Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6500.2
Transmittal Sheet
July 28, 2016

MANAGEMENT OF BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION

1. **REASON FOR ISSUE:** This Handbook establishes procedures for Department of Veterans Affairs (VA) management of breaches involving VA Sensitive Personal Information (SPI). It implements 38 U.S.C. §§ 5721-28 and 38 C.F.R. §§ 75.111-119; section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (codified at 42 U.S.C. § 17932) and the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule at 45 C.F.R. §§ 164.400-414; the Privacy Act of 1974; and Office of Management and Budget (OMB) Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES**: This Handbook:

   a. Establishes revised procedures for managing breaches and updates the criteria used to determine whether a reported incident is a breach involving VA SPI. It also contains the criteria used to determine whether VA should notify or offer credit protection services to individuals whose VA SPI is involved in a breach ("record subjects");

   b. Contains the roles and responsibilities of VA organizations for the oversight, management, and reporting of incidents and breaches; and

   c. Describes the updated processes that VA has implemented to comply with the breach notification provisions of the HITECH Act and the HIPAA Breach Notification Rule**.**

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005), Office of Information Security (005R), Office of Privacy and Records Management (OPRM) (005R1), Data Breach Response Service (005R1E).

4. RELATED DIRECTIVE/HANDBOOK: VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*, September 20, 2012; and VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,* March 10, 2015.

5. **RESCISSIONS:** VA Handbook 6500.2, *Management of Security and Privacy Incidents*, January 6, 2012.

CERTIFIED BY:

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

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

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

Distribution: Electronic Only

MANAGEMENT OF BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION

TABLE OF CONTENTS

1. PURPOSE AND SCOPE 5
2. BACKGROUND 5
3. ROLES AND RESPONSIBILITIES TABLES 7
TABLE 1 SECRETARY 7
TABLE 2 UNDER SECRETARIES, ASSISTANT SECRETARIES, AND 7
KEY OFFICIALS 7
TABLE 3 DATA BREACH RESPONSE SERVICE 7
TABLE 4 DATA BREACH CORE TEAM (DBCT) 10
TABLE 5 VA-NSOC 10
TABLE 6 OFFICE OF ACQUISITION AND LOGISTICS 12
TABLE 7 FACILITY CHIEF INFORMATION OFFICERS (FCIO) 12
TABLE 8 PRIVACY OFFICERS (PO) 14
TABLE 9 INFORMATION SECURITY OFFICERS (ISO) 16
TABLE 10 SUPERVISORS 17
TABLE 11 USERS OF VA INFORMATION AND INFORMATION SYSTEMS 18
TABLE 12 PUBLIC AFFAIRS OFFICERS (PAOs) 18
4. INCIDENT MANAGEMENT PROCESS 20
5. VA CRITERIA FOR BREACH AND RISK ASSESSMENT 21
6. BREACH MANAGEMENT OVERSIGHT STRUCTURE 23
7. BREACH MANAGEMENT PROCESS 25
8. VA HITECH AND HIPAA BREACH NOTIFICATION RULE COMPLIANCE OVERVIEW 52
9. INDIVIDUAL, MEDIA, AND HHS BREACH REPORTING PROCESS 52
10. HITECH/HIPAA SIGNIFICANT RULING NOTIFICATION PROCESS 54
11. BREACH NOTIFICATION AND THE VHA PAO 61
12. HIPAA/HITECH LAW ENFORCEMENT DELAY OF NOTIFICATION 62
13. TERMS AND DEFINITIONS 62
14. REFERENCES 64

MANAGEMENT OF BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION

1. PURPOSE AND SCOPE

a. **Purpose**. This Handbook provides oversight, management, and reporting procedures to ensure appropriate and expeditious managing of breaches involving Sensitive Personal Information (SPI) under the ownership of the Department of Veterans Affairs (VA). This Handbook also contains the criteria that should be used to determine whether a reported incident is a breach involving SPI, and whether VA should notify or offer credit protection services to the record subjects

b. **Scope**. The procedures in this Handbook apply to VA employees, contractors, researchers, students, volunteers, and all other individuals authorized access to VA information or information systems in order to perform a VA-authorized activity (hereinafter referred to as "VA Personnel," unless otherwise indicated). This Handbook does not address VA's response to a data breach involving other VA sensitive data that is not SPI, such as embargoed budget data.

2. BACKGROUND

a. The primary goal in managing breaches is to provide prompt and accurate notification and remediation, if necessary, to those individuals whose SPI may have been inappropriately, accessed, used, or disclosed in a manner not permitted by applicable confidentiality provisions. Another significant goal is to ensure continued public trust in VA as the guardian of SPI with which VA has been entrusted. NOTE: SPI includes personally identifiable information (PII) and protected health information (PHI).

b. Prompt risk identification, subject notification, and remediation involves close coordination, both within VA through the activities of the Data Breach Response Service, and with entities outside of VA, such as the US Computer Emergency Readiness Team (US CERT), Office of Management and Budget (OMB), and Congressional committees. This Handbook provides guidelines to enhance coordination efforts for greater efficiency, accuracy, and promptness in communicating with the record subjects.

c. VA's breach management process incorporates compliance with all relevant breach response laws, regulations, and policies, as explained below:

(1) OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification (Sept. 20, 2006), provides recommendations for planning and responding to data breaches that could result in identify theft. As a result, VA established a national Data Breach Response Service to support local and regional Data Breach Response Teams for the management of VA breaches.

(2) The VA Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450 (codified at 38 U.S.C. §§ 5721-28), established information technology (IT) requirements for VA SPI. The Act mandated, among other things, that VA develop procedures for detecting, immediately reporting, and responding to security incidents; notify Congress of any significant data breaches involving SPI; and, if necessary, provide credit protection services to those

individuals whose SPI may have been compromised. VA has promulgated implementing regulations at 38 C.F.R. Part 75, Information Security Matters.

(3) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), required agencies to develop and implement a breach notification policy while maintaining proper safeguards to protect such information.

(4) Section 13402 of the HITECH Act and the HIPAA Breach Notification Rule at 45 C.F.R. § 164.400-414 required covered entities (CEs) and their business associates (BAs) to notify individuals of breaches involving their unsecured PHI. The VA Data Breach Response Service provides breach incident response activities as a BA to the Veterans Health Administration (VHA), the CE under HIPAA.

d. Based on these above authorities, an incident is any event that has resulted in, or has the potential to result in, unauthorized access to or disclosure of VA SPI in a manner not permitted under the applicable confidentiality provisions**.**

3. ROLES AND RESPONSIBILITIES TABLES

TABLE 1	SECRETARY
Role	**Responsibilities**
Incident Preparation	1. Designate the Office of Information and Technology (OI&T), Office of Privacy and Records Management (OPRM), and the Data Breach Response Service to provide policy, procedures, and adequate resources to the POs and ISOs in the field for managing incidents. 2. Ensure that every VA Facility and Staff Office has a designated PO and ISO.
Incident Prevention	3. Ensure that there is a VA user awareness and training program to educate users on appropriate privacy and security procedures. 4. Create, communicate, and enforce a set of clear rules governing the use of PHI and PII.

TABLE 2	UNDER SECRETARIES, ASSISTANT SECRETARIES, AND KEY OFFICIALS
Role	**Responsibilities**
Incident Preparation	1. Ensure that all users of VA information or information systems under their responsibility take annual security and privacy training in accordance with VA policies. 2. Ensure that users support and comply with the incident response process. 3. Ensure appropriate Regional and Local Data Breach Mitigation Teams are established within each organization in accordance with VA Directives 6500 and 6502.
Incident Prevention	4. Implement and comply with all VA policies, directives, and handbooks on information security, privacy, and records management regarding the use, disclosure, storage, transmission, and protection of VA information in their organization.

TABLE 3	DATA BREACH RESPONSE SERVICE
Role	**Responsibilities**
Oversight Support	1. Implement and follow up on decisions made by the DBCT. 2. Confer with other VA Senior Management officials and/or external authorities on breaches as necessary.
Incident Preparation	3. Ensure VA-wide incident response policies are aligned with applicable federal law and guidance as well as the Secretary's and OI&T goals and objectives related to IT. 4. Establish and maintain formal and informal incident response communication channels with stakeholders throughout the organization.

TABLE 3	DATA BREACH RESPONSE SERVICE
Role	**Responsibilities**
	5. Set high-level compliance doctrines across the organization. 6. Provide advance planning, guidance, analysis, and recommendations to the VA Chief Information Officer (CIO), Regional Directors, local Directors, and VA senior management to properly address and mitigate potential incidents.
Incident Prevention	7. Ensure that VA policies and directives related to data confidentiality and protecting data from the risk of exposure to identity theft meet all federal requirements.
Incident Analysis	8. Draft monthly, quarterly, and ad hoc reports to Congress. 9. Respond to requests to address specific VA-wide IT incident response issues that may require study or analysis and recommend options for addressing these issues. 10. Perform breach analysis, defined as the process used to determine the likelihood of a breach to result in the misuse of SPI, upon request. 11. Manage contracts for all credit protection services, including breach analysis and independent risk analysis (IRA). 12. Identify incidents involving breaches by performing a daily evaluation on incidents from the Privacy and Security Event Tracking System (PSETS). 13. Coordinate and manage activities during incidents involving a breach. This includes providing credit monitoring service promotion codes within 48 hours of a request from the PO for the code. 14. Produce and maintain an incident communication plan coordinated with Office of Public Intergovernmental Affairs (OPIA), Office of Congressional Legislative Affairs (OCLA), and the Office of General Counsel (OGC) as necessary. 15. Provide the Administration and Staff Offices with a report of incidents requiring notification and/or credit monitoring that is still pending action. This is prepared to assist the Administrations and Staff Offices to meet the 30-day notification turnaround time after a breach. 16. Facilitate and participate in incident reviews. 17. Arrange for an IRA, if necessary, by a non-VA entity to determine the level of risk for potential misuse of any SPI involved in the breach. 18. Coordinate with other VA offices, as well as regional and local Data Breach Response Service teams to assure the appropriate risk-based, tailored response for privacy incidents within VA. 19. Work closely with other federal agencies, offices, and teams as appropriate.

TABLE 3	DATA BREACH RESPONSE SERVICE
Role	**Responsibilities**
	20. Ensure that Administrations and Staff Offices are aware of the Appeal Process for requesting reconsideration from the DBCT when they obtain new information about an incident, and request incidents be reopened, if necessary.
Incident Documentation	21. Maintain records about the status of each incident, along with other pertinent information. 22. Maintain a detailed log of actions, as necessary, taken by all parties working the incident. 23. Produce information for management as necessary for breaches including those that have unique circumstances. 24. Produce incident progress updates for management as necessary.
Incident Notification	25. Notify the Secretary, Inspector General, OMB, the House and Senate Committees on Veterans' Affairs, and other federal agencies, as required or appropriate. 26. Serve as liaison between the functional area(s) affected, VA organizations, and certain non-VA entities, including OMB, the Government Accountability Office (GAO), and Congress. 27. Fully integrate with already-established incident reporting and response processes and procedures of VA-NSOC, and work closely with VA-NSOC to provide timely and concise incident reports and fact synopses. These reports will be used to conduct a preliminary breach analysis in order to make risk-based decisions regarding breaches, potential identity theft, risk mitigation, and follow-up actions. 28. When an IRA is deemed necessary, issue instructions regarding mitigation of associated risk and concur with, or recommend, corrective actions to prevent a breach recurrence. 29. Coordinate with the DBCT in analyzing, addressing, and mitigating breaches to ensure timeliness, uniformity, and visibility of VA responses. Additionally, VA must follow and report the results of all assessments, plans, and procedures required under federal laws, regulations, executive instructions, and other legal authorities. 30. Coordinate with the DBCT for the responsibility of responding to breaches and addressing notification requirements from a collaborative perspective, whereby responsible parties will work together in formulating plans and sharing best practices. 31. Prepare the Monthly Report and Quarterly Notice to Congress on Data Breaches on the number of incidents involving exposure of SPI categorized by VHA, Veterans Integrated Service Networks (VISN), Veterans Benefits Administration (VBA) regions, and all others, as well as incidents that do not meet the notification timeframe.

TABLE 3	DATA BREACH RESPONSE SERVICE
Role	**Responsibilities**
Containment Strategy	32. Coordinate and advise in the execution of the containment strategy and efforts at the national level. 33. Make decisions about containment actions. 34. Report to senior VA officials on the status of the incident.

TABLE 4	DATA BREACH CORE TEAM (DBCT)
Role	**Responsibilities**
Oversight	1. Adjudicate specific incidents to determine type of event, impact, and reporting requirements.
Incident Prioritization	2. Provide administrative oversight of incident reporting involving the loss or compromise of data. 3. Has the authority and responsibility to escalate any incident, regardless of the risk assessment.
Incident Notification	4. Work with the Data Breach Response Service in analyzing, addressing, and mitigating breaches to ensure timeliness, uniformity, and visibility of VA responses. 5. Work with the Data Breach Response Service for the responsibility of responding to breaches and addressing notification requirements from a collaborative perspective, whereby responsible parties will work together in formulating plans and sharing best practices.
Containment Strategy	6. Determine need for initial notification and credit protection offers to individuals whose SPI was involved in a breach. 7. Coordinate response actions until the incident is resolved.

TABLE 5	VA-NSOC
Role	**Responsibilities**
Incident Preparation	1. Maintain contact information for team members and others within and outside VA, such as law enforcement (Office of the Inspector General (OIG)) and other incident response teams. 2. Ensure the field has appropriate incident response mechanisms, such as phone numbers, email addresses, and tools available to report suspected incidents. 3. Ensure that VA-NSOC staff is adequately trained to manage incidents and to assist the field. 4. Provide the necessary evidence collection, forensics, or containment actions as applicable. 5. Configure all hardware and software to ensure that reporting and alerts are proactive and effective in bringing abnormal conditions to the attention of the right people in a timely manner.

TABLE 5 VA-NSOC	
Role	**Responsibilities**
	6. Collaborate with stakeholder organizations to ensure they have an after-action report process in place to review root causes and future prevention mechanisms. 7. Ensure that incident escalation procedures are in place for reported events. 8. Ensure processes are clearly written, tested, and updated on a regular basis as conditions or changes occur in strategies, organizations, people, or devices.
Incident Prevention	9. Ensure that VA's network perimeter is configured to deny all unauthorized access. 10. Ensure only certified devices are placed into the operational enterprise and configurations are properly maintained to minimize potential compromise or other adverse events which could expose SPI to unacceptable risks. 11. Perform scans as necessary.
Incident Detection	12. Provide incident detection capabilities, systems, procedures, and expertise. 13. Configure and maintain monitoring capabilities of enterprise security systems.
Incident Analysis	14. Provide a central response coordination and incident management function for all incidents affecting the VA enterprise. 15. Validate that the occurrence of a breach involving an IT-based event is an incident. VA-NSOC will attempt to validate all reported IT-based events in order to eliminate false positives. Validation will be via an investigative process .VA-NSOC may request additional logs and other information in order to further validate the event. 16. If an event is determined to be an incident involving an IT-based breach of VA SPI, ensure that a PSETS Ticket is created and notify the Data Breach Response Service.
Incident Documentation	17. Collaborate with ISOs and PSOs, as necessary, to track (IT based systems) the progress of response activity via PSETS, if the event is determined to be a breach, and performing all necessary documentation of incident progress. 18. Update records (IT based systems) about the status of incidents, along with other pertinent information.
Incident Notification	19. Alert appropriate personnel about the potential or actual incident in a timely manner: a. Affected Network ISO/PO. b. Facility ISO and Technical point of contact (POC). c. CIO, Network CIO. d. Others as appropriate (e.g., US Computer Emergency Readiness

TABLE 5	VA-NSOC
Role	**Responsibilities**
	Team (US CERT), OIG, Law Enforcement). e. Notify US-CERT on incidents that involve IT based systems.
Containment Strategy	20. Direct a remediation strategy. 21. Coordinate, with the Data Breach Response Service, the response efforts. 22. Coordinate with network ISO and local ISOs and others as appropriate (e.g., US CERT, law enforcement, OIG, OCS). 23. Prepare situation updates on status throughout response efforts. 24. Recommend and coordinate containment actions.
Evidence Gathering and Management	25. Coordinate and assist law enforcement or the OIG with the collection of evidence. 26. Document all evidence collected and preserved, including compromised systems.

TABLE 6	OFFICE OF ACQUISITION AND LOGISTICS
Role	**Responsibilities**
Incident Preparation	1. In accordance with VA Handbook 6500.6, ensure that all contracts involving contractor access to VA-owned information or information systems, especially VA SPI, contain the appropriate security and privacy clauses as required by federal and VA Acquisition Regulations, VA policy including Handbook 6500.6, Contract Security, and other appropriate federal authorities.

TABLE 7	FACILITY CHIEF INFORMATION OFFICERS (FCIO)
Role	**Responsibilities**
Incident Preparation	1. Maintain current facility incident response contact information. 2. Make training available as is appropriate and necessary to the facility incident response personnel. 3. Ensure that all users of VA information and information systems under their responsibility take annual privacy training. 4. Work closely with the facility ISO to maintain continuity of service. 5. Ensure that all users of VA information and information systems under their responsibility take ownership/responsibility for the data at their disposal.
Incident Prevention	6. Adhere to VA configuration standards to ensure appropriate workstation and/or server setup by: a. Hardware/software patch installation and maintenance b. Anti-virus software and patch installation and maintenance c. Appropriate configuration setup and maintenance 7. Ensure the appropriate user awareness and training programs on

TABLE 7	FACILITY CHIEF INFORMATION OFFICERS (FCIO)
Role	**Responsibilities**
	privacy procedures are available. 8. Ensure that users are aware of the reporting procedures and the policies in place to protect information systems, employees, and property. 9. Conduct regular review of user level permissions to network shares. 10. Maintain a strong working relationship with the facility ISO and PO. 11. Ensure systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored and/or rebuilt.
Incident Detection	12. Implement enterprise tools in a timely fashion. 13. Provide consistent monitoring and automated alert implementation. 14. Maintain a strong working relationship with staff to encourage reporting of incidents/suspected incidents.
Incident Analysis	15. Maintain pertinent information including, but not limited to, audit and event logs as well as user account information when appropriate.
Incident Documentation	16. Provide updates to open incidents as directed. 17. Provide input as required in any documentation requested from top management both inside and outside the facility. 18. Safeguard data and sensitive information related to the incident. 19. Ensure that access to incident data is properly restricted.
Containment Strategy	20. Coordinate and advise in the execution of the containment strategy and efforts at the regional and local levels. 21. Make decisions about containment actions. 22. Coordinate response actions until the incident is resolved. 23. Report to senior VA officials on the status of the incident. 24. Work with the OI&T staff to assure containment actions are performed in a timely and efficient manner. 25. Safeguard the integrity of involved hardware/software as appropriate.
Evidence Gathering and Management	26. Preserve hardware/software as appropriate and requested. 27. Preserve audit and event logs as appropriate.
Corrective/Mitigation Action	28. Balance mission needs with recommended risk mitigation. 29. Own the restoration plan. 30. Coordinate with Network ISOs, PO, and staff to implement eradication and remediation actions. 31. Assure response actions are carried out by Local Area

TABLE 7	FACILITY CHIEF INFORMATION OFFICERS (FCIO)
Role	**Responsibilities**
	Network/Wide Area Network (LAN/WAN) managers. 32. Implement recommendations as appropriate. 33. Maintain a record of costs associated with repair, restoration, business disruption, and labor.
Lessons Learned	34. Participate with the facility incident response staff in a post mortem review of all documentation surrounding the incident/suspected incident. 35. Implement “best practices” as appropriate based on the review.

TABLE 8	PRIVACY OFFICERS (PO)
Role	**Responsibilities**
Incident Preparation	1. Take appropriate privacy and security training. 2. Obtain and maintain a PSETS account and develop familiarity with the system. 3. Review VA Handbook 6502.1, *Privacy Event Tracking*. 4. Review PSETS Basic User’s Handbook. 5. Maintain awareness of the privacy laws, regulations, and policies that affect their organizations. 6. Ensure that individuals within their organizations know who their POs are. 7. Acquire template of Incident Notification/Credit Monitoring letter. 8. Establish a working relationship with the ISO(s) for their organizations. 9. Ensure that facility privacy personnel have appropriate incident response mechanisms, such as phone numbers, email addresses, and tools available to report suspected privacy incidents. 10. Ensure an after-action report process in place to look at root causes and future prevention mechanisms.
Incident Prevention	11. Implement Departmental and appropriate Administration privacy policies and procedures. 12. Establish an internal privacy audit or compliance monitoring and audit program. 13. Monitor and report that individuals in their organizations complete the appropriate annual Privacy training(s). 14. Ensure that privacy issues and concerns are communicated to and coordinated with appropriate parties. 15. Become aware of the systems in their organizations that collect and/or maintain PHI and/or PII. 16. Participate in the preparation and updating of Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA) for

TABLE 8	PRIVACY OFFICERS (PO)
Role	**Responsibilities**
	systems within the purview of their organizations. 17. Understand what constitutes a Privacy Act system of records (SOR), and ensure that all PII that is retrieved by individuals' names or other unique identifiers are maintained in an official SOR published in the Federal Register. 18. Promote activities to foster privacy awareness (e.g., Privacy Day or Information Protection Awareness Week).
Incident Detection	19. Receive complaints from Veterans or anyone within their organization who believes an incident has occurred. 20. Enter all complaints received into the system allotted for the reporting of incidents within one (1) hour of discovery. 21. Follow guidance provided by the VA Privacy Service in order to record all incidents in PSETS. 22. Monitor all incidents that they have entered into PSETS. 23. Provide updates to PSETS, as appropriate.
Incident Documentation	24. Enter updates to PSETS, as necessary, for any incident with a status of "Open". 25. Track the progress of response activity via a PSETS ticket, if the event is determined to be a breach, and perform all necessary documentation of progress. 26. Enter updates into the reporting tools when prompted by reminders. If the ticket is in "pending" status, then an update is required after one week. 27. Review tickets at least every 72 hours for updates. 28. Immediately update the risk assessment with new information about the incident as soon as it becomes available.
Incident Notification	29. Notify and keep local management and support staff apprised of the incident. 30. Prepare Incident Notification/Credit Monitoring Letters for signature 31. Obtain Promo Codes for Credit Monitoring Letters when applicable
Containment Strategy	32. Participate in initiating containment actions. 33. Suggest alternate containment actions, as necessary.
Restoration	34. Ensure timely closure of incidents and complaints.
Evidence Gathering and Management	35. Execute direction provided by the Data Breach Response Service, VA-NSOC, law enforcement, and the OIG. 36. Begin fact-finding investigation once initial complaint is logged into PSETS. 37. Consult with law enforcement or the OIG as necessary. 38. Log all comments and details of their investigation into PSETS or

TABLE 8	PRIVACY OFFICERS (PO)
Role	**Responsibilities**
	the subsequent system designated for the reporting of privacy complaints and incidents.
Lessons Learned	39. Log resolution of incident. 40. Raise user awareness through lessons learned.

TABLE 9	INFORMATION SECURITY OFFICERS (ISO)
Role	**Responsibilities**
Incident Preparation	1. Obtain and maintain PSETS user accounts and obtain training in Remedy and Risk Assessment. 2. Complete appropriate privacy and security training. 3. Become aware of the security laws, regulations, and policies that apply to the organization. 4. Ensure that individuals within the organization know who their ISOs are. 5. Ensure that facility incident response personnel have appropriate incident response mechanisms, such as phone numbers, email addresses, and tools available to report suspected incidents. 6. Become familiar with and establish a working relationship with the PO, CIO, and OI&T staff for the organization. 7. Ensure that an after-action report process is in place to look at root causes and future prevention mechanisms. 8. Provide local organization policy and procedures for reporting and managing incidents.
Incident Prevention	9. Advise users on proper security protocols to prevent incidents. 10. Provide training to staff on their roles in preventing, reporting, and managing security incidents. 11. Ensure systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored and/or rebuilt. 12. Provide local organization policy and procedures for reporting and managing incidents. 13. Verify that all users complete the VA Privacy and Security Awareness and Rules of Behavior (ROB) training annually. 14. Verify that all users sign the VA National ROB annually.
Incident Detection	15. Initiate protective measures when an incident or vulnerability is discovered. 16. Ensure that incidents are properly reported, responses are coordinated, and incident updates are provided as required. 17. Coordinate with the PO to determine if a detected or reported security incident is also a privacy incident.

TABLE 9	INFORMATION SECURITY OFFICERS (ISO)
Role	**Responsibilities**
Incident Analysis	18. Enter all reported incidents into the PSETS within one (1) hour of receiving or identifying an incident. 19. Complete a risk evaluation at the time of reporting the incident and update information on each incident accordingly.
Incident Documentation	20. Enter updates to the system allotted for the reporting of privacy/security complaints or violations, as necessary, for any incident with a status of "Open". 21. ISOs and POs will also receive an email alert from the reporting tools reminding them to provide an update. If the ticket is in "pending" status, then an update is required after one week. 22. Tickets should be reviewed at least every 72 hours. The ISOs and POs should immediately update the risk assessment with new information about the incident as soon as it becomes available. 23. Track the progress of response activity via a PSETS ticket, if the event is determined to be a breach, and performing all necessary documentation of incident progress
Incident Notification	24. Notify and keep local management and support staff apprised of the incident.
Containment Strategy	25. Participate in initiating containment actions. 26. Suggest alternate containment actions, as necessary.
Evidence Gathering and Management	27. Execute direction provided by the Data Breach Response Service, VA NSOC, law enforcement, or the OIG. 28. Consult with law enforcement or the OIG as necessary. 29. Log all comments and details of their investigation into the PSETS or the system designated for the reporting of privacy complaints and incidents.
Lessons Learned	30. Log resolution of incident. 31. Raise user awareness through lessons learned.

TABLE 10	SUPERVISORS
Role	**Responsibilities**
Incident Preparation	1. Complete annual privacy and security training and ensure staff has completed all required training. 2. Sign the VA National ROB annually and ensure that staff has signed.
Incident Prevention	3. Comply with all directives and policies. 4. Provide an inventory of the affected software, documents, etc., with an operational impact assessment of the potential data compromise and to assist with investigations. 5. Ensure that all subordinates complete the required Privacy and Information Security Awareness and ROB training annually.

TABLE 10	SUPERVISORS
Role	**Responsibilities**
Incident Detection	6. Ensure that incidents are properly reported, responses are coordinated, and incident updates are provided as required.

TABLE 11	USERS OF VA INFORMATION AND INFORMATION SYSTEMS
Role	**Responsibilities**
Incident Preparation	1. Complete mandatory security training and privacy training on an annual basis. 2. Sign the VA National ROB annually.
Incident Prevention	3. Be alert to their surroundings and report any suspected incidents to their ISO, PO, and supervisor immediately. 4. Be vigilant in watching for unusual system behavior that may indicate a security incident in progress. 5. Comply with all directives and policies on the appropriate use and security of VA IT resources and information.
Incident Detection	6. Observe their physical surroundings and make sure that no SPI data is left unsecured. 7. Report any anomaly that they notice with their applications and computers to their ISO. 8. Report any suspicion of inappropriate privacy or security practices to the PO, ISO, and supervisor (and VA law enforcement as necessary). After normal business hours notify the VA-NSOC.

TABLE 12	PUBLIC AFFAIRS OFFICERS (PAOs)
Role	**Responsibilities**
Incident Notification	1. Work with facility POs to ensure that the press release and notification letters contain identical descriptions of the incident. 2. Prepare a news release, using a previous news release provided by the Data Breach Response Service as a sample, based on the DBCT template letter. 3. Send out the news release and arrange for the publication of the legal notice using appropriate media outlets. For those incidents requiring news releases, the news release will go out after the notification letters are sent. 4. Provide a copy of the news release to the local ISO, PO, General Counsel, Regional Counsel, and VA OIG (Office of Inspector General) . 5. For breaches requiring substitute notice, prepare a summary

TABLE 12	PUBLIC AFFAIRS OFFICERS (PAOs)
Role	**Responsibilities**
	write-up and submit it, along with the notice itself, to the VA website Webmaster for posting on the website for 90 days unless specified for a longer period by the local PAO. The local PAO will provide a copy of the summary write-up and the notice to the local ISO, PO, and Regional Counsel. For Department of Health and Human Services (HHS) reportable breaches: 1. Draft local releases to include all information the HIPAA Breach Notification Rule requires to be in individual letters of notification 2. Consider the prospect of having their regional OPIA staff as a resource. 3. Give draft release to facility PO, who will send it to OI&T's Data Breach Response Service. When the news release has been approved and sent out, give a copy to the facility PO and identify the media outlet(s), to which it was sent.
Incident Follow Up	1. When contacted by the news media, be prepared to say what the facility has done or is about to do to prevent a recurrence.

4. INCIDENT MANAGEMENT PROCESS

a. **Introduction**. Breach management is part of the overarching incident management process designed to mitigate risk. The incident management process contains four main areas:

(1) Incident Preparation;

(2) Incident Detection, Reporting, and Analysis;

(3) Corrective/Mitigation Action; and

(4) Post-Incident Activity.

b. **Incident Preparation**

(1) **Roles and Responsibilities.** Incident preparation begins with assigning roles and responsibilities across VA to manage incidents. Paragraph 3 above lists the VA organizational roles and responsibilities for managing incidents.

(2) **Incident Prevention.** Security and privacy policies and system security controls are the primary mechanisms for preventing and reducing the number of incidents and breaches. Office of Information Security (OIS) and Service Delivery and Engineering (SD&E) ensures that appropriate policies and controls exist to protect SPI and VA information systems using, storing and transmitting SPI.

c. **Incident Detection, Reporting, and Analysis.**

(1) Incident detection and reporting occurs either through technical detection or reporting of an incident. A user must immediately report to his/her VA supervisor, PO, and ISO any incident involving the possible compromise or loss of any VA sensitive information. The PO or ISO will promptly report the incident (within one (1) hour of notification) via the PSETS in accordance with the OI&T Incident Management procedures. *See* VA Handbook 6502.1, *Privacy Event Tracking*. After an incident has been detected and reported, the PO or ISO will investigate the privacy or security incident and provide feedback to the Data Breach Response Service. The Data Breach Response Service, through the DBCT, will determine based on the available facts whether a breach has occurred. If a breach has occurred, the DBCT will follow the breach management process and determine the level of risk and whether notifications and credit protection services are warranted.

(2) If the incident involves Federal Tax Information (FTI), VA personnel will follow the above VA reporting procedures and will: a) report suspected security incidents pertaining to FTI to the VA incident response resources upon discovery of the incident and b) contact the appropriate special agent-in-charge, the Treasury Inspector General for Tax Administration (TIGTA), the VA OIG (Office of Inspector General), and the IRS Office of Safeguards immediately, but no later than 24 hours after identification of a possible incident involving FTI. For further information, including contact information, VA personnel should see IRS Publication 1075.

d. **Corrective/Mitigation Action.** Depending on the results of the incident analysis, mitigation or corrective actions may include training employees on applicable policy and proper procedures, revising policy or procedures to prevent a recurrence, and providing notifications or credit protection services to individuals whose SPI was involved in a breach in accordance with VA policy and federal law. While engaging in these activities, VA officials will also collect evidence to support any potential legal proceedings if warranted.

e. **Post-Incident Activity.**

(1) Post-incident activity involves: a full incident review from beginning to end; evaluating how well staff and management responded; confirming that the incident is closed by addressing the incident in writing and providing closure; and using collected incident information to improve processes and retain evidence.

(2) For VA systems that retain FTI, post-incident activity includes that audit logs be maintained for seven years "to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements." IRS Publication 1075 (October 2014), Paragraph 9.3.3.11.

5. VA CRITERIA FOR BREACH AND RISK ASSESSMENT

a. **Introduction.** For purposes of simplifying and standardizing the breach management process, VA developed the VA breach criteria for defining a breach that must be reviewed for notification and credit protection services and the VA standard risk assessment criteria for determining when the risk of compromise is so low that notification and credit reporting are not warranted. The below paragraphs discuss these criteria in more detail.

b. **Breach Criteria**

(1) The VA Data Breach Response Service uses the VA breach criteria in determining whether the reported event constitutes a breach that must be reviewed to decide whether VA should notify the record subjects of the event and offer them credit protection services.

(2) For purposes of the VA breach criteria and determining whether the reported event constitutes a breach that must be reviewed for determination of notification and credit protection services, the term "breach" means the acquisition, access, use, or disclosure of VA SPI, including PII and PHI, in a manner not permitted by law or VA policy which compromises the security or privacy of the SPI.

(a) Under 38 U.S.C. § 5727(4), a "data breach" is "the loss, theft, or unauthorized access, other than those incidental to the scope of employment, to data containing SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data."

(b) With respect to PHI maintained by VHA or its BAs, a "breach" is "the acquisition, access, use, or disclosure of [PHI] in a manner not permitted [by the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI]."

(3) Breach excludes:

(a) Any unintentional acquisition, access, or use of SPI by a workforce member (i.e., VA employee, without compensation employee, VA volunteer, student, trainee) or person acting under the authority of VA or its contractors or other agents (e.g., BAs), if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in the further use or disclosure in a manner not permitted by law or VA policy.

(b) Any inadvertent disclosure by a person who is authorized to access SPI at VA to another person authorized to access SPI at VA or its contractors or other agents, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by VA policy.

(c) A disclosure of SPI where VA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(d) An acquisition, access, use, or disclosure of SPI where VA demonstrates that there is a low probability the SPI has been compromised based on a risk assessment outlined in Paragraph 5.c below.

(4) The VA breach criteria also considers and incorporates the breach definitions of the following authorities, which use slightly different phrasing, but generally refer to unauthorized access to SPI that results in the potential compromise of the confidentiality or integrity of the information.

(a) OMB M-07-16, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*" (May 22, 2007), footnote 5 states, "the term 'breach' is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic." The Memorandum specifically states that a breach occurs when: "An individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred."

(b) The HITECH ACT defines a breach as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an authorized person to whom such information is disclosed would not have reasonably have been able to retain such information." 42 U.S.C. § 17921(1).

(5) The term "data breach" appears in this document only when quoting from specific statutes where this term is used.

c. **Risk Assessment**

(1) Except for breach exclusion under paragraph 5.b.(3) above, an acquisition, access, use, or disclosure of SPI is presumed to be a breach, unless VA demonstrates there is a low

probability the SPI has been compromised based on a risk assessment of factors including the following:

(a) The nature and extent of the SPI involved, including the types of identifiers and likelihood of re-identification;

(b) The unauthorized person who acquired, accessed, or used the SPI, or to whom the disclosure was made;

(c) Whether the SPI was actually acquired or viewed; and

(d) The extent to which the risk to the PHI has been mitigated. This is mitigation of the risk to the SPI for the specific ticket and does not encompass every mitigation activity by the agency to prevent this type of incident in the future.

(2) If VA is unable to determine the level of probability the SPI has been compromised based on the risk assessment of the above four factors, the following additional factors should be considered:

(a) The amount of time for which the SPI was out of VA control or unsecured;

(b) Whether the SPI was eventually recovered and secured, or remains missing;

(c) Ease of logical access to the SPI in light of the degree of protection for the data (e.g., unencrypted, plain text);

(d) Ease of physical access to the SPI (e.g., in a publicly accessible area);

(e) Indication that the SPI was the target of, rather than incidental to, unlawful acquisition; and

(f) Whether the credit protection services may assist the individuals in avoiding or mitigating any harm resulting from the breach.

(3) Compromise means made accessible to and usable by unauthorized persons. 38 C.F.R. § 75.115 (b)(7)

(4) VA uses the facts of the incidents described in the below matrices (see Paragraph 7.b) to describe the VA standard risk assessment criteria. If the facts of the incident described in the matrices describe a low risk of compromise, then they fall within the criteria of the standard risk assessments, and there is no breach. As a result, there is no notification or credit protection required, and reporting to HHS for breaches involving PHI is not required.

(5) If the facts fall outside the criteria of the standard risk assessments then a complete/full risk assessment to determine if a breach has occurred is required. The Data Breach Response Service will perform the complete/full risk assessment for all tickets when required. The Data Breach Response Service will determine which complete/full risk assessments need to be provided to the DBCT based on the scoring results in order for the DBCT to make a decision on whether or not there is a low probability of risk of compromise of the SPI.

6. BREACH MANAGEMENT OVERSIGHT STRUCTURE

a. The Data Breach Response Service provides the necessary oversight to ensure that VA promptly identifies and responds appropriately to breaches involving VA SPI, and includes the DBCT in breach response activities as necessary.

b. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, describes the responsibilities of VA senior officials, information owners, and information system users in VA incident management. In addition, this Handbook contains the list of VA organizational roles and responsibilities for managing breaches. Figure 1 illustrates the DBCT organization.

Data Breach Core Team
OI&T
Director, Data Breach Response Service – CHAIR Director, OI&T Privacy Service Director, Field Security Service Data Breach Response Service staff members
Business Partners
Director, Health Care Security Requirement Office of General Counsel (4 members) Office of Congressional Affairs Office of Public and Intergovernmental Affairs OI&T Privacy Service (2 members) Veterans Health Administration Privacy Officer Veterans Benefit Administration Privacy Officer Board of Veterans' Appeals (2 members) Consolidated Mail Outpatient Pharmacy VHA 10N Watch Officer (2 member) Human Resource Information Service Office of Acquisition and Logistics National Cemetery Administration

Figure 1: DBCT Organization

7. BREACH MANAGEMENT PROCESS

a. Overview

(1) Laws, policies, and other authorities establish clear and proper procedures for deterring and responding to breaches. VA Information Security statutes require that "[i]f the Secretary determines, based on the findings of a risk analysis, that a reasonable risk exists for the potential misuse of SPI involved in a data breach, the Secretary shall provide credit protection services in accordance with the regulations prescribed by the Secretary under this section." 38 U.S.C. § 5724(a)(2).

(2) As required by § 5724(b), the Secretary prescribed regulations, 38 C.F.R. §§ 75.111 to 75.119, for the provision of the following credit protection services after the Secretary determines that there is at least a reasonable risk of potential misuse of SPI involved in a breach:

(a) Notification

(b) Data mining

(c) Fraud alerts

(d) Breach analysis

(e) Credit monitoring

(f) Identity theft insurance

(g) Credit protection services

NOTE: The decision to provide credit monitoring following a particular breach does not indicate that VA has determined that a reasonable risk exists for the potential misuse of SPI involved in the incident. In the event of a breach, VA may, as a matter of discretion, provide credit protection services even when it is not legally required because the level of risk is lower than reasonable.

(3) In compliance with these authorities, the DBCT breach management process includes the following main areas illustrated in Figure 2 and explained in detail below:

(a) Breach Detection, Reporting, and Analysis

(b) Corrective/Mitigation Action

(c) Post-Breach Activity

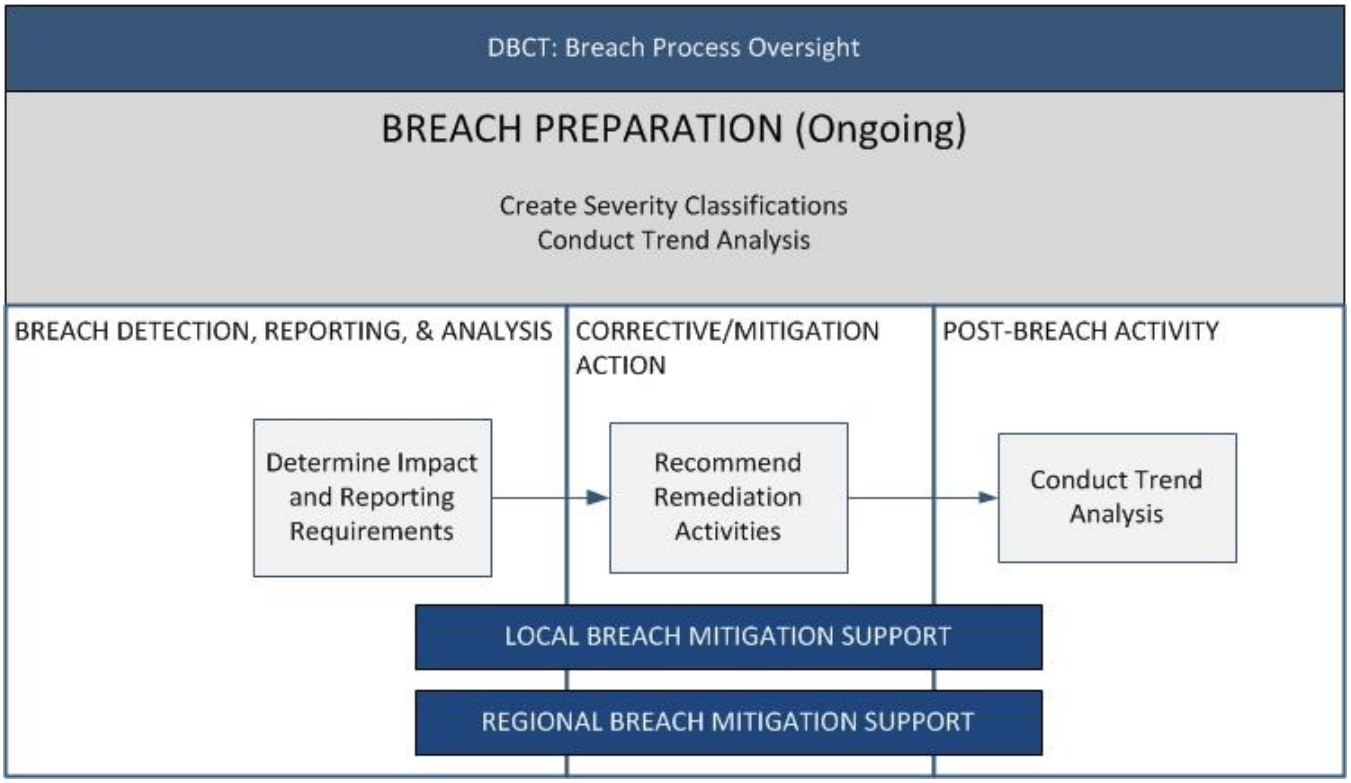

Figure 2: DBCT Breach Incident Process Oversight

b. **Breach Detection, Reporting, and Analysis**

(1) **Overview.** All suspected incidents and breaches should be entered into the PSETS database by local ISOs and POs upon detection. This database is managed by the VA Office of Privacy and Records Management (OPRM) (005R1). The VA breach management process continues with local ISOs and POs who determine whether a breach has actually occurred and complete the local risk assessment. After these steps are completed, the facility-level Data Breach Response Service, in collaboration with the DBCTs at the local, regional, and national levels, will conduct further analysis as necessary and manage the response to the breach.

(2) **Breach Determination and Risk Assessment Guidance**

(a) **Applying the Standard Risk Assessment Matrices.** The following matrices include columns that describe incidents and indicate if a breach has occurred and will be reported to HHS under the HIPAA Breach Notification Rule. If the answer in the "Breach Occurred" column is "No," the facts of the incident fall within the standard risk assessment criteria, and there is no breach because the risk of compromise is deemed low (see Paragraph 5.c above for an explanation of risk assessment and exceptions to a breach based on a low probability the SPI has been compromised). If a breach has not occurred, VA will not provide notification or credit protection and will not report the incident to HHS. If the answer in the "Breach Occurred" column is "Yes", then the facts describe an incident outside of the standard risk assessment criteria, and the Data Breach Response Service must perform a complete/full risk assessment. In this case, VA will have to report a breach to HHS if PHI is involved. A few of the incidents described in the matrices require further facts to determine if the incidents meet the standard risk assessment criteria and are not a breach. For these incidents, the "Breach Occurred" and "HIPAA Breach Reporting" columns refer to the paragraphs below the matrix, which give additional facts needed to determine that the incidents are not a breach. If these additional facts apply to the incident, then the incident falls within the standard breach assessment criteria and, therefore, is not a breach and will not be reported to HHS. If the additional facts do not apply to the incident, then the Data Breach Response Services must perform a complete/full risk assessment (see Paragraph 7.b.(2)(h)).

(b). **Mis-Mailing**

1. The mis-mailing category consists of all hard-copy materials sent through a mail carrier (e.g., United States Postal Service (USPS), commercial carrier), or hand-carried either inside or outside a VA facility. Mailing of SPI includes prescriptions sent by a Consolidated Mail Outpatient Pharmacy (CMOP), correspondence to or from VA components (e.g., VBA or VHA), about an individual's VA benefits or medical care, and other day-to-day business communications that VA conducts that may contain SPI, and is subject to Directive 6609, *Mailing of Sensitive Personal Information*. The mis-mailing category includes incidents in which the communication is delivered to the incorrect address or is damaged en route such that someone other than the intended recipient or sender may view SPI. The category also includes one type of electronic communication: sending SPI by fax.

2. In each category, the hard-copy material containing SPI is sent in a sealed container (e.g., an envelope that prevents any one from seeing the contents of the container until it is opened or its physical integrity is breached). If hard-copy material containing SPI is sent in an unsealed container, the mailing is a breach without any further intervention.

Matrix 1: Breach Determination for SPI Contained on Compromised Hard Copy Format Sent Through a Third Party Carrier.		
Hard-Copy Mail Event	**Breach Occurred**	**HIPAA Breach Reporting – PHI Only**
VA container (e.g., envelope or package, containing SPI sent to incorrect address): Returned sealed and unopened to VA	No [Excluded]	No
VA container containing SPI sent to incorrect address: HIPAA CE (e.g., health care provider) or other federal agency, regardless of whether returned to VA or not	Refer to Para. 7.b.(2)(b)3.a.	Refer to Para. 7.b.(2)(b)3.a.
VA container containing SPI sent to incorrect address: Opened by third party (i.e., anyone other than the intended recipient or VA personnel), regardless of whether returned to VA or not	Yes	Yes for PHI
Damaged container - SPI Content Exposed to VA workforce (e.g., mailed within VA)	No [Excluded]	No
Damaged container - SPI Content Potentially Exposed to Third Party	Refer to Para. 7.b.(2)(b)3.b.	Refer to Para. 7.b.(2)(b)3.b.
VA container or content lost or damaged en route – no SPI or PHI	No	No
VA container with SPI content lost en route by mail carrier – Name and home address only on label or outside of container	No	No
VA container with SPI content lost in route by mail carrier – Name, home address and SSN, date of birth (DOB), or other unique identifier on label or outside of container	Yes	Yes for PHI
SPI faxed to wrong location within VA by mistake	No [Excluded]	No
SPI faxed to wrong location outside of VA (e.g., to public fax, another CE, another federal agency)	Refer to Para. 7.b.(2)(b)3.c..	Refer to Para. 7.b.(2)(b)3.c.

3. With respect to certain incidents referenced in the matrix above, an event is not a breach if it involves only the disclosure of:

a. (i) any SPI; (ii) to a HIPAA CE or other federal agency; (iii) where the SPI was viewed; and (iv) the recipient returned the envelope or package to VA with all of the contents intact.

b. (i) any SPI; (ii) exposed to USPS or other mail carrier staff only; (iii) where the SPI was not acquired, but may have been viewed by mail carrier staff during the performance of their official duties; and (iv) the envelope or package was delivered to appropriate recipient with all content intact.

c. (i) any SPI; (ii) to HIPAA CE or other federal agency; (iii) where the SPI was viewed; and (iv) the recipient destroyed the fax and certified such destruction in writing.

4. Refer to Paragraph 7.b.(2)(h) for further explanation of the standard breach risk assessment criteria and instructions on when a complete/full risk assessment is needed.

(c) **Mis-Handling**

1. It is the policy of VA to handle documents that contain SPI in a secure manner so that the information is not improperly exposed. Such documents may include prescriptions, logs, health records, billing/financial documents, employee/staff sensitive information, and other day-to-day sensitive business communications containing VA SPI.

2. There are incidents in which the SPI is found unexposed, such as in an unopened envelope or box, or in a location where any access in violation of any of the applicable confidentiality provisions is unlikely. By contrast, the SPI could have been exposed, such as a document or chart which is not covered or hidden in any manner, found in a location where access in violation of any of the applicable confidentiality provisions could have occurred, including inappropriate locations within the VA facility or on the VA facility grounds, such as a VA parking garage, or outside of the VA facility or grounds (e.g., subway cars and restaurants).

Matrix 2: Breach Determination for SPI Contained on Storage Media That Are Mishandled by VA		
Storage Media Contents	**Breach Occurred**	**HIPAA Breach Reporting – PHI Only**
Readable SPI contents exposed only to VA workforce member (e.g., employees, contractors, volunteers, students, etc.)	No [Excluded]	No
Readable contents not exposed	No	No
Readable SPI content exposed to a Veteran (e.g., paperwork of a Veteran handed to another Veteran) and the Veteran leaves the facility with the SPI	Yes	Yes for PHI
Readable SPI content exposed to a Veteran briefly within the facility and handed back to VA employee	No [Excluded]	No
Readable SPI content correctly provided to a Veteran, and Veteran leaves SPI unsecured at facility	No [Not VA]	No
Readable SPI contents exposed to anyone else	Refer to Para. 7.b.(2)(c)3.	Refer to Para. 7.b.(2)(c)3.
Readable SPI content lost and exposure undeterminable	Yes	Yes for PHI

3. With respect to the incident referenced in the matrix above, an event is not a breach if it involves only the disclosure of: (i) any SPI; (ii) to a HIPAA CE or other federal agency; (iii) where the SPI was viewed; and (iv) the recipient returned the SPI to VA or appropriately destroyed the SPI.

4. Refer to Paragraph 7.b.(2)(h) for further explanation of the standard breach risk assessment criteria and instructions on when a complete/full risk assessment is needed.

(d) **Equipment**

1. It is VA policy that VA facilities, contractors, and BAs will immediately report upon discovery all lost, stolen, or missing IT equipment that may be used to store, transmit, create, access, duplicate or copy, disclose or use SPI, whether it is encrypted or unencrypted. Examples of covered IT equipment include laptops, workstations, thumb drives, hard drives, routers, Universal Serial Bus (USB) device, Personal Digital Assistant (PDA), smart phones, Blackberry device, tablets, and other similar devices. VA must report this unaccounted for, stolen, or missing equipment to Congress if the storage capability on the equipment was not encrypted with an encryption application approved by the Office of Cyber Security (OCS), even if VA determines that the devices do not contain SPI. Even if not reportable to Congress, all missing equipment is reportable to the US-CERT and VA upper management.

2. Unaccounted for equipment is IT equipment that the facility lists on its inventory that has not been assigned to a specific employee or location and cannot be located but where there is no indication that it was stolen.

3. Stolen equipment is equipment VA has determined was stolen based on the available evidence (e.g., a laptop is missing from an employee's locked car and there is evidence someone broke into the car, a laptop stolen from a treatment unit after cutting the tether to the storage cart; or a hard drive is removed from a work station). There should be affirmative evidence that would lead a reasonable person to conclude someone intentionally took the equipment or the container for the equipment (e.g., someone steals an employee's car containing a laptop, and the laptop is not in the car when it is recovered).

4. Missing equipment is equipment that is assigned to a specific employee or location, and the equipment is lost or misplaced (e.g., an employee puts a laptop on top his/her car and drives off).

Matrix 3: Breach Determination for Unaccounted for, Missing or Stolen Equipment and SPI		
Equipment Contents	**Breach Occurred**	**HIPAA Breach Reporting – PHI Only**
Unaccounted for, stolen, or missing equipment that does not contain SPI	No	No
Unaccounted for, stolen, or missing equipment that contains encrypted SPI or encrypted PHI	No [Excluded]	No
Unaccounted for, stolen, or missing equipment with SPI not encrypted	Yes	Yes for PHI
Unaccounted for, stolen, or missing equipment that is not encrypted and contains SPI that is a Limited Data Set (LDS) only as defined by the HIPAA Privacy Rule	Refer to Para 7.b.(2)(d)5.	Refer to Para 7.b.(2)(d)5.
Unaccounted for, stolen, or missing equipment that is not encrypted and contains any other SPI	Yes	Yes for PHI

5. With respect to the incident referenced in the matrix, an event is not a breach if it involves only the disclosure of: (i) an LDS as defined by the HIPAA Privacy Rule (i.e., no unique or patient identifier); (ii) where it is unknown whether the equipment containing the SPI was lost or stolen; (iii) where it is unknown whether SPI was acquired or viewed; and (iv) police have been notified and the risk to the SPI being re-identified is low due to the nature of an LDS.

6. Refer to Paragraph 7.b.(2)(h) for further explanation of the standard breach risk assessment criteria and instructions on when a complete/full risk assessment is needed.

(e) **Email:** Email containing VA SPI must be encrypted with an encryption application certified by the National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS) 140-2 compliant and approved by OCS, unless a written risk-based decision memorandum from the VA CIO is in place that justifies and memorializes the decision not to encrypt the email. VA has identified specific encryption applications that must be used with VA data. Email sent or received by a VA source that contains SPI that is not encrypted with a FIPS 140-2-compliant encryption application is treated in this Handbook as unencrypted email.

Matrix 4: Breach Determination for SPI Contained in Compromised Emails		
Email Contents	**Breach Occurred**	**HIPAA Breach Reporting – PHI Only**
Email with no SPI	No	No
Encrypted email containing SPI sent inside or outside VA to wrong party	No [Excluded]	No
Unencrypted email containing SPI sent to VA workforce member (e.g., employees, contractors, volunteers, students, etc.) inside VA Network	No [Excluded]	No
Unencrypted email containing SPI sent to the intended recipient, who is a Trusted Entity(e.g., Veterans Service Organizations (VSOs)) inside VA network	No [Excluded]	No
Unencrypted email containing SPI sent to intended Veteran, patient, or his/her personal representative outside VA Network	No [Right of Access]	No
Unencrypted email containing SPI sent to anyone other than a VA workforce member or intended Veteran, patient, or his/her personal representative outside VA	Refer to Para. 7.b.(2)(e)1.	Refer to Para. 7.b.(2)(e)1.

1. With respect to the incident referenced in the matrix above, an event is not a breach if it involves only the disclosure of: (i) any SPI including name, SSN, or other unique identifiers; (ii) to another HIPAA CE, another federal agency, or other entity with whom VA has a formal agreement, such as a Data Use Agreement; (iii) the SPI was acquired regardless of whether the SPI was viewed; and (iv) the recipient was the intended party and had legal authority to receive the SPI, or, if the recipient was not the intended recipient and inappropriately received the SPI, the email was promptly deleted .

2. Refer to Paragraph 7.b.(2)(h) for further explanation of the standard breach risk assessment criteria and instructions on when a complete/full risk assessment is needed.

(f) **Unauthorized Access:** Unauthorized access to SPI is access to SPI in violation of any of the applicable confidentiality statutes. Such access may include:

1. Access to SPI by an unauthorized user (i.e., has not met the requirements to access the data, such as no background investigation, if required).

2. Access to SPI by someone who has met all requirements to access the data, but accesses SPI for an unauthorized purpose (i.e., curiosity, malice).

Matrix 5: Breach Determination for Unauthorized Access to SPI or Access for an Unauthorized Purpose		
Unauthorized Access/Purpose	**Breach Occurred**	**HIPAA Breach Reporting – PHI Only**
SPI accessed by VA workforce member (e.g., employees, subcontractors, volunteers, students) without authority or permission, and investigation reveals an intent to access in violation of policy (e.g., curiosity, malice).	Yes	Yes for PHI
SPI accessed by VA workforce member (e.g., employees, contractors, volunteers, students) unintentionally or accidentally (e.g., in error)	No [Excluded]	No
SPI accessed by a Trusted Entity (e.g., VSO) without authority or permission, and investigation reveals an intent to access in violation of policy (e.g., curiosity, malice)	Yes	Yes for PHI
SPI on another Veteran accessed electronically by a Veteran through his VA issued account (e.g., My HealtheVet, eBenefits) due to a technical issue	Refer to 7.b.(2)(f)3.a.	Refer to 7.b.(2)(f)3.a.
SPI accessed electronically by any third party (e.g., non-VA personnel)	Refer to 7.b.(2)(f)3.b.	Refer to 7.b.(2)(f)3.b.

3. With respect to certain incidents referenced in the matrix above, an event is not a breach if it involves only the disclosure of:

a. (i) SPI that does not include unique identifiers (e.g., name, SSN) of a Veteran; (ii) to another Veteran through only his/her VA issued account; (iii) where the SPI was acquired and was or may have been viewed; and (iv) VA removed the first Veteran's information from the second Veteran's account or system and received confirmation from the second Veteran that the information was not downloaded through Blue Button or other program.

b. (i) Any SPI; (ii) to another HIPAA CE, federal agency, or other entity with whom VA has a formal agreement, such as a Data Use Agreement; (iii) where the SPI was acquired and may have been or was viewed; and (iv) the recipient confirms no SPI was stored or retained on IT system.

4. If SPI is exposed to possible unauthorized access or misuse but VA cannot determine unauthorized access to or misuse of the SPI, a complete/full risk assessment is required under Paragraph 7.b.(2)(h).

5. Refer to Paragraph 7.b.(2)(h) for explanation of the standard breach risk assessment criteria and instructions on when a complete/full risk assessment is needed.

(g) **Improper Disposal**

1. Improper disposal covers those situations in which storage media containing SPI are compromised at any time between release by a VA office or Trusted Entity, and the ultimate destruction of the storage media or rendering of the SPI on the storage media permanently inaccessible. This category would cover paper records containing SPI in a dumpster located behind a Community Based Outpatient Clinic (CBOC), including CBOCs on leased property, or a hard drive containing SPI on excessed VA computer equipment.

2. SPI is considered compromised whenever the information was made available in a readable or usable form (e.g., unencrypted electronic data) to unauthorized individuals (i.e., not authorized to see the SPI), whether employees or not, and to individuals who may be authorized to see the SPI for some purpose, but do so for a different purpose.

Matrix 6: SPI Compromised During Disposition in Violation of VA Disposal Requirements		
Unauthorized disposal procedure	**Breach Occurred**	**HIPAA Breach Reporting – PHI Only**
Encrypted SPI on storage media improperly disposed (i.e., in violation of policy)	No	No
Readable SPI accessible only by VA workforce members (e.g., employees, contractors, volunteers, students, etc.) or Trusted Entity employees (e.g., HIPAA CE, BA)	No [Excluded]	No
Storage media or paper with readable SPI accessible by any third party	Refer to 7.b.(2)(g)3.	Refer to 7.b.(2)(g)3.
Readable SPI, such as paper, left unattended on VA property but sealed and secured in a manner that no SPI was actually acquired, accessed, or disclosed	No	No

3. With respect to the incident referenced in the matrix above, an event is not a breach if it involves only the disclosure of: (i) any SPI; (ii) recovered by a HIPAA CE, federal agency, other entity with whom VA has a formal agreement, such as a Data Use Agreement, or law enforcement; (iii) where the SPI was or may have been viewed; and (iv) there is no indication that any SPI was removed or accessed from the storage media.

4. Refer to Paragraph 7.b.(2)(h) for further explanation of the standard breach risk assessment criteria and instructions on when a complete/full risk assessment is needed.

(h) **Complete/Full Risk Assessment**

1. If the facts of the incident described in the above matrices fall within the standard risk assessment criteria, then there is no breach since the risk of compromise is deemed low. As a result, there will be no notification or credit protection for the record subjects or, for breaches involving PHI, reporting to HHS.

2. If the facts fall outside of the standard risk assessment criteria, then a complete/full risk assessment is required to determine if a breach has occurred.

3. The Data Breach Response Service will perform a complete/full risk assessment on incident tickets involving SPI when required.

4. The Data Breach Response Service will determine which complete/full risk assessments need to be provided to the DBCT based on the scoring results. The DBCT will determine whether there is a low probability of risk of compromise of the involved SPI.

5. If, upon review of the available information, the DBCT finds that more information is necessary to determine if there is more than a low probability of risk of compromise to the SPI of the record subjects, the DBCT may ask the involved VA personnel to provide additional information as the DBCT determines necessary to make the decision in that case in a timely manner.

(i) **Notification Determination for Breaches**

1. If the incident is not determined to be a breach based on the definition and exclusions or the risk assessment process, no notification or credit monitoring will be provided.

2. If the incident is determined to be a breach, notification or credit monitoring may be warranted and should be provided, if appropriate, as outlined in Matrix 7. In addition, reporting to HHS will be required for breaches involving PHI.

3. A “yes” answer in the “notification warranted” column or credit protection warranted column means that the responsible VA entity must notify the record subject of the breach and/or provide credit protection, if the Data Breach Response Service or the DBCT so determines. When a breach involves PHI, the notification letter must meet the requirements of the HIPAA Breach Notification Rule.

4. If the record subject is a deceased Veteran and the answer in the “notification warranted” column is “yes”, VA will send a next-of-kin letter to the next-of-kin of record. An offer of credit

protection services will not be sent to individuals who are next-of-kin of a deceased Veteran unless the data of the next-of-kin was involved in breach or the deceased individual's SPI involved in the breach could be used to harm the next-of-kin.

Matrix 7: Notification or Credit Protection Services for Specific Data Elements Involved in Any Type of Breach		
Type of Information Exposed	**Notification Only Warranted**	**Credit Protection Warranted**
Full Name only	No	No
Full Name with other SPI	Yes for PHI Only	No
Full Name and DOB	No	Yes
Full Name and Home Address	Yes	No
Full Name and Email Address	No	No
Full SSN	No	Yes
Full Name and Partial SSN	Yes	No
Full Name and PHI, including account numbers or disability codes	Yes	No
Partial SSN only	No	No
Partial SSN with other SPI	Yes for PHI Only	No
Other PII	To be determined by DBCT	To be determined by DBCT

(3) **Local and Regional Levels.** At the local and regional/VISN levels, mitigation teams may convene any time there is a breach. The chair of the meeting oversees discussion of the breach, based upon the information entered in the PSETS database, and charters direct action to mitigate the breach at the local or regional level, in coordination with all appropriate entities. Incidents that are confirmed at the local and regional level are followed by an Incident Brief, which is attached to the PSETS ticket.

(4) **Data Breach Response Service.** The Data Breach Response Service reviews the entries in the PSETS database daily, evaluates them for clarity and internal consistency, and determines whether or not further action is required. Further action may include breach notification, credit monitoring, or referral to the DBCT for additional analysis.

(5) **Local ISOs and POs.** Local ISOs and/or POs take all action required locally and as directed by the Data Breach Response Service or the DBCT to bring the incident or breach to resolution and must update the PSETS ticket accordingly.

(6) **Independent Risk Analysis (IRA) Requirement**. The Data Breach Response Service reviews each breach to determine if an IRA by VA OIG or a non-VA entity is necessary per 38 U.S.C. § 5724(a).

(a) **Accelerated Response**. Pursuant to 38 C.F.R. § 75.114, VA may, as a matter of discretion, provide an Accelerated Response to a breach by offering notification and credit protection service without an IRA if it determines that there is an “immediate, substantial risk of identity theft of the individuals whose data was the subject of the breach” upon consideration of the following factors:

1. The nature and content of the lost, stolen or improperly accessed data (e.g., the data elements involved, such as name, SSN, DOB);

2. The ability of an unauthorized party to use the lost, stolen, or improperly accessed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects, if able to access and use the data;

3. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data (e.g., unencrypted, plain text);

4. Ease of physical access to the lost, stolen or improperly accessed data (e.g., the degree to which the data is readily available to unauthorized access, such as being in a dumpster readily accessible by members of the general public);

5. The format of the lost, stolen or improperly accessed data (e.g., in a standard electronic format, such as American Standard Code for Information Interchange (ASCII), or on paper);

6. Evidence indicating that the lost, stolen or improperly accessed data may have been the target of unlawful acquisition; and

7. Evidence that the same or similar data had been acquired from other sources improperly and used for identity theft.

NOTE: The decision to provide an Accelerated Response following a particular breach does not indicate that VA has determined that an “immediate, substantial risk of identity theft” or even a “reasonable risk” exists for the potential misuse of SPI involved in the incident. In the event of a breach, VA may, as a matter of discretion, provide an Accelerated Response even in the absence of any of the above-described factors or a finding of reasonable risk.

(b) **IRA and Notification**. If a prior IRA conducted for VA on a similar incident concluded that notification and credit protection services should be offered, VA may rely on those findings to determine that such services are warranted for another breach.

(c) **Substitute IRA.** VA may also rely on the results of a prior risk assessment on a similar incident to conclude that notification and credit protection services are not warranted in a particular breach.

(d) **Independent Source Requirement**. When an IRA is required, the Data Breach Response Service will obtain an IRA from a non-VA entity (e.g., a non-VA entity, or VA OIG), pursuant to 38 U.S.C. § 5724(a)).

c. **Corrective/Mitigation Action**

(1) **General Communication Procedures**

(a) **Obtaining Contact Information**

1. It is the responsibility of local sites, through the PO, to contact the record subjects when required and to report out when completed. Contact information for individuals may be found in the applicable system of records and should not be requested of the next-of-kin.

2. VA maintains accurate and up-to-date contact information. There is not a single VA repository, but rather, each Administration maintains a distinct repository. The information is gathered when an individual registers for healthcare or Veterans’ benefits. Homeless Veterans provide contact information of a relative or another who is able to contact them. Each Administration utilizes their primary applications as their repository for contact information.

a. VBA uses SHARE, and the contact information is cross-referenced with the Social Security and/or Compensation and Pension Records Interchange (CAPRI) databases for accuracy. In some cases, the Veteran's banking institution may be contacted to validate current address information.

b. The National Cemetery Administration (NCA) collects information to record the burial for historic purposes and provide eligibility for spouse’s burial. The name and address of the next-of-kin are collected to facilitate any follow-up with the family that might be necessary. The contact information is kept in readable format and is retrievable from the Burial Operations Support System (BOSS)/Automated Monument Application System (AMAS).

c. VHA uses their applications, such as Computerized Patient Record System (CPRS), for obtaining, storing, and maintaining Veterans’ contact information. The information is verified each time a Veteran receives services from VHA.

3. In those instances where there is insufficient or out-of-date contact information that prevents direct written notification to an individual, a substitute form of notice may be provided. This substitute notice may be either a conspicuous posting on the home page of VA's web site or notification in major print and broadcast media in the geographic areas where the record subjects likely reside. Such a notice must include a toll-free phone number where an individual can learn whether or not his/her personal information might have been involved in the data breach. See 38 C.F.R. § 75.117(b) and 45 C.F.R. § 164.404(d)(2).

(b) **External Communications**

1. **Communicating with Individuals.** Communication with individuals whose SPI was involved in a breach is an important process. It is critical that the information that is sent to these individuals be both timely and accurate. This communication typically takes the form of either a notification letter or a letter offering credit protection services paid for by VA, prepared by the PO, or a person designated by the Facility's Director to serve as the PO, with guidance from the Data Breach Response Service (See Paragraphs 7.c.(2)-(4) in this Handbook for more information on breach notification letters and credit protection services).

2. **Communicating with Congress**. All communication with Congress must take place through OCLA.

3. **Communicating with the General Public**

a. In accordance with the HIPAA Breach Notification Rule, and to achieve greater transparency, several breach reporting measures have been adopted for incidents involving PHI maintained by VHA to complement existing procedures.

b. The three most recent monthly and quarterly breach reports to Congress are posted on a publicly accessible website, located at http://www.va.gov/about_va/va_notices.asp.

c. A toll-free phone number will be established for breaches potentially involving more than 500 individuals. The number will be activated and posted, along with notification to the media as required by the HIPAA Breach Notification Rule, on the VA Notices web page at http://www.va.gov/about_va/va_notices.asp, so that individuals can call to ask questions about the incident.

d. Media communications with the public concerning breaches must be coordinated through the associated VA OPIA. VA personnel should not speak directly to members of the press about any breaches but refer all inquiries to OPIA.

(2) **Notification**

(a) The Data Breach Response Service uses PSETS to make preliminary assessments of incidents. The Data Breach Response Service will review each breach report, in collaboration with the DBCT if necessary, and make a categorization determination using the criteria in the appropriate breach determination matrix, which are provided in Paragraph 7.b of this Handbook. The result will be a report that will be used to identify appropriate response activities and determine if notification is required.

(b) 38 C.F.R. §§ 75.114-118 specify the factors that should be addressed in an IRA and the factors that shall be considered when considering notification to record subjects. In determining whether the breach resulted in a reasonable risk for the potential misuse of the compromised SPI, all the factors relevant to the decision will be considered, including:

1. The likelihood that the SPI will be or has been made accessible to and usable by unauthorized persons;

2. Known misuses, if any, of the same or similar SPI;

3. Any assessment of the potential harm to the affected individuals provided in the risk analysis;

4. Whether the credit protection services that VA may offer under 38 U.S.C. § 5724 may assist record subjects in avoiding or mitigating the results of identity theft based on the VA SPI that had been compromised;

5. Whether private entities are required under federal law to offer credit protection services to individuals if the same or similar data of the private entities had been similarly compromised; and

6. The recommendations, if any, concerning the offer of, or benefits to be derived from, credit protection services in this case that are in the risk analysis report.

(c) Contents of the notification, pursuant to 38 C.F.R. § 75.117, should include:

1. A brief description of what happened, including the date(s) of the breach and of its discovery;

2. To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, SSN, DOB, home address, account number, disability code);

3. A statement as to whether the information was encrypted or protected by other means and when determined, such information would be beneficial and would not compromise the security of the system;

4. What steps individuals should take to protect themselves from potential harm, if any;

5. A brief description of what VA is doing, if anything, to investigate the breach, mitigate losses, and protect against any further breaches;

6. Contact procedures for those wishing to ask questions or learn additional information, including:

a. A toll-free telephone number, an email address, web site, and/or postal address; and

b. Steps individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts (alerts of any key changes to such reports and on demand personal access to credit reports and scores), if appropriate, and instructions for obtaining other credit protection services offered by VA.

(d) If notification is required, the Data Breach Response Service, in collaboration with the DBCT if necessary, determines the content of the notification and the method of delivery pursuant to 38 C.F.R. § 75.117. (See also Paragraphs 8-12 on the VA Process for compliance with HITECH and the HIPAA Breach Notification Rule.)

(e) The HIPAA Breach Notification Rule requires notification of a breach when an incident involves:

1. A disclosure of PHI;

2. In a manner not permitted by the HIPAA Privacy Rule;

3. Which compromises the security or privacy of the PHI; and

4. Does not consist of any of the following:

a. Any unintentional acquisition, access, or use of PHI by a workforce member or agent of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule;

b. Any inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, and the information received is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule; or

c. A disclosure of PHI where a CE or BA has a good faith belief that an authorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(f) Where an incident involving PHI meets the HIPAA definition of a breach, VA must notify the record subjects without unreasonable delay, but in no case later than 60 days after discovery of the breach.

1. For incidents that do not meet the HIPAA definition of a breach, VA must apply the standard provided by 38 U.S.C. § 5724 and first determine whether there is at least a reasonable risk of harm to the subjects due to the potential misuse of the PHI and whether VA's offer of notification or credit protection services to the subjects will enable them to promptly take actions that will assist them in preventing, limiting, or mitigating potential, identifiable harm from the breach.

2. The requirements for the content of the breach notices are the same under the HIPAA Breach Notification Rule and 38 U.S.C. § 5724.

(3) **Other Protection Services**: In addition to notification of a breach, the Data Breach Response Service, in collaboration with the DBCT if necessary, may provide other protection services.

(a) Other types of protection services include the following:

1. One year of credit monitoring services consisting of automatic daily monitoring of three relevant credit bureau reports;

2. Breach analysis;

3. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; or

4. One year of identity theft insurance.

(b) In deciding whether to provide such other credit protection services, 38 C.F.R. § 75.118 requires the following factors be considered:

1. The data elements involved;

2. The number of individuals affected or potentially affected;

3. The likelihood the SPI will be or has been made accessible to and usable by unauthorized persons;

4. The risk of potential harm to the affected individuals; and

5. The ability to mitigate the risk of harm.

NOTE: The decision to provide any or all of the services listed in paragraph (3)(a) above following a particular breach does not indicate that VA has determined that a reasonable, immediate, or substantial risk exists for the potential misuse of SPI involved in the incident. In the event of a breach, VA may, as a matter of discretion, provide any or all of these services even without a finding of reasonable risk or any of the above-described factors.

(c) The Data Breach Response Service will log, track, and close (when complete) routine incidents with established remediation processes. Non-routine incidents requiring senior leader involvement will be reported (escalated) to the DBCT for review, action, and follow-up reporting.

(4) **Procurement of Remediation (Credit Protection) Services**

(a) The Data Breach Response Service is responsible for establishing and maintaining all credit protection services provided by VA, including, but not limited to, credit monitoring, identity theft insurance, toll-free assistance lines, and fraud resolution services.

(b) When it is determined that a notification letter or an offer of credit protection services is needed, the local facilities' PO, or another person designated by the Facility's Director to serve

as the PO, will draft the letters based on templates that are provided. The letters must be on VA letterhead paper. After the letters have been mailed, a copy with individuals' names and addresses redacted will be attached in PSETS, along with information on the number of letters mailed, the date mailed, and a request to have the incident ticket closed. The incident is not considered closed until the letters are received in the mailbox and entered into PSETS. A weekly report of incidents requiring notification letters/credit monitoring that are still pending action is sent to the Administrations and Staff Offices to assist them in meeting the 60-day turnaround time for notifying Veterans.

(c) The template letters are available on the Data Breach Response Service Webpage http://vaww.oprm.va.gov/ir/ir_howTo.aspx . Letters must be mailed within 60 days from the date the incident occurred.

(d) The VA OI&T maintains a national contract for credit protection services. When the DBCT determines that credit protection services will be offered, the PO mails a letter providing enrollment instructions and a unique enrollment code. The code is required by the credit protection company to provide services at VA's expense.

(e) Codes are requested by the PO by sending an email to the Data Breach Response Service (vairstpromocodes@va.gov). The Data Breach Response Service provides codes to the PO. The following information must be included on the email request for codes:

1. Number of codes needed (i.e., the total number of living individuals impacted by the incident for whom VA maintains valid current addresses);

2. Facility responsible for the incident; and

3. The PSETS ticket number of the incident.

(5) **Incident Closure.** The Data Breach Response Service, in collaboration with the DBCT if necessary, makes the final determination that an incident is closed, and Data Breach Response Service staff notes the closure in the PSETS database. Generally, an incident may be considered closed when either:

(a) The Data Breach Response Service determines that no further action is needed, or

(b) All record subjects have been notified and/or offered remediation pursuant to that determination, and the responsible facility official has sent a copy of the redacted letter to the DBCT mailbox.

d. **Post Incident Activity**

(1) **Monthly Report to Congress on Data Breaches**. The Data Breach Response Service prepares the Monthly Report to Congress on Data Breaches for submission to Congress. The report should include:

(a) Incidents involving theft or missing hardware (whether or not they contain SPI);

(b) Incidents involving mishandling, mis-mailing, inappropriate access, and improper disposal that include SPI and are mistakenly sent to a person(s) other than the intended recipient; and

(c) Incidents involving 50 or more individuals.

(2) **Decision Appeal Process**

(a) VA components may appeal a decision by the Data Breach Response Service or the DBCT that a privacy incident is a breach or requires notification to or credit protection services for the individuals whose SPI was involved in the breach. The person responsible for the incident ticket may appeal the decision by emailing (mailto:VAIRCTMailbox@va.gov). Appeals must be made within 10 days of the Data Breach Response Service's or DBCT's initial decision using the Appeals Request form. Upon receipt of an appeal, the DBCT will determine whether to sustain, reverse, or modify the earlier decision based upon the information contained in, or presented with, the appeal. The Data Breach Response Service will notify the requester of the decision.

(b) The Data Breach Response Service or DBCT may modify their earlier decision if new facts are presented that demonstrate (1) a breach did not occur, that is, that VA SPI was not exposed to an unauthorized user, (2) the SPI involved in the breach does not face a reasonable (or greater) risk that the information may be misused to the record subject's detriment, or (3) VA is unable to provide individual notification in a breach involving SPI that is not PHI or involving PHI of fewer than 10 individuals. (When individual notification is not possible in a breach involving PHI of more than 10 individuals, notice must be via VA's web site or media outlets in compliance with the HIPAA Breach Notification Rule.)

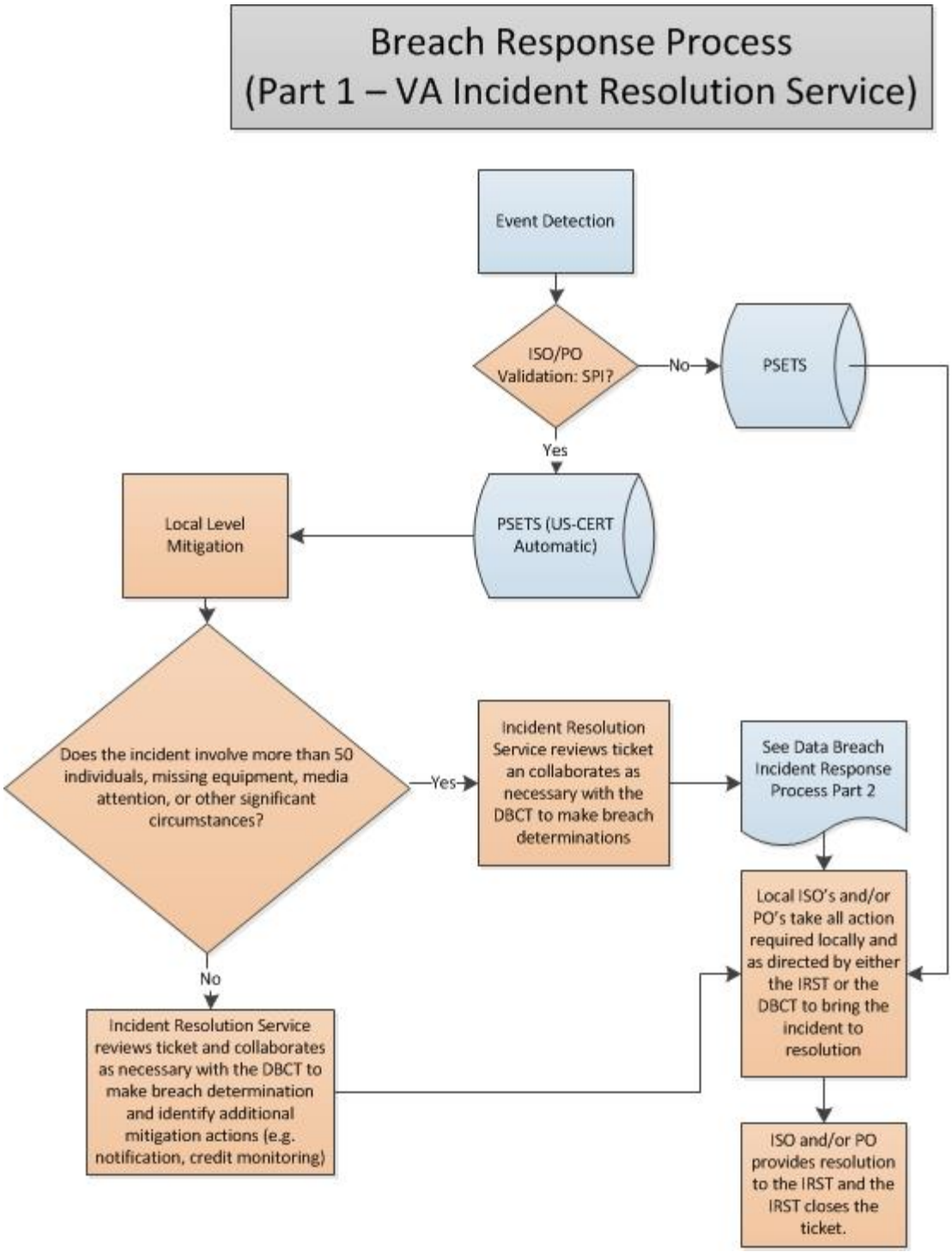

Figure 3: Breach Response Process (Part 1 – Data Breach Response Service)

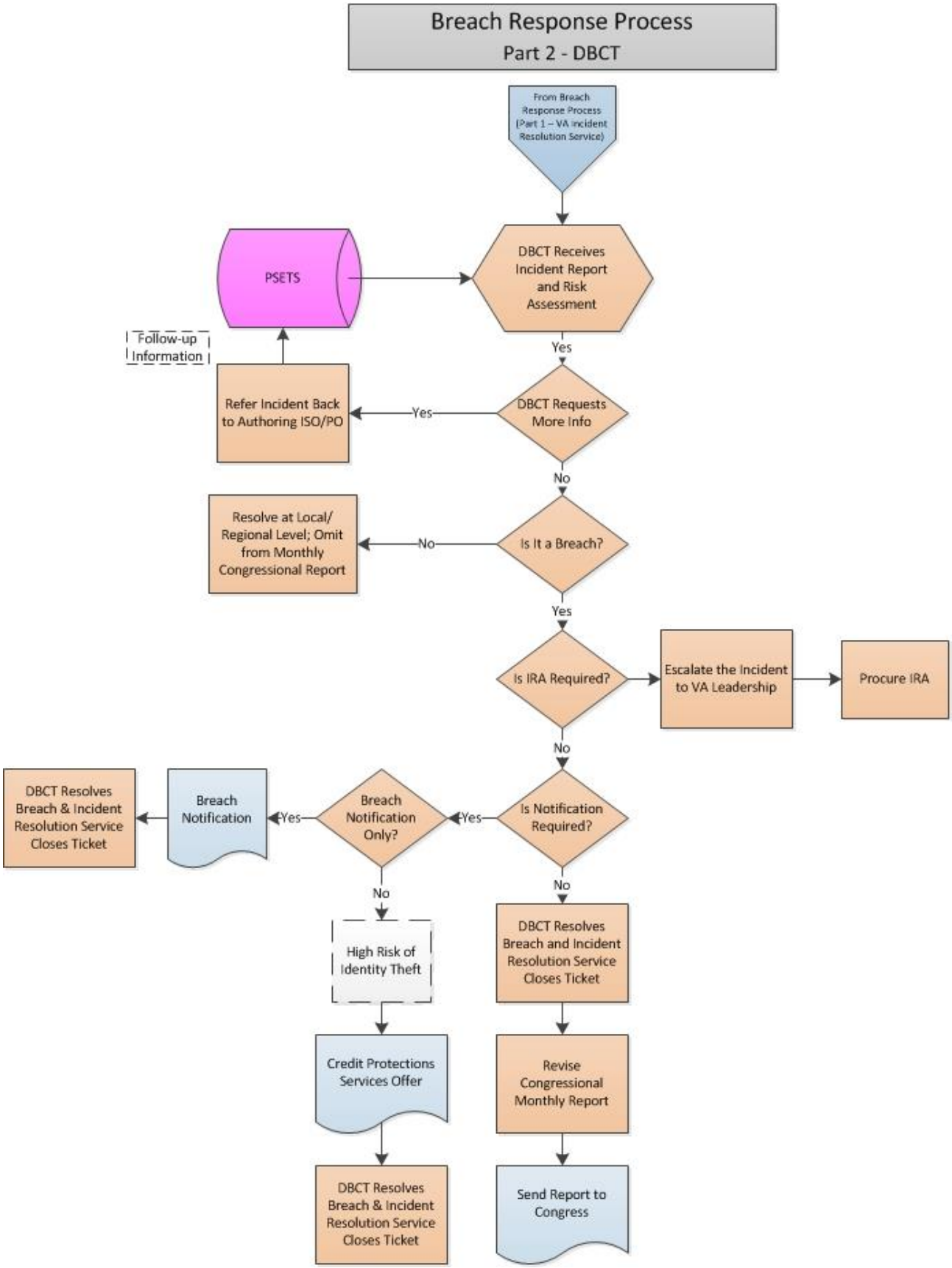

Figure 4: Breach Response Process (Part 2 - DBCT)

8. VA HITECH AND HIPAA BREACH NOTIFICATION RULE COMPLIANCE OVERVIEW

a. The HIPAA Breach Notification Rule applies only to VHA and its BAs. VHA's response to breaches under the Rule is coordinated by the Data Breach Response Service and the DBCT, which have been designated by the VA CIO to work closely with VHA and its BAs in taking actions necessary to comply with the Rule.

b. A toll-free phone number will be established for breaches potentially involving 500 or more individuals. The number will be activated and posted, along with notification to the media, as required by the HIPAA Breach Notification Rule, on the VA facility's web page so that individuals can call to ask questions about the incident.

c. Approved letter templates and press release templates, if needed, will be provided by the Data Breach Response Service.

d. PAOs must work with facility POs to ensure that the press release and notification letters contain identical descriptions of the incident. The press release should tell no more than the letter tells and should be released to local media within the jurisdiction of the facility, although the local media are not required to publish the press release.

e. If there is a breach involving 500 or more individuals, the Data Breach Response Service will report the breach in the OI&T Daily Brief. The Director, Data Breach Response Service, will also notify VA Senior Leadership and VA OIG via email of the breach.

f. Press releases under HITECH/HIPAA documents and quarterly and monthly breach reports to Congress may be found at: http://www.va.gov/notices.asp.

9. INDIVIDUAL, MEDIA, AND HHS BREACH REPORTING PROCESS

a. **Overview of Reporting Process.** The process for reporting breaches to the individual, the media, and HHS to meet HIPAA Breach Notification Rule requirements, which apply only to breaches that involve unsecured PHI maintained by VHA or its BAs and do not fall under one of the enumerated exceptions, is as follows:.

(1) In addition to individual notification to the record subjects, HHS must be notified annually about any breach as defined by the Rule. Breaches involving 500 or more individuals also require immediate notification to HHS, notification to the media, and posting of information about the breach on the VA web page.

(2) The process for notifying individuals, pursuant to 45 C.F.R. § 164.404, is managed within the PSETS.

b. **Breaches Treated as Discovered.** A breach is treated as discovered on the first day that the breach is known or, through the exercise of reasonable diligence, would have been known to the CE or BA.

(1) A breach is considered "known" on the day that any workforce member or agent, except those committing the breach, learns of the breach.

(2) Reasonable diligence is the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. Factors to consider in determining whether reasonable diligence was performed include whether:

(a) A CE or BA took reasonable steps to learn of breaches; and

(b) Indications of breaches were present that should have triggered an investigation.

c. **Required Notification Elements.** Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include:

(1) Description of the breach, including date of the breach and date of its discovery, if known;

(2) Description of the type of information that was involved in the breach (e.g., name, address, SSN, DOB);

(3) Steps that the individuals should take to protect themselves from potential harm;

(4) Brief description of what the CE is doing to investigate the breach, mitigate the harm, and prevent future breaches; and

(5) Contact information for the CE.

d. **Substitute Notice to Individuals.** If the CE does not have a valid, current address for individuals whose unsecured PHI is involved in a breach, substitute notice must be provided to them. If the CE does not have valid, current addresses for fewer than 10 individuals involved in the breach, an alternative form of written notice, or notice by telephone or other means, may be provided. If the CE does not have valid, current addresses for 10 or more individuals, it must provide substitute notice by posting the notice either conspicuously on the VA and VHA websites for 90 days or in major print or broadcast media in the geographic area where the individuals are likely to reside. In either situation, the CE must also provide a toll-free number for at least 90 days, so the individual can learn whether his/her data was involved in the breach.

e. **Notification to HHS**. HHS must be notified of any breach involving unsecured PHI for 500 or more individuals, contemporaneously with the individual notice (in no case later than 60 days after discovery of the breach). Information regarding these breaches is posted on the HHS web site. For breaches involving fewer than 500 individuals, the CE must provide HHS with annual notice or notice on a rolling basis, but in either event no later than 60 days after the end of each calendar year. The Data Breach Response Service handles notification to HHS.

f. **Notification to the Media**. If the breach involves 500 or more individuals in one state or jurisdiction, a press release regarding the breach must be issued in one of the major news media outlets in that state or jurisdiction.

10. HITECH/HIPAA SIGNIFICANT RULING NOTIFICATION PROCESS

a. **Overview.** The notification procedure for breaches involving PHI is as follows:

(1) Incidents involving fewer than 500 individuals and 500 or more individuals who are not in the same state or jurisdiction – refer to the section of the flowchart colored in green (Figure 5).

(2) Incidents involving 500 or more individuals located in the same state or jurisdiction – refer to the section in light purple (Figure 5).

(3) The Conspicuous Posting/Substitute Notice – refer to the section in red (Figure 6).

(4) Incidents involving SPI other than PHI (i.e., not subject to the HIPAA Breach Notification Rule) – refer to the section in blue (Figure 7).

b. **Individual Notification of Fewer Than 500 Individuals.** Figure 5 demonstrates the process used when a breach involves fewer than 500 individuals and therefore may be reported annually to HHS rather than concurrently with the individual notification.

(1) The local PO will complete notification letters, using the template letter provided by the Data Breach Response Service, and ensure mailing of the notification letters to the record subjects. The facility Director, or the designee, will sign the letter.

(2) A redacted letter will be attached to PSETS for archival purposes, along with mitigating and corrective actions taken.

(3) The local PO will maintain a list of individuals who were sent notification letters in the same spreadsheet used for tracking notification letters.

(4) Entering the breach on the HHS website will satisfy the requirement for annual reporting under the HIPAA Breach Notification Rule to HHS. The annual method of reporting requires that all breaches from the prior year are entered into the HHS website by March 1 of the current year. The reporting may be made annually or on a rolling basis. For incidents involving fewer than 500 individuals, the Data Breach Response Service will submit the information to HHS when the redacted letters are received and then will close out the PSETS ticket.

c. **Individual Notification of 500 or More Individuals.** Figure 5 illustrates the process used when a breach involves 500 or more individuals. If the breach affects 500 or more individuals, notice to HHS must be provided concurrent with the individual notification. If the 500 or more affected individuals are within the same state or jurisdiction, the CE must also notify prominent media outlets serving that area without unreasonable delay and in no case later than 60 days from the date of the discovery of the breach.

(1) The local PO will complete Notification Letters, using the DBCT provided template letter, and will ensure mailing of the notification letters to the record subjects. The facility Director, or the designee, will sign the letter.

(a) The local PAO will prepare a news release, using a sample provided by the Data Breach Response Service, based on the DBCT template letter. The news release will serve as the

media notice and the legal notice. It will also serve as the substitute notice. The details will be consistent with the details provided in the notice to the individuals.

(b) The package will go through the Data Breach Response Service, DBCT, and VA Central Office (VACO) approval channels for processing.

(c) Once the package is approved, the local PAO will send out the news release after the notification letters are sent and arrange for the publication of the legal notice using appropriate media outlets.

(2) The local PAO will provide a copy of the news release to the local ISO, PO, and Regional Counsel.

(3) The local PO will email the news release to the Data Breach Response Service, and the Data Breach Response Service will add it to the PSETS ticket for archiving.

(4) The Data Breach Response Service will submit the report to HHS, for breaches involving 500 or more individuals, within 60 days of the date that the breach was discovered, but no later than when the individuals are notified, whichever is sooner.

(5) If law enforcement, including the OIG, requests in writing a delay in notifications, then the Data Breach Response Service will delay providing the notice for the time period specified by the request. Notification will be delayed for 30 days if the request is provided orally. Documentation of written or oral requests will be added to the PSETS ticket.

d. **Substitute Notice for Fewer Than 10 Individuals Without a Valid Current Address.**

(1) Figure 6 illustrates the process used to provide substitute notice to fewer than 10 individuals because VA does not have their valid current addresses. The substitute notice may be in the form of an alternative form of written notice, or notice by telephone or other means.

(2) The local PO is responsible for tracking all returned letters and action taken on them, using a spreadsheet or other means as directed by the VHA Privacy Office.

(3) The local PO will also provide a copy of the substitute notice to the local ISO and Regional Counsel.

(4) The local ISO/PO will attach to the PSETS a description of the method by which substitute notice was provided.

e. **Substitute Notice for 10 or More Individuals Without a Valid Current Address.**

(1) Figure 6 illustrates the process used to provide substitute notice to 10 or more individuals because VA does not have their valid current addresses. The substitute notice may be made by either posting the notice conspicuously on the VA and VHA websites for at least 90 days or in major print or broadcast media in the geographic area where the individuals are likely to reside. In addition, a toll-free number must be provided for at least 90 days, so that individuals can learn whether their data were involved in the breach.

(2) The local PO is responsible for tracking all returned letters and action taken on them, using a spreadsheet or other means as directed by the VHA Privacy Office.

(3) If the local PO has 10 or more individuals without a valid current address, including those for whom letters were returned as undeliverable, the PO will notify the local PAO.

(4) The local PAO will prepare a summary write-up and submit it, along with the notice itself, to the VA Webmaster.

(5) The VA Webmaster will post the summary write-up and notice on the VA website. It will remain on the website for at least 90 days unless specified for a longer period by the local PAO.

(6) The local PAO will provide a copy of the summary write-up and the notice to the local ISO, PO, and Regional Counsel.

(7) The local ISO will email the summary write-up and the notice to the Data Breach Response Service, and the Data Breach Response Service will add the write-up and notices to the PSETS ticket for archival purposes.

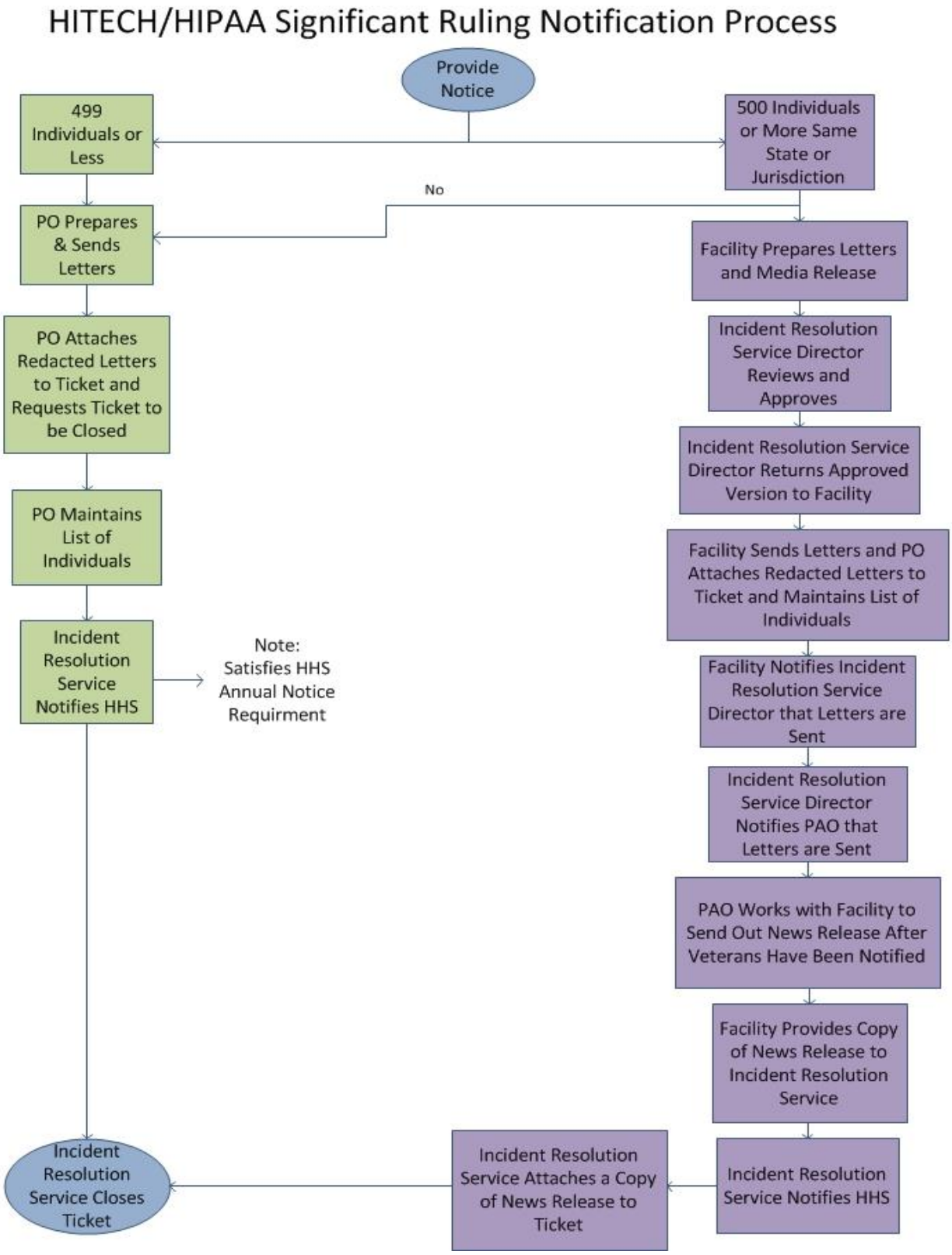

Figure 5: HITECH Significant Ruling Flow Chart

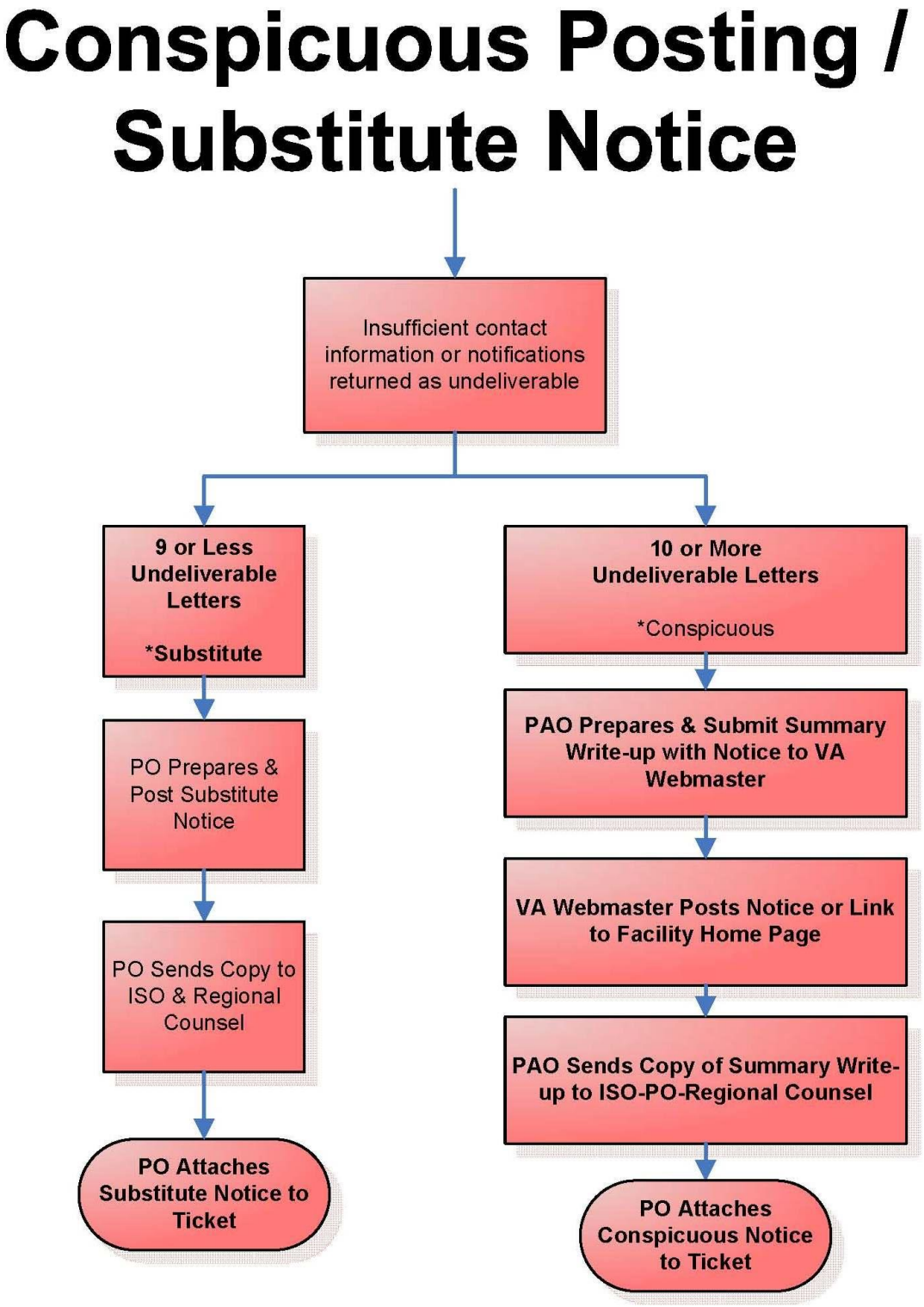

Figure 6: Conspicuous Posting / Substitute Notice Flow Chart

f. **Non-HHS Reportable Incidents**

(1) The flowchart 7 is the process used for breaches that do not meet the definition under the HIPAA Breach Notification Rule but have the potential to compromise the SPI of individuals.

(2) The local PO will complete letters, using the DBCT provided letter template, and will ensure mailing of the notification letters to the individuals affected by the breach. The facility Director, or the designee, will sign the letter.

(3) A redacted copy of the letter will be attached by the PO to the PSETS ticket for archival purposes.

(4) The local PO will maintain a list of individuals, with pertinent information, who were sent notification letters.

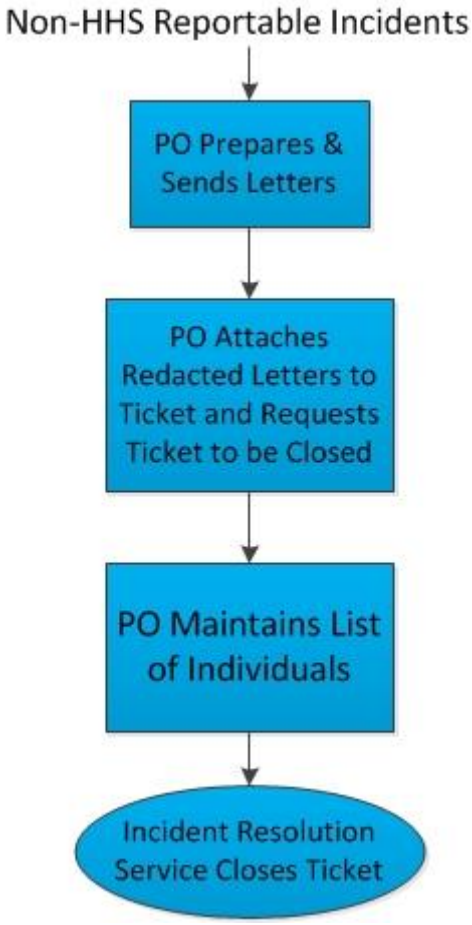

Figure 7: Non-HHS Reportable Incidents Process Flow Chart

11. BREACH NOTIFICATION AND THE VHA PAO

a. The HIPAA Breach Notification Rule requires CEs to send a local news release and information to HHS for Web posting within 60 days of the discovery of a breach, if the incident involves the PHI of more than 500 people within a state or local jurisdiction. If there is insufficient or out-of-date contact information for more than 10 individuals, substitute notification must be provided on the VA website or in major print or broadcast media in geographic areas in which the individuals affected by the incident are likely to reside.

b. Templates for notification letters are included with the other template letters located on the Data Breach Response Service Webpage vaww.incidentresolution/templates.va.gov. Sample news releases are available from OPIA regional offices.

c. PAOs required to prepare a news release will receive previous news releases from the Data Breach Response Service to serve as guides, depending on whether credit protection is offered. Working with the facility PO, who must prepare the notification letter to Veterans, PAOs draft local releases to include all the information for individual notification, including:

(1) Description of the incident, including date of the breach and date of its discovery, if known;

(2) Description of the type of information that was involved (e.g., name, address, SSN, DOB);

(3) Steps that the individuals should take to protect themselves from potential harm (e.g., monitoring their credit reports, contacting the credit reporting companies to request fraud alerts);

(4) Description of what the facility is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

(5) Contact information for individuals with questions.

d. PAOs should consider the prospect of having their regional OPIA staff as a resource.

e. PAOs should give their draft release to their facility PO, who will send it to OI&T's Data Breach Response Service. That group ensures that the release and the notification letter are reviewed by the DBCT at its weekly meeting. The DBCT has representatives from all three Administrations and the OGC, OI&T, OCLA, OPIA, and OS/Strategic Communications. When the news release has been approved and sent out, the PAO must give a copy to the facility PO and identify the media outlet(s), to which it was sent. The PO sends it to the Data Breach Response Service staff, who notifies HHS of the incident.

f. When news media contact PAOs for more information, PAOs should be prepared, in collaboration with their PO or ISO, to say what the facility has done or is about to do to prevent a recurrence.

12. HIPAA/HITECH LAW ENFORCEMENT DELAY OF NOTIFICATION.

a. If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed.

b. If the law enforcement request to delay is made in writing and specifies the time period for which a delay is required, notification must be delayed for that time period.

c. If the request is made orally, the identity and statement of the law enforcement official must be documented, and the notification must be delayed for no longer than 30 days, unless a written request that specifies the time period for which a delay is required is received during that time.

13. TERMS AND DEFINITIONS

a. **Business Associate (BA).** A person or entity (other than a member of VHA's workforce), that performs or assists in the performance of a function or activity on behalf of VHA that involves the creating, receiving, maintaining or transmitting of PHI, or that provides to or for VHA certain services as specified in the Privacy Rule that involve the disclosure of PHI by VHA. The term "Business Associate" also includes a subcontractor of a Business Associate that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate.

.

b. **Covered Entity (CE).** An organization or individual that is covered by the compliance requirements of HIPAA and is: (a) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Privacy Rule; (b) a health care clearinghouse; or (c) a health insurance plan. VHA is both a health plan and a health care provider.

c. **Credit Protection Services.** All of the services listed in 38 U.S.C. § 5724(b) and 38 C.F.R. § 75.118. Using this Handbook, the Data Breach Response Service, in collaboration with the DBCT if necessary, may decide to offer one or more of the services listed in section 5724(b). Credit protection services need not be provided if there is less than a reasonable risk of identity theft. Note: The decision to provide credit protection services does not indicate that VA has determined that a reasonable risk exists for the potential misuse of SPI involved in the incident.

d. **Federal Tax Information (FTI)**. Any return or return information received from the IRS or secondary source, such as Social Security Administration. It includes any information created by the recipient derived from the return or return information.

e. **Incident.** Any event that has resulted in, or has the potential to result in, unauthorized access to or disclosure of VA SPI in a manner not permitted under the applicable confidentiality provisions.

f. **Individually Identifiable Health Information (IIHI).** As defined by the HIPAA Privacy Rule, information that: "(1) is created or received by a health care provider, health plan, or health care clearinghouse; (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 (3)(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

g. **Limited Data Set (LDS).** As defined by the HIPAA Privacy Rule, PHI that excludes the following list of direct identifiers of the individual or his/her relatives, employers, or household members: names; postal address information, other than town or city, State, and zip code; telephone numbers; fax numbers, electronic mail addresses; Social Security Numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocols (IP) address numbers; biometric identifiers; and full face photographic images and any comparable images.

h. **Personally Identifiable Information (PII).** Any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with other personal identifying information that is linked to a specific individual, such as date and place of birth, mother's maiden name.

i. **Protected Health Information (PHI).** As defined by the HIPAA Privacy Rule and except as provided in para. (2) of this definition, IIHI (see definition of IIHI above) that:

(1) By a CE, is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium; and.

(2) Excludes IIHI: (i) in education records covered by the Family Education Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) in records described at 20 U.S.C. § 1232g(a)(4)(B)(v); (iii) in employment records held by a CE in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.

VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements, defines PHI as a subcategory of PII that applies only to individually-identifiable health information that is under the control of VHA, as VA's only CE under HIPAA, or its BAs, such as OI&T, OGC, OPIA, or OCLA.

j. **Sensitive Personal Information (SPI).** As defined in 38 U.S.C. § 5727, any information about an individual maintained by VA, including the following:

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

(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, or biometric records; and

(3) Information that requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information.

SPI is sometimes characterized as PII (see definition of PII above). A subset of SPI is PHI (see definition of PHI above).

k. **Unsecured PHI.** PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS in guidance. This guidance will be updated annually and is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

14. REFERENCES

a. **Statutes**

(1) 38 U.S.C. §§ 5721-28, Information Security.

(2) Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 123 Stat. 226, 260 (2009), codified at 42 U.S.C. § 17932.

(3) Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996).

(4) 44 U.S.C. §§ 3551-58, Federal Information Security Modernization Act of 2014.

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

(6) 38 U.S.C. § 5701, VA Claims Confidentiality Statute.

(7) 38 U.S.C. § 5705, Confidentiality of Medical Quality Assurance Review Records

(8) 38 U.S.C. § 7332, Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Health Records

b. **Regulations**

(1) 38 C.F.R. §§ 75.111-.119, Data Breaches.

(2) 45 C.F.R. Parts 160 and 164, HIPAA Privacy, Security, and Breach Notification Rules.

c. **Office of Management and Budget Publications**

(1) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifying Information, (May 22, 2007).

(2) OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification (Sept. 20, 2006).

d. **National Institute of Standards and Technology Publications**

(1) Special Publication 800-61Revision 2, Computer Security Incident Handling Guide (Aug. 2012).

(2) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Apr. 2010).

(3) Special Publication 800-66 Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability Act (HIPAA) Security Rule (Oct. 2008).

e. **Other References**

(1) Final Rule for Breach Notification for Unsecured Protected Health Information, 78 Fed. Reg. 5566 (Jan. 25, 2013).

(2) Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, Office for Civil Rights, Department of Health and Human Services, 74 Fed. Reg. 19006 (Apr. 27, 2009).

(3) VA Directive 6500, Managing Information Security Risk: VA Information Security Program (Sept. 20, 2012).

(4) VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program (Mar. 10, 2015).

(5) VA Directive 6502, VA Enterprise Privacy Program (May 5, 2005).

(6) VA Handbook 6502.1, Privacy Event Tracking (Feb. 18, 2011).

(7) VA Directive 6509, Duties of Privacy Officers (Aug. 13, 2009).

(8) VA Directive 6609, Mailing of Sensitive Personal Information (May 20, 2011).

(9) VHA Handbook 1605.05, Business Associate Agreements (July 22, 2014).