

## PRIVACY EVENT TRACKING

**I. REASON FOR ISSUE:** This handbook revises Department-wide procedures for the OneVA tracking of complaints and privacy incidents, and implements the policies set forth in Department of Veterans Affairs (VA) Directive 6502, VA Enterprise Privacy Program, and VA Handbook 6500.2, Management of Security and Privacy Incidents.

**2. SUMMARY OF CONTENTS/MAJOR CHANGES:** In accordance with provisions of VA Directive 6502, Privacy Program, and in order to centralize and monitor the complaint and privacy incident resolution process, VA has established a system for privacy event tracking. This handbook describes the responsibilities, requirements, and procedures for this process. The system for tracking privacy events, currently called the Privacy Violation Tracking System (PVTs), serves as a central repository of complaints and privacy incidents. The system for tracking privacy events provides a Department-wide log of complaints and privacy incidents that are registered by VA personnel, Veterans, or their dependents and beneficiaries under applicable Federal privacy laws and regulations. The complaints and privacy incidents are addressed by VA Privacy Officers (PO) in compliance with applicable Federal privacy laws and regulations.

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

**4. RELATED DIRECTIVE:** VA Directive 6502, VA Enterprise Privacy Program.

**5. RESCISSION:** VA Handbook 6502.1, Privacy Violation Tracking System (PVTs), dated March 25, 2004.

**CERTIFIED BY:**

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

*/s/*

Roger W. Baker  
Assistant Secretary for  
Information and Technology

*/s/*

Roger W. Baker  
Assistant Secretary for  
Information and Technology

Distribution: Electronic Only

**PRIVACY EVENT TRACKING  
CONTENTS**

<b>PARAGRAPH</b>	<b>PAGE</b>
1. PURPOSE AND SCOPE.....	5
2. RESPONSIBILITIES.....	6
3. ESSENTIAL REQUIREMENTS AND PROCEDURES.....	8
4. ESCALATION.....	10
5. AUDIT.....	11
6. REFERENCES.....	11
7. DEFINITIONS.....	13

## PRIVACY EVENT TRACKING

### 1. PURPOSE AND SCOPE

a. This handbook provides the OneVA procedures and requirements for recording privacy-related complaints and privacy incidents in the designated system for tracking privacy events, currently called the Privacy Violation Tracking System (PVTS). Privacy event tracking is a component of the Department of Veterans Affairs (VA) Privacy Program, mandated in VA Directive 6502, VA Enterprise Privacy Program, and administered by the VA Office of Information Security, Privacy Service.

b. Federal privacy regulations and guidance provide individuals with a right to file a complaint about the manner in which VA maintains their personally-identifiable information (PII), and any observed or perceived lapses in VA's protection of PII. The system for tracking privacy events provides a VA-wide centralized, auditable database of all Health Insurance Portability and Accountability Act (HIPAA) complaints and privacy incidents.

c. The system for privacy event tracking documents all HIPAA complaints and potential or actual privacy incidents received from VA Privacy Officers (PO). It also provides statistics to the VA Privacy Service and VA management. This system supports the "documentation of privacy complaints" requirement in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164, as published by the Department of Health and Human Services (HHS) as well as the requirements of Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450, codified at 38 U.S.C. §§ 5721-28, which mandates procedures for:

- (1) Detecting, immediately reporting, and responding to security incidents;
- (2) Notifying Congress of any data breaches involving sensitive personal information; and
- (3) Providing credit protection services, if necessary, to those individuals whose sensitive personal information has been compromised.

d. In order to achieve consistent privacy practices throughout the Department, this system is for use VA-wide. However, it is not intended to replace existing practices for documenting information requests made under the Freedom of Information Act (FOIA), the Privacy Act of 1974, or the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

e. This handbook identifies the required minimal elements for the documentation of the HIPAA complaint and privacy incident registration and resolution process in the system for tracking privacy events. It also provides the procedures for VA Privacy Service audit of these HIPAA complaints and privacy incidents.

## 2. RESPONSIBILITIES

a. **The Assistant Secretary for Information and Technology (AS/IT).** The AS/IT shall ensure that funding is in place to provide a mechanism for the tracking of HIPAA complaints and privacy incidents.

b. **Deputy Assistant Secretary, Information Security (DAS IS).** The DAS IS shall work with the DAS for Enterprise Development to ensure that required updates and modifications are made to the system for tracking privacy events.

c. **Deputy Assistant Secretary, Office of Enterprise Development (DAS OEM).** The DAS OEM shall collaborate with the DAS IS in the development of updates, modification, or in the development of any new system for tracking privacy events.

d. **Associate Deputy Assistant Secretary, Office of Privacy and Records Management (ADAS OPRM).** The ADAS OPRM shall work with the Director of the Office of Risk Management and Incident Response to ensure that all HIPAA complaint and privacy incident reporting requirements currently in place are met by the system for privacy event tracking.

e. **Director, VA Privacy Service.** The Director shall establish the OneVA procedure for tracking and auditing HIPAA complaints and privacy incidents by:

(1) Managing a Department-wide system to track HIPAA complaints and privacy incidents;

(2) Providing a manual to POs explaining the functions and reporting requirements of the Department-wide system, and instructions for the use of the system for tracking privacy events;

(3) Maintaining audit records and documentation provided by the system for tracking privacy events;

(4) Reporting to oversight agencies and VA management on HIPAA complaints and privacy incidents;

(5) Providing oversight and guidance for VA compliance with law and regulations applicable to HIPAA complaints and privacy incidents;

(6) Designating a system for tracking privacy events, in accordance with the requirements of VA Directive 6502, VA Enterprise Privacy Program;

(7) Setting the requirements and access rights for submission of all HIPAA complaints and privacy incidents to the system for tracking privacy events; and

(8) Ensuring the security and privacy requirements of the system for tracking privacy events and the records that it generates, stores, and transmits are met.

f. **Director, Risk Management and Incident Response.** The Director shall periodically review the privacy incidents captured in the system for tracking privacy events in accordance with VA policy.

g. **Inspector General.** The Inspector General will be requested to:

(1) Provide assistance and guidance to the VA Privacy Service in the conduct and design of audits of the system for tracking privacy events;

(2) Review and monitor the VA Privacy Service audits of the system for tracking privacy events; and

(3) Provide recommendations on the HIPAA complaint and privacy incident resolution process.

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

(1) Ensure that POs report all HIPAA complaints, where appropriate, and actual or suspected privacy incidents within one hour of their discovery during normal business hours and as soon as possible outside of normal business hours, using the designated system for privacy event tracking;

(2) Ensure that POs, and other authorized users, record all updates and resolutions of HIPAA complaints, as appropriate, and privacy incidents, into the designated system for tracking privacy events, as soon as possible; and

(3) Provide guidance on the appropriate complaint and privacy incident referral process.

i. **VHA Privacy Officers.** As Privacy Officers acting within VA's Covered Entity, VHA POs shall:

(1) Report all HIPAA complaints and potential or actual privacy incidents using the designated system for tracking privacy events, within one hour of discovery during normal business hours and as soon as possible outside of normal business hours;

(2) Update and resolve all HIPAA complaints and privacy incidents as soon as possible;

(3) Obtain and maintain their usernames and passwords for the system for tracking privacy events; and

(4) Review and investigate all HIPAA complaints within the PO's purview to determine if facts support that the complaint be escalated to a privacy incident.

j. **Non-VHA Privacy Officers.** VA POs who do not work for VHA shall:

- (1) Report all potential or actual privacy incidents using the designated system for tracking privacy events within one hour of discovery during normal business hours, and as soon as possible outside of normal business hours;
- (2) Update and resolve all privacy incidents as soon as possible; and
- (3) Obtain and maintain their usernames and passwords for the system for privacy event tracking.

k. **The VA Network and Security Operations Center (VA-NSOC).** The VA-NSOC shall:

- (1) Provide and maintain a program capable of tracking HIPAA complaints and privacy incidents in accordance with the security and privacy requirements determined by the VA Privacy Service;
- (2) Train VA-NSOC call center personnel according to the requirements for the system for tracking privacy events that is designated by the VA Privacy Service;
- (3) Provide secure and limited access to the system for tracking privacy events through a system of user licenses and passwords; and
- (4) Provide for the notification of complaints and privacy incidents through the privacy hierarchy in the appropriate VA Administration, Staff Office or facility.

### 3. ESSENTIAL REQUIREMENTS AND PROCEDURES

a. **General Procedures.** As the manager of the system for tracking privacy events, the VA-NSOC maintains the database and provides secure and limited access to it through a system of user licenses and passwords. The system designated for tracking privacy events must:

- (1) Generate statistical reports about the number and status of tickets reflecting HIPAA complaints and privacy incidents in accordance with requirements provided by the VA Privacy Service;
- (2) Enter HIPAA complaints and privacy incidents into a database that may be monitored and audited by the VA Privacy Service;
- (3) Record HIPAA complaints and privacy incidents and their resolutions into tickets;
- (4) Escalate delinquent tickets automatically; and
- (5) Report the statistics of complaints, and privacy incidents.

b. **Recording Complaints and Incidents.** POs are responsible for recording all HIPAA complaints or suspected or actual privacy incidents into the system designated for tracking privacy events within one hour of discovery during normal business hours and as soon as possible outside of normal business hours. A HIPAA complaint or privacy incident is recorded when it is entered into the system for tracking privacy events via a Web-based form. A description of each menu and instructions for using the system can be found in the manual for system for tracking privacy events. The required elements of the recording procedure are:

(1) **Entry of the Event.** The HIPAA complaint or privacy incident is entered into the system for tracking privacy events by one of two ways:

(a) The PO enters a HIPAA complaint or privacy incident into the system for tracking privacy events by opening a ticket, as soon as possible after the complaint is received or the privacy incident is recognized; or

(b) The VA-NSOC receives a HIPAA complaint or notification of possible privacy incident through the call center (via phone or email) and enters the complaint or privacy incident into the system for tracking privacy events by opening a ticket and assigning it to the appropriate PO, who is then notified of the opened ticket and assumes responsibility for resolution.

(2) **Categorization.** The HIPAA complaint or privacy incident must be categorized by the PO according to the type(s) of event. The system for tracking privacy events lists the information categories in a menu.

(3) **Description.** A complete description of the nature of the HIPAA complaint, or privacy incident must be entered into the ticket.

(4) **Definition.** The HIPAA complaint or privacy incident must be further defined according to the type of data breach that is alleged. The following types of data breaches are specified in the privacy event tracking system manual, listed in a menu of the system for tracking privacy events, and will be updated as required:

(a) Safeguard Events – data breaches or other failures of administrative, technical, and physical safeguards, and are always considered privacy incidents;

(b) Collection – a compilation of PII that is not authorized, relevant, or necessary, as provided in applicable law;

(c) Disclosure – the communication of PII in any medium without proper authority, or in an improper manner;

(d) Usage Event – sharing, examination, or analysis of PII that is not required for the official performance of authorized VA duties under applicable law;

(e) Disposal – unauthorized deletion or destruction of PII or improper disposal of properly discarded material; and

(f) Access and amendment – potential privacy incidents that pertain to denial of the right of access and of the right to request an amendment that are specific to the requirements of the HIPAA Privacy Rule and the Privacy Act.

c. **Resolution of Complaints and Incidents.** The PO must resolve each HIPAA complaint or privacy incident as soon as possible. The types of corrective actions may include education, reprimand, or sanction. The following types of corrective actions are illustrative of the categories that are specified in the user manual for the system for tracking privacy events and will be updated as required.

(1) **Education.** If the PO or resolution authority determines that the data breach occurred because VA personnel were not informed of their responsibilities, or the requirements for the proper use, disclosure, or collection of PII, the category “Education” should be selected and remedial training assigned.

(2) **Reprimand.** If the PO proposes it, and the supervisor and resolution authority such as the Human Resources Specialist determines that VA personnel have engaged in unacceptable actions or inactions resulting in the reported data breach, the category “Reprimand” should be selected.

(3) **Sanction.** If the PO proposes it, and the resolution authority such as the Human Resources Specialist determines that VA personnel have engaged in unacceptable actions that warrant personnel sanctions, the category “Sanction” should be selected.

(4) **No Data Breach.** If the PO determines that the reported HIPAA complaint or privacy incident is not a data breach under law or VA policy, the category “No Incident” should be selected.

d. **Referral of Complaints and Incidents through the Privacy Hierarchy.** If the call center receives a HIPAA complaint or privacy incident directly from the complainant, then the call center should refer the complaint or privacy incident to the appropriate PO. If a PO cannot resolve the HIPAA complaint or privacy incident, then he or she should refer the complaint or privacy incident to the next level of the privacy hierarchy within his or her organization or facility as soon as possible.

e. **Referral to the Secretary of Health and Human Services.** HIPAA complaints may be referred to HHS by the appropriate resolution authority when the complainant is unsatisfied with the final VA determination regarding his or her complaint.

#### 4. ESCALATION

a. Typically, each Administration and Staff Office assigns the PO to a privacy hierarchy beginning at the facility level, and moving up to VISN/regional and headquarters levels. The number of levels will vary with the size of the Administration or Staff Office. The privacy hierarchy will be observed when following complaints and privacy incidents through the appropriate resolution process.

b. If a ticket has not been acted upon, or does not show a change of status in a period of time designated by the VA Privacy Service, the ticket will automatically escalate to the next level in the privacy hierarchy. The next higher level PO will be notified that the ticket has not been acted on or a change in status has not been made then, he or she will be responsible for working with the originating PO to ensure the ticket is resolved.

c. Privacy incidents that cannot be resolved within the Administrations or Staff Offices, such as those pertaining to cross-organizational procedures, will be escalated to the VA Privacy Service.

## 5. AUDIT

a. Records of the number, type, resolution, and status of HIPAA complaints and privacy incidents will be maintained in the system for tracking privacy events. The system for tracking privacy events will generate statistical analyses of these records according to direction provided by the VA Privacy Service. The VA Privacy Service, VA NSOC, and the Office of Risk Management and Incident Response (RMIR) Incident Response Team (IRT) will have access to all records and reports. POs will have access to the statistical reports and tickets that fall under their authority. Information on how to generate reports is provided in the user guide for the system for tracking privacy events.

b. The VA Privacy Service will provide periodic reports of the VA-wide status of HIPAA complaints and privacy incidents. The VA Privacy Service will provide these reports to the VA Chief Information Officer (CIO), each Administration, and to other entities or Federal agencies in compliance with applicable privacy law.

## 6. REFERENCES

- a. 38 C.F.R. Part 75, Information Security Matters.
- b. 38 U.S.C. 5701, Confidential Nature of Claims.
- c. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records, 17.500-.511.
- d. 38 U.S.C. 7332, Confidentiality of Certain Medical Records, 1.460-1.496.
- e. Freedom of Information Act (FOIA), 5 U.S.C. 552.
- f. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191.
- g. HIPAA Privacy Rule, 45 CFR Parts 160 and 164.
- h. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

- i. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.
- j. Privacy Act of 1974, 5 U.S.C. 552a.
- k. Privacy Violation Tracking System Manual.
- l. VA Directive 6066, Protected Health Information.
- m. VA Directive 6371, Destruction of Temporary Paper Records.
- n. VA Directive 6500, Information Security Program.
- o. VA Directive 6502, VA Enterprise Privacy Program.
- p. VA Directive 6600, Responsibility of Employees and Others Supporting VA in Protecting Personally Identifiable Information (PII).
- q. VA Directive 6609, Mailing of Personally-Identifiable and Sensitive Information.
- r. VA Handbook 6300.2, Management of the Vital Records Program.
- s. VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act (FOIA).
- t. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA).
- u. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records.
- v. VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses.
- w. VA Handbook 6300.8, Procedures for Shipment of Records to the VA Records Center and Vault in Neosho, Missouri.
- x. VA Handbook 6301, Procedures for Handling Electronic Mail Records.
- y. VA Handbook 6330, Directives Management Procedures.
- z. VA Handbook 6500, Information Security Program.
- aa. VA Handbook 6500.1, Electronic Media Sanitization.
- bb. VA Handbook 6500.2, Management of Security and Privacy Incidents.

- cc. VA Handbook 6500.3, Certification and Accreditation of VA Information Systems.
- dd. VA Handbook 6502.3, Web Page Privacy Policy.
- ee. Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. 109-461, codified at 38 U.S.C. §§ 5721-28.

## 7. DEFINITIONS

a. **Call Center.** The call center is a branch of the VA-NSOC that receives complaints or notifications of possible privacy incidents by telephone or email, enters these complaints and privacy incidents into the system for tracking privacy events, and refers each complaint and privacy incident to the appropriate PO.

b. **Covered Entity.** A covered entity is an organization or individual that is covered by the compliance requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and is:

- (1) A health care provider that conducts certain transactions in electronic form;
- (2) A health care clearinghouse; or
- (3) A health insurance plan.

c. **Data Breach.** A data breach is the loss, theft, unauthorized access, or any access other than that which is incidental to the scope of employment of VA personnel, to data containing PII, in electronic or printed form that results in the potential compromise of the confidentiality or integrity of the data.

d. **HIPAA Complaint.** A HIPAA complaint is the formal registration of any grievance to VHA, as VA's only covered entity, concerning the way that Protected Health Information (PHI) is collected, maintained, stored, disseminated or disposed of. Access and amendment complaints, which pertain to denial of access and amendment rights, are considered complaints.

e. **Incident.** The term "incident" means "security incident" as defined in 38 U.S.C. § 5727(18).

f. **Personally-Identifiable Information (PII).** Typically, PII casts a wider net than VA sensitive personal information (SPI); however, for purposes of this Handbook, PII is considered to be the same as VA SPI (see definition below). PII is any information about an individual that can reasonably be used to identify that individual, and that is maintained by VA. PII includes but is 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. Different PII may have different levels of sensitivity. For example, at VA, some PII is public (e.g., the names, titles and salaries of VA officials) and is not considered sensitive.

g. **Privacy Incident** A privacy incident is a privacy or security-related event in which PII may have been exposed through either unauthorized access or disclosure; it includes the loss, theft, or inadvertent misdirection of PII and any other unauthorized access, or any other access other than that which is incidental to the scope of employment, to data containing PII in electronic, printed, or any other format, and results in the potential compromise of the confidentiality or integrity of the data regardless of the manner in which the breach might have occurred.

h. **Privacy Hierarchy.** The privacy hierarchy is the organization of each Administration's or Staff Office's cadre of POs according to increasing responsibilities and authority over privacy-related matters.

i. **Resolution.** A resolution is the representation of the corrective action taken by the manager, Human Resources Representative, or authorized official, in accordance with VA policy, in response to a complaint or privacy incident. Resolution includes "no action taken" if no privacy incident is found or "no action necessary" if the complaint is determined to be unfounded.

j. **Resolution Authority.** Resolution authority is the supervisor of the individual who caused the incident, their Human Resources Representative or another official with the authority and responsibility to enforce a recommended resolution.

k. **Sensitive Personal Information (SPI).** For purposes of this Handbook, the term PII is being used interchangeably with SPI, as defined in 38 U.S.C. § 5727(19), 38 C.F.R. § 75.112, and VA Handbook 6500. SPI is a statutory term unique to VA while PII is the term used elsewhere in the Federal government and in the private privacy industry. SPI is defined 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. SPI includes PHI. Within VA, PHI is specific to VHA and refers to individually-identifiable health information covered by HIPAA.

l. **Ticket.** The ticket is the Web-based form in which each complaint, or privacy incident is recorded and tracked within the designated system for privacy event tracking. "Complaint" encompasses only the privacy aspect of the ticket, whereas "privacy incident" also incorporates security elements.