Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6508
Transmittal Sheet
October 15, 2014

IMPLEMENTATION OF PRIVACY THRESHOLD ANALYSIS AND PRIVACY IMPACT ASSESSMENT

1. REASON FOR ISSUE: To establish a VA Enterprise-wide policy for incorporating and implementing the Privacy Threshold Analysis (PTA) into the current compliance process as recommended by the National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). This Directive also reinstitutes policy for the Privacy Impact Assessment (PIA), pursuant to the E-Government Act of 2002 (P.L.107-347).

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

a. Establishes a new policy for which information content maintained in VA information technology systems (IT), rulemakings, programs, and/or projects, are reviewed and assessed for privacy implications through the inclusion of the PTA;

b. Reinstitutes VA policy for privacy compliance through the use of the PIA. Pursuant to Section 208 of the E-Government Act of 2002, Office of Management and Budget (OMB) Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, and NIST Spec. Pub. 800-122, VA Administrations and staff offices are required to complete a PIA for all new and substantially changed (IT) systems, rulemakings, programs, and/or projects that have been determined by the adjudication of the PTA to collect, maintain, or disseminate PII and/or Personal Health Information (PHI); and

c. Expands on PIA requirements set forth in the Department of Veterans Affairs (VA) Directive 6502, Enterprise-Wide VA Privacy Program.

3. RESPONSIBLE OFFICE: Office of the Assistant Secretary for Information and Technology (005), Office of Information Security (005R), Office of Privacy and Records Management, Privacy Service (005R1A).

4. RELATED DIRECTIVE(S)/HANDBOOK(S): VA Directive 6502, Enterprise-Wide Privacy Program; VA Handbook 6508.1, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment; and the Privacy Threshold Analysis and the Privacy Impact Assessment Guide

RESCISSION(S): VA Directive 6508, Privacy Impact Assessments, dated October 3, 2008

CERTIFIED BY:

/s/
Stephen W. Warren
Executive in Charge
and Chief Information Officer
for Office of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Stephen W. Warren
Executive in Charge
and Chief Information Officer
for Office of Information and Technology

IMPLEMENTATION OF PRIVACY THRESHOLD ANALYSIS AND PRIVACY IMPACT ASSESSMENT

1. PURPOSE

a. This Directive establishes a VA enterprise-wide policy for incorporating use of the PTA as recommended by NIST and the PIA as required under privacy provisions of the E-Government Act of 2002; applicable Office of Management and Budget (OMB) guidance; and VA Directive 6502, Enterprise-Wide VA Privacy Program.

b. To establish a policy for privacy compliance and risk management for all IT systems, rulemakings, programs, and/or projects that collect and maintain PII and/or PHI.

c. To address public concerns regarding the protection of PII and/or PHI supported by the process of performing a PTA and PIA.

d. To incorporate use of the PIA as a requirement of the Authority and Accreditation (A&A) package. All PIAs will be evaluated by certifying officials when determining whether or not systems are granted authorizations to operate.

2. POLICY

Implementation of the PTA:

a. As prescribed in VA Directive 6502, Enterprise-wide Privacy Program, VA officials responsible for the initiation and implementation of rulemaking, IT systems, and/or projects are required to complete a PTA annually. If a PTA determination indicates no PIA is required, the PTA will be included in the A&A documentation as official record that no PIA is required. (A PIA is required for all systems that are subject to the A&A process; these provisions are codified in OMB Circular A-130, Appendix III)

b. A PTA will be conducted when any of the following are applicable:

(1) Develops or procures any new technologies or IT systems that collect, maintain, or disseminate PII and/PHI;

(a) Systems for which a PTA has not been officially verified by the Associate Deputy Assistant Secretary for Policy, Privacy, and Incident Response or their designee will not be considered certified, and cannot be accredited.

(b) Unaccredited systems will not be granted an Authorization to Operate (ATO).

(2) Initiates a new collection of PII and/or PHI on ten (10) or more persons is proposed.

(3) Revises existing systems. If the project, rulemaking, and/or IT system, are not covered under a current System of Records Notice (SORN), a new or updated SORN may be required.

(4) Issues a new or updated rulemaking that affects PII and/or PHI. If an agency rulemaking results in or is likely to result in a new collection or use of VA maintained PII and/or PHI

(5) All Project Management Accountability System (PMAS) programs or projects

(6) If a project, rulemaking, and/or IT system have statutory authority to collect or use PII/and or PHI.

(7) A PTA must be completed for every new electronic data collection or when a major change occurs to an existing IT system.

c. Annually, the System Owner is required to reassess and certify that no major changes have occurred by completing the PTA. Completed PTAs should be submitted to the VA Privacy Service annually according to their annual scheduled due date. In the event of a major change or an expired PIA, a new PIA will be required.

d. **There are two types of PTA's:**

(1) **Program Management Accountability System (PMAS) PTA Template**: This PTA is required as a part of the Milestone 0 and Milestone 1 reviews as indicated in VA Directive 6071, Project Management Accountability System (PMAS). The Integrated Project Team (IPT) Business Sponsor Privacy Officer is responsible for coordinating the completion of the document with the Business Sponsor and other relevant IPT members. VA Privacy Service does not review PMAS PTA's.

(2) **Standard PTA Template**: This template is required for efforts associated with the Federal Information Security Management Act (FISMA) and Authorization and Accreditation (A&A) processes or when it has been determined that you need to complete a PTA outside of the PMAS process.

(a) The System Owner is responsible for completing the Standard PTA and coordinating with other relevant stakeholders such as the Privacy Officer.

(b) VA Privacy Service is responsible for the review and determination of Standard PTA's and IPT Privacy Officers are responsible for the review and determination of PMAS PTA's.

e. **Implementation of the PIA:**

(1) The PIA determines whether an existing SORN should be revised or if a new SORN is required.

(2) VA Administrations and staff offices are required to complete a PIA for all new and substantially changed (IT) systems, rulemakings, programs, and/or projects that have been determined by the adjudication of the PTA to collect, maintain, or disseminate PII and/or PHI. If there have been no major changes made to the system, then a PIA is required every three years.

(3) A PIA is required when the PTA identifies that PII and/or PHI is being collected, maintained, or disseminated. As set forth in the VA A&A process, systems will be assessed to identify whether PII and/or PHI is being collected or changes have occurred that require a new PIA.

3. RESPONSIBILITIES

a. **The Assistant Secretary for Information and Technology (ASIT).** The ASIT, as the Department's Chief Information Officer (CIO) and Senior Agency Official for Privacy (SAOP), will:

(1) Ensure that a mechanism is in place for the review, and approval of all PIAs per OMB's instructions;

(2) Ensure the monitoring of all VA-wide systems for compliance with security and privacy statements contained in the respective PIAs; and

(3) Designate the Director of Office of Privacy and Records Management (OPRM) as the principal Department official responsible for ensuring the reporting of all PIAs received pursuant to the E-Government Act of 2002.

b. **The Director of OPRM.** The Director of OPRM will:

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

(2) Ensure that the PTA and PIA templates and instructions are made available to the Privacy Officer (PO), System Owner (SO) and the Information Security Officer (ISO); and

(3) Ensure that guidance and assistance is provided that meets OMB and VA requirements;

c. **Director, Privacy Service.** The Director will establish Enterprise-wide privacy compliance requirements and processes by:

(1) Enforcing all PTA and PIA compliance responsibilities as designated by the Director of OPRM;

(2) Developing PTA and PIA templates and instructions;

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

(4) Review each PIA received and submit approved PIAs to the O&IT CIO, as appropriate; and

(5) Publish approved PIAs on the VA web site.

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

(1) Perform 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 privacy sensitive information that could potentially require a PIA.

e. **Inspector General.** This Office will be requested to independently create and maintain PTAs, PIAs, SORNs, and similar documentation as part of its self-governing IT and privacy operations.

f. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials will be requested to:

(1) Work in conjunction with the VA Privacy Service to enforce PTA and PIA requirements; and

(2) Monitor compliance with security and privacy statements in each PIA for all rulemaking, IT programs, and/or projects under their authority.

g. **Program Managers.** Program Managers will:

(1) Work with Project Managers, System Managers/System Owners, POs, and ISO to complete the PTA and determine whether a PIA is necessary for the rulemaking, IT programs, and/or projects being commenced or significantly modified

(2) Validate that PTAs and PIAs are completed in a timely and accurate manner in accordance with guidance established by this Directive;

(3) Ensure that PTAs are reviewed annually and PIAs are updated accordingly; and

(4) Affirm that each project for which they are responsible is compliant with the security and privacy mitigations stated in the PIA.

h. **Project Managers.** Project Managers will:

(1) Coordinate with POs, Program Managers, ISOs, and System Managers/System Owners to complete the PTA and complete a PIA, if necessary;

(2) Ensure that PTAs and PIAs are completed in a timely and accurate manner in accordance with the guidance established by this Directive;

(3) Coordinate with their POs, ISOs, System Managers/System Owners, and with VA Privacy Service to ensure that all PTAs and PIAs under the responsibility of these officials are finalized;

(4) Initiate or update all PTAs and PIAs as set forth in this policy; and

(5) Ensure that each rulemaking, IT program, and/or project is compliant with security and privacy requirements described in each PIA.

i. **System Managers/System Owners.** The System Manager/System Owners will:

(1) Work with the PO, Program Manager, Project Manager, ISO, and System Developer to address the rulemaking, IT program, and/or project privacy issues that are identified through completion of the PTA;

(2) Work with the PO to finalize the PTA and prepare a PIA, if necessary;

(3) Obtain the Program and Project Manager's approval of PTA and PIA submissions;

(4) Submit Standard PTAs and PIAs to VA Privacy Service for review and approval; and

(5) Serve as point of contact for the system.

j. **System Developers.** System Developers will:

(1) Ensure that the system design and specifications conform to privacy standards and requirements; and

(2) Ensure that technical controls are in place for safeguarding PII and/or PHI from compromise or unauthorized access.

k. **Data Owners.** Data Owners will:

(1) Work with the POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions;

(2) Serve as point of contact for questions related to system data; and

(3) Respond to questions from POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers that are related to the PA submission.

l. **Information Security Officers (ISO).** ISOs will coordinate with their Privacy Officers and System Managers to ensure that security risks are identified and documented in all PIA submissions. In addition, Information Security Officers shall coordinate with their POs, their System Managers, and VA Privacy Service to ensure that the PIA(s) for each system is finalized.

m. **Privacy Officers (PO).** POs will coordinate with their local ISOs and System Managers to ensure that all data and associated risks are identified and documented in all PTA and PIA submissions. In addition, POs shall work with their ISOs, System Managers, and VA Privacy Service to ensure that the PIA(s) for each system immediate area of operation is of a quality that will reasonably ensure its approval by VA Privacy Service. PO's who are also identified and tasked by the Business Sponsor to be the IPT Privacy Officer for PMAS programs or projects will review and make determinations whether or not a PIA is required for the program of project.

4. REFERENCES

a. Clinger-Cohen Act of 1996, 40 U.S.C. §§ 11101 and 11103.

b. E-Government Act of 2002 (Pub. L. 107-347), 44 U.S.C. Chapter 36.

c. Federal Information Security Management Act (FISMA) of 2002.

d. Paperwork Reduction Act of 1995 (as amended by Clinger-Cohen Act of 1996).

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

f. NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information

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

h. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems.

i. OMB Memo-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003).

j. VA Directive 6212, Security of External Electronic Connections.

k. VA Directive 6500, Information Security Program.

l. VA Directive 6502, Enterprise-wide Privacy Program.

m. VA Handbook 6300.2, Management of the Vital Records Program.

n. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA).

o. VA Handbook 6300.5, Procedures for Establishing and Managing a Privacy Act System of Records.

p. VA Handbook 6500, Information Security Program.

5. DEFINITIONS

a. **Data Owner.** A person who can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.

b. **Information Technology (IT).** Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(1) Of that equipment; or

(2) Of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.

c. **Major Change.** A change to the information collected or maintained that could result in greater disclosure of information or a change in the way personal data is used.

d. **Protected Health Information (PHI)** PHI, for purposes of this VA 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. 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 education records. It includes genetic information.

e. **Personally Identifiable Information (PII).** A subcategory of VA Sensitive Data, PII means any information about the individual maintained by an agency, including but not limited to the following:

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

(2) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records or any other personal information which is linked or linkable to an individual.

f. **Practice.** Practice is the actual performance or application of a repeated or customary action.

g. **Privacy Impact Assessment (PIA).** A PIA is an analysis that seeks to identify and mitigate the privacy and security risks associated with the use of PII by a program, system, or practice. A PIA provides a framework for examining whether privacy, security and other vital data issues have been identified, addressed, and incorporated into the plan, design, operation, maintenance, and disposal of electronic information systems. PIAs are required to be performed in the conceptualization phase of the system lifecycle and updated whenever a system change could create a new privacy risk.

h. **Privacy Threshold Analysis (PTA)**. A PTA is used to identify IT systems, rulemakings for privacy risks, programs, or projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Director, VA Privacy Service, and to assess whether there is a need for a PIA. A PTA includes a general description of the IT system, technology, rulemaking, program, project, or other Department activity and describes what PII is collected (and from whom) and how that information is used.

i. **Program.** A planned, coordinated group of projects, services, activities, procedures, etc., often for a specific purpose or designed to meet a public need.

j. **Program Manager.** An individual who devises and executes a plan of action aimed at accomplishing a clear objective, with details on what work is to be done, by whom, when, and what means or resources will be used.

k. **Project.** A set of interrelated tasks to be executed over a fixed period which creates a unique product or service.

l. **Project Manager.** An individual who arranges a set of interrelated tasks to be executed over a fixed period and within certain cost and other limitations.

m. **Rulemaking.** The process that executive agencies use to implement, interpret or prescribe law or policy, or to describe the organization, procedure or practice requirements of any agency. This term includes the amendment or repeal of an existing rule. An example of a rulemaking is the issuance or amendment of a regulation.

n. **System.** A working combination of hardware, software, and data communications devices.

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

p. **System Manager.** An administrator of distributed or central computer systems who is responsible for system storage management, fault management, configuration management, performance management, and user activities monitoring.

q. **VA Sensitive Information/ Data.** All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act.