be conducted by lawful and fair means.

4. The Principle of Limited Retention. VA will retain personal information only for as long as necessary to fulfill the purposes for which it is collected. Records will be destroyed in accordance with established VA records management principles.

5. The Principle of Data Quality. VA will make every effort to maintain only accurate, relevant, timely, and complete data about individuals.

6. The Principle of Limited Internal Use. VA will use personal data for lawful purposes only. Access to any personal data will be limited to those individuals within VA with an official need for the data.

7. The Principle of Disclosure. VA personnel will zealously guard all personal data to ensure that all disclosures are made with written permission or in strict accordance with privacy laws.

8. The Principle of Security. All personal data shall be protected by safeguards appropriate to ensure security and confidentiality. Electronic systems will be periodically reviewed for compliance with the security principles of the Privacy Act, the Computer Security Act, Heath Insurance Portability and Accountability Act (HIPAA), and related statutes. Electronic collection of information will only be conducted in a safe and secure manner.

9. The Principle of Accountability. VA, its employees, and contractors are subject to civil and criminal penalties for certain breaches of privacy. VA shall be diligent in sanctioning individuals who violate privacy rules.

10. The Principle of Challenging Compliance. An individual may challenge VA if he or she believes that VA has failed to comply with these principles, privacy laws, or the rules in a system of records notice. Challenges may be addressed to the VA Privacy Service in addition to any other remedy provided by any applicable authority.