DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA HANDBOOK 6500.2
Transmittal Sheet
January 6, 2012

MANAGEMENT OF DATA BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION (SPI)

1. REASON FOR ISSUE: This Handbook establishes procedures for Department of Veteran Affairs (VA) management of data breaches involving VA Sensitive Personal Information (SPI). It implements 38 U.S.C. §§ 5721-28; and the implementing regulations at 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 interim final regulations at 45 C.F.R. §§ 164.400-.414, and Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information*.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: In accordance with the provisions of VA Directive 6500, *Information Security Program*, this Handbook provides the procedures that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting. This Handbook also contains criteria that the Data Breach Core Team (DBCT) uses to evaluate data breaches to determine whether VA should offer one or more credit protection services.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OIT) (005), Office of Information Security (005R), Risk Management and Incident Response (RMIR) (005R3).

4. RELATED ISSUES

a. VA Directive and Handbook 6500, *Information Security Program*.

b. Appendix E contains additional references related to this Handbook.

5. RESCISSIONS

a. VA Handbook 6500.2, *Management of Security and Privacy Incidents*, June 17, 2008.

b. Interim Process for Communication and Escalation of VA IT Resource Outage Notifications and Failover Requests (005OP1), October 11, 2007.

CERTIFIED BY:

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

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

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

Distribution: Electronic Only

MANAGEMENT OF DATA BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION (SPI)

CONTENTS

PARAGRAPH **PAGE**

APPENDIX B: ROLES AND RESPONSIBILITIES

APPENDIX C: INCIDENT RESOLUTION TEAM PROCESS

APPENDIX D: VA PROCESS FOR COMPLIANCE WITH HITECH ACT

MANAGEMENT OF DATA BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION (SPI)

1. PURPOSE AND SCOPE

a. Purpose. This Handbook provides incident oversight, management, and reporting procedures to ensure appropriate and expeditious handling of data breach incidents involving SPI under the ownership of the Department of Veterans Affairs (VA).

b. Scope. The procedures in this Handbook apply to all 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 (VA personnel).

2. BACKGROUND

a. The VA Information Security Enhancement Act of 2006, Pub. L. No. 109-461, 120 Stat. 3450, (codified at 38 U.S.C. §§ 5721-28 (2010)), 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.

b. Section 13402 of the HITECH Act and the Breach Notification Rule at 45 C.F.R. § 164.400-414 required covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates to notify individuals of breaches involving their unsecured protected health information (PHI).

c. The Office of Management and Budget (OMB) M-07-16, *Safeguarding Against and Responding to Breach of Personally Identifiable Information,* required agencies to develop and implement a breach notification policy while maintaining proper safeguards to protect such information.

d. Based on these three provisions, 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 which poses a risk of financial, reputational, or other harm to the individual**.**

3. DOCUMENT ORGANIZATION

a. **Handbook**. The Handbook describes the incident handling process and the oversight role of the Incident Response Governance Board (IRGB).

b. **Appendices**. The appendices contain the procedures VA employees must follow for handling data breach incidents, as well as information applicable throughout the Handbook and Appendices, such as Abbreviations and Acronyms and the Glossary of Terms.

(1) **Appendix A: Data Breach Core Team Review Process.** Contains the criteria that the Data Breach Core Team (DBCT) uses to determine whether an incident reported to the DBCT is a data breach involving VA SPI. It also contains the criteria that the DBCT uses to determine whether VA should notify individuals impacted in an actual or potential data breach involving VA SPI and/or offer credit protection services. This appendix is used in conjunction with Appendix C.

(2) **Appendix B: Roles and Responsibilities**. Contains the roles and responsibilities of VA organizations for the oversight, handling, and reporting of data breach incidents.

(3) **Appendix C: Office of Information and Technology (OIT) Incident Resolution Team Process.** Describes the functions and processes of the Incident Resolution Team for managing data breaches, and includes links to credit protection and notification letter templates.

(4) **Appendix D: VA Process for Compliance with the HITECH Act.** Describes the process that VA has implemented to comply with the data breach notification provisions of the HITECH Act.

(5) **Appendix E: References**. Contains statutory, OMB, National Institute of Standards and Technology (NIST), VA, and Health and Human Services (HHS) references that apply to the information in this Handbook.

(6) **Appendix F: Acronyms**. Contains a list of acronyms that appear in this Handbook.

(7) **Appendix G: Glossary of Terms**. Contains a list of terms that are used in this Handbook and their definitions.

4. DATA BREACH INCIDENT RESPONSIBILITIES

a. **Introduction**. Data breach incident handling is part of the overarching incident handling process designed to manage and mitigate risk. The process contains four main areas: Incident Preparation; Incident Detection, Reporting, and Analysis; Corrective/Mitigation Action; and Post-Incident Activity. The IRGB provides the necessary oversight to ensure that VA promptly identifies and responds appropriately to data breaches involving VA SPI.

b. **Incident Handling**. This section provides an overview of VA's process for addressing data breaches. Appendix B contains the list of VA organizational roles and responsibilities for handling data breaches, specifically the IRGB and DBCT. Figure 1 illustrates the IRGB organization. This Handbook only identifies responsibilities associated with handling data breaches.

Figure 1: IRGB Organization

c. **IRGB Oversight**. The role of the IRGB, as stated in its charter, is to "provide oversight and policy direction for analyzing and reporting data breach incidents across VA." The IRGB is responsible for promulgating policy, recommending corrective actions, and overseeing the process that prepares for, detects, reports, analyzes, contains, eradicates, recovers, and performs process improvement to resolve incidents. Figure 2 illustrates the IRGB process. For an extensive flowchart, which depicts the entire Incident Response Process and all its stakeholders, click the IRT Service Disruption and Data Breach Communications Flowchart link.

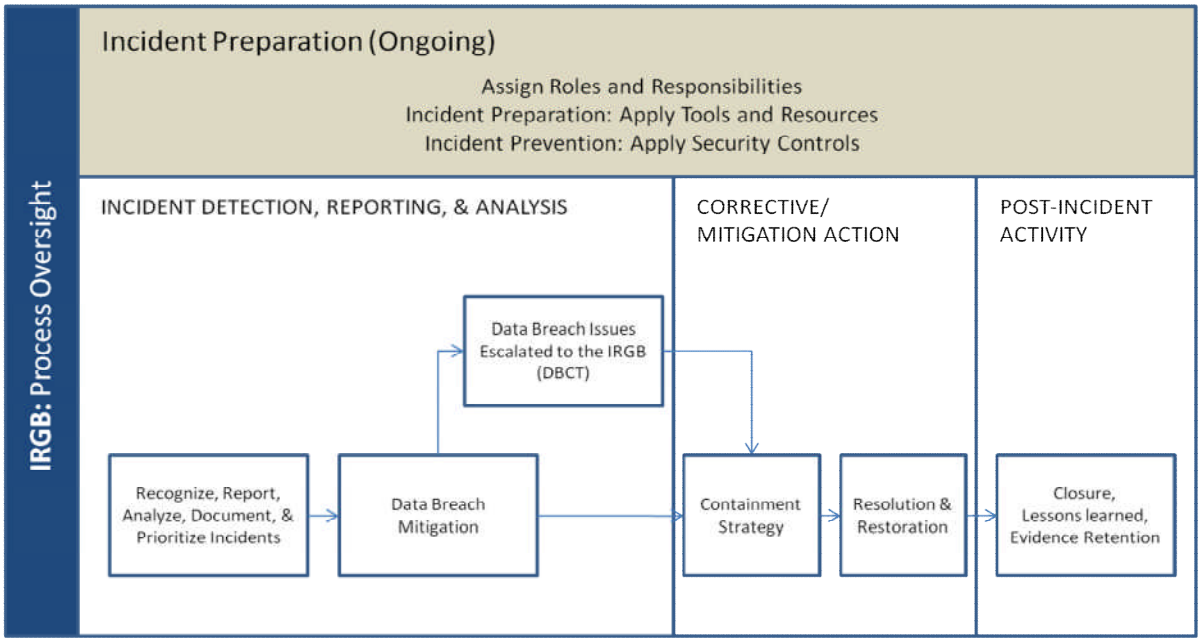

Figure 2: Incident Handling Chart

(1) **Incident Preparation**

(a) **Roles and Responsibilities.** Incident Preparation begins with assigning the roles and responsibilities across VA to handle data breach incidents. Appendix B contains the list of VA organizational roles and responsibilities for handling data breaches.

(b) **Incident Prevention.** Security and privacy policies and system security controls are the primary mechanisms for preventing and reducing the number of data breach incidents. The IRGB, through the DBCT and the SDCT, ensures that appropriate policies and controls exist to protect SPI and VA information systems using, storing and transmitting SPI.

(2) **Incident Detection, Reporting, and Analysis.** Incident detection and reporting occurs either through technical detection or reporting of the incident. A user must immediately report to his/her VA supervisor, Privacy Officer (PO), and Information Security Officer (ISO) any data incident involving the compromise of any VA sensitive information. The PO and/or ISO will promptly report the incident (within one hour of notification) to the VA-Network Security Operations Center (VA-NSOC) in accordance with the OIT Incident Management procedures. *See* VA Handbook 6502.1, Privacy Event Tracking.

(3) **Corrective/Mitigation Action.** After an incident has been detected and reported, DBCT will determine and take the steps necessary to contain the incident. Depending on the results of the analysis, recovery activities may include training employees on applicable policy and proper procedures and providing notice or credit protection services to individuals who's SPI was compromised in a data breach. While engaging in these activities, VA officials will also collect evidence to support potential legal proceedings.

(4) Post-Incident Activity. Post incident activity involves: Asking questions about the incident, such as, what happened; when; how well staff and management responded; confirming that the incident is closed by addressing the incident in writing and providing closure; using collected incident information to improve processes, and retain evidence.

APPENDIX A
DATA BREACH CORE TEAM REVIEW PROCESS

1. PURPOSE

a. This appendix contains the criteria that the DBCT uses to determine whether an incident reported to the DBCT is a data breach involving SPI. This appendix also contains the criteria that the DBCT uses to determine whether VA should offer credit protection services to the individuals involved with data breaches involving VA SPI. Finally, this appendix lists several recurring situations that VA has determined warrant the offer of credit protection services under an Accelerated Response.

b. This appendix does not address VA's response to a data breach involving VA sensitive data that is not SPI, such as embargoed budget data.

c. This appendix does not identify or discuss the security and privacy incidents that VA officials and facilities must report to the DBCT.

2. TERMS: This appendix uses three phrases defined by statute, regulation or government-wide guidance. These phrases are: "data breach," "sensitive personal information," and "credit protection services."

a. **Data Breach**

(1) The VA-specific definition of the term "data breach" in 38 U.S.C. § 5727(4)[1] is "the loss, theft, or other 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."

(2) OMB Memorandum M-07-16, "*Safeguarding against and Responding to the Breach of Personally Identifiable Information*," issued May 22, 2007, uses the term "breach." Footnote 5 of the Memorandum explains that "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 personally identifiable information, whether physical or electronic." The OMB 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."

(3) 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).

---

[1] Added to title 38, United States Code, by PUB. L. NO. 109-461, section 902(a), 120 STAT. 3403, 3450-60 (Dec. 22, 2006), which added sections 5721-28 to title 38. Section 5727 begins on page 3457.

(4) Interim regulations promulgated by the Department of Health and Human Services (HHS) clarify that "compromises the security of privacy of such information," is limited to those instances where there is a "significant risk of financial, reputational, or other harm to the individual." 45 C.F.R. § 164.402 (2010) (interim final regulation). It is unclear whether the final regulations will include this risk threshold, which is higher than the "reasonable risk of potential misuse" standard under 38 U.S.C. § 5724.

(5) While the three definitions of a data breach (or breach) use slightly different phrasing, they generally refer to unauthorized access to SPI that results in the potential compromise of the confidentiality or integrity of the information. Consequently, the VA DBCT uses the VA-specific term, data breach, and its definition in determining whether the reported event constitutes a data breach that the DBCT reviews to decide whether VA has to notify the record subjects of the event and offer them credit protection services.

a. **Sensitive Personal Information**

(1) "Sensitive Personal Information" is individually identifiable information protected by one or more confidentiality provisions, such as the Privacy Act, 5 U.S.C. § 552a; 38 U.S.C. §§ 5701, 5705, and 7332; or the HIPAA Privacy Rule. The term is defined in 38 U.S.C. § 5727 as any information about the individual maintained by VA, including the following:

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

(b) 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.

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

(2) SPI is sometimes characterized as: Personally Identifiable Information (PII) defined by OMB as "information that can be used to distinguish or trace an individual's identify such as their name, social security number (SSN), or biometric records, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual such as a date or place of birth or mother's maiden name, etc."

(3) A subset of SPI is Protected Health Information (PHI) defined in the HIPAA Privacy Rule as 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 (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.

(a) In VA, individually identifiable health information maintained by VHA, as a covered entity (CE), or a business associate (BA) on behalf of VHA, such as OIT, OGC, OPIA, or OCLA, is the only SPI that is considered PHI.

(b) The HITECH Act requires notification of a breach only when an incident involves:

1. A disclosure of unsecured PHI

2. In violation of the HIPAA Privacy Rule

3. That compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual and

4. Excludes (i) any unintentional acquisition, access, or use of PHI by an employee 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 unauthorized use or disclosure, (ii) any inadvertent disclosure by an employee or agent of a CE or BA to another employee or agent of the same CE or BA that does not result in further unauthorized use or disclosure, or (iii) a disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

5. The appendix reflects the requirement that where an incident involving PHI meets the HITECH definition of a data breach, VA must notify the record subjects without unreasonable delay, but in no case later than 60 days after discovery of the breach as required by the HITECH Act. As noted above, pursuant to interim final regulations a breach of PHI occurs where there is a "significant risk of financial, reputational, or other harm to the individual." For incidents that do not meet the HITECH definition of a data breach, VA must apply the standard provide by 38 U.S.C. § 5724 and determine whether there is at least a reasonable risk of harm of potential misuse to the subjects and whether VA's offer of credit protection services, including notice, 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 before offering credit protection services or simply notifying subjects of the breach. The requirements for the content of the data breach notices are the same under the HITECH Act and section 5724.

3. CREDIT PROTECTION SERVICE PROCESS

a. This appendix uses the phrase "credit protection services" to include all of the services listed in 38 U.S.C. § 5724(b) and 38 C.F.R. § 75.118. Using this appendix, the DBCT may decide to offer one or more of the services listed in section 5724(b). Credit protection need not be provided if there is less than a reasonable risk of identity theft.

b. Upon receipt of an Incident Report from the VA-NSOC, the DBCT will review the report to determine if a data breach has occurred and, if so, if VA should notify or offer credit protection services to those individuals involved in the data breach.

c. A data breach occurs when VA, or someone with authorized access to VA SPI, loses control of VA SPI, and, after the loss of control, unauthorized individuals may have access to that SPI. Loss of control may occur in different ways, including loss of the data, theft of the data, or unauthorized access to the data, which includes access to data for an unauthorized purpose, impermissible disclosure, or inappropriate disposal of the data. If VA regains control of the data, a data breach still occurred while the data was outside VA's control, assuming that while outside VA control, unauthorized individuals may have had access to the data. The DBCT considers the risk of compromise of the data while it was exposed to determine if VA should notify or offer credit protection services to those individuals affected

by the breach. Access to the data means that an unauthorized individual may see, use, obtain, distribute, disclose, destroy, or copy the data. In other words, the unauthorized user of the data may obtain control of the data or a copy of the data and use the data as the unauthorized user wishes. The degree to which an unauthorized user may have had access to the data is also considered by the DBCT.

d. In evaluating the information provided about a reported data breach, the DBCT makes several decisions in the following order when deciding if notification or credit protection services are warranted, and, if so, which service to offer. In the flow chart in Figure A-1, each decision, in order, must be yes or the DBCT does not make the next decision in the following sequence.

(1) The DBCT decides whether VA SPI may have been exposed to any unauthorized individuals, that is, whether an unauthorized user could obtain access to the compromised data in a readable or usable form while it was exposed in violation of any of the applicable confidentiality provisions. The DBCT decides if an unauthorized user could view, use, obtain, distribute, disclose, destroy, or copy the data as he or she wishes, which defines a data breach.

(2) The DBCT determines if the compromised SPI came from a VHA Patient record. If it does, VA must provide the notice to the record subject (the HIPAA Notice) if required by the HITECH standard. The DBCT then continues with the rest of the analysis below to determine if VA has to provide credit protection services under 38 U.S.C. § 5724.

(3) The DBCT determines whether there is a risk of harm to the subjects of the compromised data from possible misuses of the data by an unauthorized user. The potential misuse(s) and possible harm(s) must be identifiable, but need not be certain ~ that is, the DBCT has to identify at least one potential misuse of the data, and at least a possible harm to the record subject, as a result of the identified potential misuse of the SPI involved in the data breach. Figure A-1 shows the sequence of steps of the credit protection service.

(4) The DBCT determines the likelihood of the harm - that is, how likely is it that the data may be misused in an identifiable way for a particular purpose, e.g., identity theft.

(5) The DBCT determines the level of the risk of harm associated with the potential misuses of the data to cause an identifiable harm. There are three possible levels: an immediate and substantial risk, a reasonable risk, or a low level risk.

(6) If the level of risk is either immediate and substantial or reasonable, the DBCT determines whether providing timely notice to the record subjects may enable them to promptly take steps to protect themselves from the potential harm. If the answer is yes, then the DBCT refers the matter to the appropriate office to provide notice.

(7) Simultaneously, if the level of risk is either immediate and substantial or reasonable, the DBCT determines whether the offer of other credit protection services to the record subjects will assist in timely prevention, limitation, or mitigation of possible harm to them. In answering this question, the DBCT decides which credit protection services will assist the record subjects in preventing, limiting or mitigating possible harm. The DBCT then refers the matter to the appropriate office to provide other credit protection services identified as appropriate by the DBCT [see Procurement of Remediation

(Credit Protection) Services in Appendix C for additional details and credit protection services templates].

a. A member of the IRT reviews an incident prior to presentation to the DBCT. If the incident is one of the types for which the IRT has previously determined the types of services that should be offered, the initial IRT reviewer may process the incident in that manner, initiate offering of the credit protection services, and obtain DBCT confirmation of the decision. As additional types of incidents are identified, they may be handled in the same way, and later included in any update to this appendix. The DBCT and IRT (delegated by the DBCT) may use risk assessment scores or any other tool that quantifies possible risk of harm to the record subjects in determining the risk of harm and the level of risk for the identified harms.

b. If, upon review of the available information, the DBCT determines that it needs more information to determine if there is a possible misuse of the data to the potential harm of the record subjects, the level of risk associated with the data breach under review, or which services, if any, to offer 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.

c. If the DBCT decides that the data breach may involve issues that may be more appropriate for action or review by other VA officials, the DBCT may refer the matter to those officials for whatever action they consider appropriate. The DBCT is not responsible for any actions or lack of actions taken by other VA officials after such a referral.

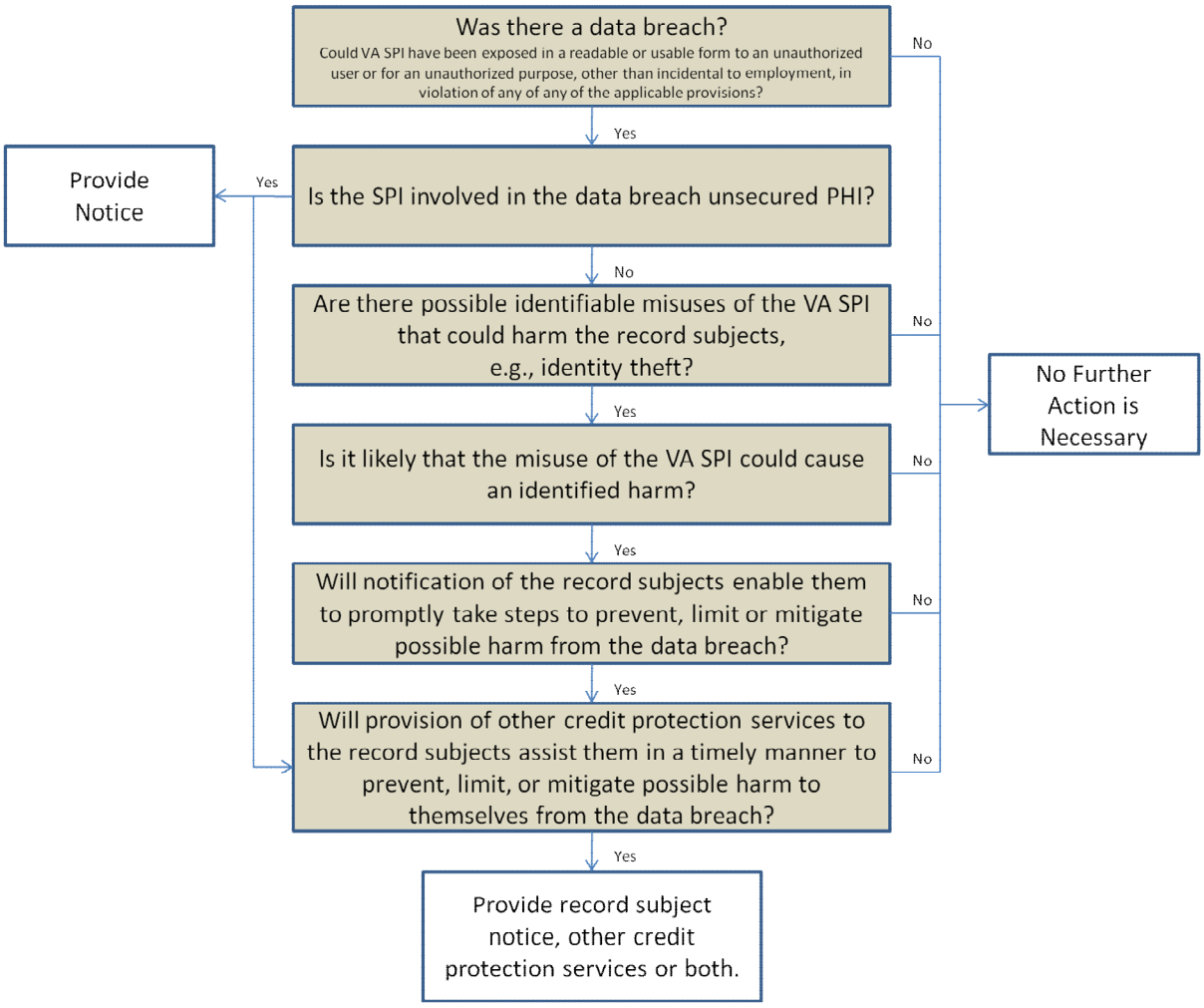

Figure A-1: Flow Chart of Credit Protection Service Sequence

4. FACTORS FOR DETERMINING THE LEVEL OF RISK FOR POTENTIAL MISUSE AND HARM ASSOCIATED WITH COMPROMISED VA SPI

a. The DBCT considers the following list of factors in determining whether there is a risk of potential harm to the subjects of VA SPI after a data breach, the level of that risk, and whether VA should provide notice or offer credit protection services to individuals whose VA SPI was compromised. The DBCT will determine the weight to be assigned to each of the factors in making these decisions under the totality of the circumstances and all information available to the DBCT at the time it reviews the data breach.

b. The nature of the data elements involved in the data breach is the first factor. The nature of the data elements also includes the context in which the data is contained when compromised, e.g., in a VHA Patient's medical health record or a Veterans' claim file. Examples of data elements include:

(1) Full name;

(2) Date of birth;

(3) Full social security number;

(4) Place of birth;

(5) Mother's maiden name;

(6) Identifying biometric information.

c. The second factor that the DBCT considers in determining the level of risk for potential misuse and harm is the likelihood that the information is or was physically and logically accessible to, and usable by, unauthorized individuals.

d. The third factor is the likelihood that the SPI is at risk, or the same information held by another entity, may be, or has been, misused by unauthorized individuals. This factor may depend, in part, upon the data elements that were compromised in the data breach.

e. The fourth factor that the DBCT considers is the range of harms to the record subjects that may be associated with misuse of the lost or compromised SPI. The potential harm to the record subject may be financial, reputational or some other type of harm. The DBCT may consider identified harms arising from other misuses of similar data, including non-VA data.

f. The fifth factor the DBCT considers is how offering credit protection services, including notification, may prevent misuse of the data, limit or mitigate the harm to the record subjects that may be associated with the misuse, or enable or assist the record subjects to achieve either or both of these goals. The DBCT considers actions that the record subjects may take themselves after notification to prevent, limit or mitigate possible harm to themselves from the data breach.

g. Additionally, the DBCT will consider the factors listed in 38 C.F.R. §§ 75.114-116 and the preamble to those rules published in the Federal Register at 72 Fed. Reg. 34395 (2007). Significant factors not previously stated include:

(1) The results of data mining or data breach analysis;

(2) The time the data has been out of VA control**;**

(3) Number of individuals affected or potentially affected;

(4) Identification of factors relating to potential risks and harms;

(5) The ability of the unauthorized user to compromise the confidentiality or integrity of the data, i.e., logical or physical access;

(6) Determination of whether the disclosure was to an entity that is required by law to provide the same or a similar level of protection to the data; and

(7) Evidence that the data or the same or similar data from other sources may have been the target of unlawful acquisition.

h. In summary, the factors are considered by the DBCT to determine whether the records in the incident identify the record subject or would permit an unauthorized individual who accesses the records to distinguish, trace, or learn the record subject's identity, either from the information involved in the breach, or from that information used with other information that is generally, publicly available, and then use that information to the potential harm of the record subject. The DBCT then decides whether offering credit protection services will help prevent, limit, or mitigate such potential misuses.

5. DECISION APPEAL PROCESS

a. VA components may appeal a decision by the DBCT to provide notification or an offer of credit protection services to the individuals whose data was involved in the data breach. Upon receipt of an appeal of an earlier DBCT decision, the DBCT will determine whether to sustain, reverse, or modify the earlier decision based upon the information contained in, or presented with, the appeal.

b. The DBCT may grant an appeal if new facts are presented that demonstrate (1) a data 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, in rare cases, (3) VA can no longer tell whom to notify of the breach (this would not apply for breaches of 10 or more individuals involving PHI for the notice would be via the Web or media outlets in compliance with the HITECH Breach Notification Rule).

6. SPECIFIC INCIDENT CATEGORIES INVOLVING VA OFFERS OF NOTIFICATION AND CREDIT PROTECTION SERVICES

a. Notification and credit protection services to the record subjects are not required if SPI is accessed or obtained by, or provided to, an individual, agency, business, or other entity that is a VA employee, or an employee or agent of a non-VA entity when the involved individuals or entities need to see SPI to perform assigned responsibilities (if a VA employee), or duties under a contract or agreement (if not a VA employee).

b. VA normally does not have to notify record subjects or offer them other credit protection services when VA inadvertently provides SPI to a HIPAA covered health care provider, or an trusted entity that provides services either to the health care provider or patients, if VA confirms that the recipient destroyed the SPI after receipt and did not share the data with any other individual or entity. For example, VA would not have to notify the patient if a VA Medical Center (VAMC) faxed a prescription to one branch of a chain pharmacy instead of the branch that the patient expects to fill the prescription.

c. Each incident type has a decision matrix that identifies situations in which VA previously determined whether notification or offering credit protection services is appropriate. However, because each security or privacy incident is fact-specific, new incidents in the situations displayed in the matrices may present unique facts that require a different result from that displayed. Further, as technological capabilities change and become available, the decision to notify record subjects, offer them credit protection services, or both, may also change. The answer in a matrix, either "Yes" or "No," reflects the

decision by the DBCT under 38 U.S.C. § 5724 and VA regulations whether a data breach involves the following:

(1) There is at least a reasonable risk that an unauthorized individual who obtains the data may use the listed data elements to harm the record subject, and

(2) Notifying the record subjects of the data breach, offering credit protection services to them, or both, may assist the individuals in preventing, limiting, or mitigating the damages from misuse of the data.

7. GENERIC DATA DISCLOSURES

a. Matrix D-1 lists SPI data fields for which VA has decided whether the Department must notify the record subject of the breach, or offer credit protection services, regardless of the type of security or privacy incident in which the confidentiality of the data fields was compromised. Matrix D-1 applies to data breaches involving all storage media (electronic, paper, etc).

b. The reference to PHI in the matrices refers to PHI that does not contain the specific identifying information that would put a person at risk for identity theft yet still risks information that would violate privacy. Basically, in the matrices, PHI means VHA individually-identifiable health information that has been stripped of obvious identifying data elements (such as name, date of birth, SSN), but contains other identifying information. An example would be a patient's telephone number or serial number on a medical device along with information about the VHA patient.

Matrix A-1: Notification or Credit Protection Services for Specific Data Elements Involved in Any Type of Data Breach

Type of Information Exposed	Notification Only Warranted	Credit Protection Warranted
Full Name only	No	No
Full Name and Date of Birth	No	Yes
Full Name and Home Address	Yes	No
Full SSN	No	Yes
Full Name and Partial SSN	Yes	No
Full Name and PHI, including acct #s or disability codes	Yes	No
Partial SSN only	No	No
Other PII	To be determine by DBCT	No

(1) **Note 1**: If the record subject of a data breach is a deceased Veteran and the answer in the "notification warranted" column is yes, VA sends a next-of-kin letter to the next of kin of record. An offer of credit protection services is not required to individuals who are next-of-kin of a deceased Veteran unless the data of the next-of-kin was the subject of a data breach or the information about the deceased individual could be used to harm the next of kin.

(2) **Note 2**: A "yes" answer in the "notification warranted" column means that the responsible VA entity must notify the record subject of the data breach, if the DBCT so warrants. Where the breach involves PHI, the notification letter is to provide the notice required under the HIPAA Privacy and Security Rules and the HITECH Breach Notification Rule, if applicable.

(3) **Note 3:** Other PII as defined in Terms – page D2 Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, such as his or her name, SSN, or biometric records, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date or place of birth or mother's maiden name.

c. The reference to PHI in the matrices refers to PHI that contains information that identifies the record subjects but does not contain specific identifying information that could lead to identity theft. In these situations, SPI refers to the following data elements: full name and date of birth, full name and home address, or full SSN. PHI refers to unencrypted, individually-identifiable PHI. If the data involved in the data breach is unencrypted VHA PHI, VA may have to provide HIPAA notice.

8. EQUIPMENT

a. It is VA policy that VA facilities, contractors, and BAs will report in a timely manner 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, USB device, PDA, Smart phones, blackberry device, i-Pad, and other similar devices. VA must report this unaccounted for, stolen, or missing equipment to Congress, even if VA determines that the devices do not contain SPI. VA does not have to report to Congress any lost, stolen, or missing equipment if VA determines that any storage capability on the equipment was encrypted with an encryption application approved by the Office of Cyber Security (OCS), but missing equipment is still reportable to VA upper management.

b. Unaccounted for equipment is IT equipment that the facility lists on its inventory which has not been assigned to a specific employee or location and cannot be located. There must be no evidence that someone stole the equipment.

c. Stolen equipment is equipment that 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 removed from a work station. There should be affirmative evidence that would lead a reasonable individual to conclude that 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.

d. 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 A-2: Unaccounted for, Missing or Stolen Equipment and SPI		
Equipment Contents	**Notification Only Warranted**	**Credit Protection Warranted**
Unaccounted for, missing or stolen equipment that does not contain SPI.	No	No
Unaccounted for, missing or stolen equipment that contains encrypted SPI.	No	No
Unaccounted for, stolen or missing equipment with SPI not encrypted.	Refer to Matrix A-1	Refer to Matrix A-1
Unaccounted for, stolen or missing equipment that is not encrypted and contains SPI that is PHI other than full social security number, or full name and date of birth or home address.	Refer to Matrix A-1	No

9. E-MAIL: It is VA policy that, before transmission, e-mail containing VA SPI will be encrypted with encryption application certified by NIST as FIPS 140-2 compliant and approved by OCS, unless a waiver has been obtained from the VA CIO. The Department has identified specific encryption applications that must be used with VA data. E-mail 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 e-mail.

Matrix A-3: Notification or Credit Protection Services for SPI contained in compromised E-mails		
E-mail Contents	**Notification Only Warranted**	**Credit Protection Warranted**
E-mail does not contain SPI	No	No
Encrypted E-mail containing SPI sent inside or outside VA to a trusted recipient	No	No
Unencrypted E-mail containing SPI sent to an un-trusted recipient inside or outside VA	No	Refer to Matrix A-1
Unencrypted E-mail containing only PHI sent to an un-trusted recipient inside or outside VA	Refer to Matrix A-1	No
Unencrypted E-mail containing SPI sent to a trusted Recipient inside or outside VA	No	No

10. MIS-MAILING

a..The mis-mailing category consists of all hard-copy materials sent through a third-party 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 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 in route such that someone other than the correct addressee or sender may view SPI. The category includes one type of electronic communication: sending SPI by fax.

b. 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.

c. "Trusted entity" has the same meaning as under Matrix A-3, compromised e-mails.

Matrix A-4: Notification or Credit Protection Services for SPI contained on compromised hard copy format sent through a third party carrier.

Hard-Copy Mail Event	Notification Only Warranted	Credit Protection Warranted
VA container, e.g., envelope, containing SPI sent to incorrect address: returned unopened	No	No
VA container containing SPI sent to incorrect address: Opened by Un-trusted recipient	Refer to Matrix A-1	Refer to Matrix A-1
VA container containing SPI sent to incorrect address: Opened by Trusted recipient	No	No
Damaged container- SPI Content Exposed to Un-trusted Entity	Refer to Matrix A-1	Refer to Matrix A-1
Damaged container- SPI Content Exposed to Trusted Entity	No	No
Container or content lost or damaged in route – no SPI	No	No
Container with SPI content lost in route – Name and date of birth or home address	Refer to Matrix A-1	Refer to Matrix A-1
SPI faxed to wrong location (trusted entity)	No	No
SPI faxed to wrong location (not trusted entity)	Refer to Matrix A-1	Refer to Matrix A-1

11. MIS-HANDLING

a. It is the policy of VA to handle documents that contain SPI in a secure manner so that the information is not improperly exposed. This consists of items such as prescriptions, logs, health records, billing/financial documents, employee/staff sensitive information, and other day to day sensitive business communications containing SPI that VA uses.

b. There are incidents in which the SPI is found un-exposed: 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, for example subway cars and restaurants.

Matrix A-5: Notification or Credit Protection Services for SPI contained on storage media that are mis-handled by a VA or trusted entity		
	Notification Only Warranted	**Credit Protection Warranted**
Readable SPI contents exposed only to VA employees or trusted entity staff.	No	No
Readable contents not exposed.	No	No
Readable SPI contents exposed to anyone else.	Refer to Matrix A-1	Refer to Matrix A-1
PHI and Full name exposed.	Refer to Matrix A-1	No

12. UNAUTHORIZED ACCESS: Unauthorized access to SPI is access to SPI in violation of any of the applicable confidentiality statues. Such access may include two situations.

a. The first is access to SPI by an unauthorized user, that is, someone who does not have VA permission to access the information or has not met the requirements to access the data, such as no background investigation if required, or both.

b. The second situation is access to SPI by someone who has met all requirements to access the data, but accesses SPI for an unauthorized purpose.

Matrix A-6: Unauthorized access to SPI or access for an unauthorized purpose		
Unauthorized Access/Purpose	**Notification Only Warranted**	**Credit Protection Warranted**
VA employee/trusted entity accesses SPI without authorization and when investigation reveals malicious intent.	Refer to Matrix A-1	Refer to Matrix A-1
VA employee/trusted entity accesses SPI without authorization and with malicious intent	No	Refer to Matrix A-1
VA employee/trusted entity accesses SPI for an unauthorized purpose.	Refer to Matrix A-1	Refer to Matrix A-1
Non VA employee/non trusted entity accesses SPI.	Refer to Matrix A-1	Refer to Matrix A-1
Non VA employee/non trusted entity accesses SPI and has full name and partial SSN only.	Refer to Matrix A-1	No

13. IMPROPER DISPOSAL

a. Improper disposal covers those situations in which storage media containing SPI are compromised at any time between release by a VA office or any component of an authorized and trusted third party, 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 CBOC in a commercial location or a hard drive containing SPI on excess VA computer equipment.

b. SPI is considered compromised whenever the information was available in a readable or usable form, e.g., unencrypted electronic data, to unauthorized individuals (individuals who are not permitted to see the SPI for any reason), whether employees or not, and individuals who may be authorized to see the SPI for some purpose, but see the information during activity unrelated to the purpose for which they are authorized to see the data.

Matrix A-7: SPI compromised during disposition in violation of VA disposal requirements		
Unauthorized disposal procedure	**Notification Only Warranted**	**Credit Protection Warranted**
Readable SPI accessible only by VA/trusted entity employees other than individuals involved in disposal process.	No	No
Readable SPI accessible by Non VA employee/non trusted entity and evidence that SPI accessed without authorization but no evidence that SPI removed	Refer to Matrix A-1	Refer to Matrix A-1
Storage media with readable SPI accessible by anyone and evidence that SPI may have been removed.	Refer to Matrix A-1	Refer to Matrix A-1
Readable SPI and has full name and partial SSN is accessible by Non VA employee/non trusted entity without authorization.	Refer to Matrix A-1	No

APPENDIX B
ROLES AND RESPONSIBILITIES

1. INTRODUCTION. This appendix identifies the organizational roles of VA, Under Secretaries, Assistant Secretaries, and Key Officials, VA-NSOC, Veterans Affairs Office of Acquisitions, DBCT, RMIR, CIOs, IRT, POs, ISOs, Supervisors, and Users of VA information and information systems.

2. ROLES AND RESPONSIBILITIES TABLES

TABLE B-1	SECRETARY
Role	**Responsibilities**
Incident Preparation	1. Delegate that the Offices of OIT RMIR and the Office of Cyber Security will provide policy, procedures, and adequate resources to the POs and ISOs in the field for handling 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 PII.

TABLE B-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. 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.
Incident Prevention	4. Implement and comply with all VA policies, directives, and Handbooks on privacy and records management regarding the use, disclosure, storage, transmission, and protection of VA information in their organization.

TABLE B-3	VA-NSOC
Role	**Responsibilities**
Incident Preparation	1. Maintain contact information for team members and others within and outside VA, such as law enforcement (OIG) and other incident response teams. 2. Ensure the field has appropriate incident response mechanisms, such as phone numbers, e-mail addresses, and tools available to report suspected incidents. 3. Ensure that VA-NSOC staff is adequately trained to handle 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 pro-active and effective in bringing abnormal conditions to the attention of the right

TABLE B-3 VA-NSOC	
Role	**Responsibilities**
	people in a timely manner. 6. Ensure that owning organizations have an after-action report process in place to look at root causes and future prevention mechanisms. 7. Ensure that 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.
Incident Detection	10. Provide incident management systems and procedures expertise. 11. Configure and maintain monitoring capabilities of enterprise security systems.
Incident Analysis	12. Provide a central coordination and incident management function for all incidents affecting VA. 13. Validate that the occurrence of a data breach event is an incident. VA-NSOC will attempt to validate all reported events in order to eliminate false positives. Validation will be via an investigative process and contacts. VA-NSOC may request logs and other information in order to further validate the event. 14. If it is determined to be an incident involving a data breach, ensure that an Incident Tracking Ticket is created and notify the IRT.
Incident Documentation	15. Track the progress of response activity via a security event trouble ticket, if the event is determined to be a data breach, and performing all necessary documentation of incident progress. 16. Update records about the status of incidents, along with other pertinent information.
Incident Notification	17. Alert appropriate personnel about the potential or actual incident in a timely manner. When required, or appropriate, notify the: 18. Critical Infrastructure Protection Service (CIPS) Director. 19. Affected Network ISO/PO. 20. Facility ISO and Technical point of contact (POC). 21. Chief Information Officer (CIO), Network CIO. 22. Others as appropriate, e.g., US-Computer Emergency Readiness Team (US-CERT), OIG, Law Enforcement. 23. VA OIG hotline if criminal activity is involved. 24. IRT, ISO, and PO for incidents involving data breaches.
Containment Strategy	25. Suggest a remediation strategy. 26. Coordinate, with IRT, the response efforts. 27. Coordinate with network ISO and local ISOs and others as appropriate (e.g., US-CERT, law enforcement (OIG), Office of Cyber Security). 28. Prepare situation updates on status throughout response efforts. 29. Recommend and coordinate containment actions.

TABLE B-3	VA-NSOC
Role	**Responsibilities**
	30. Perform scans as necessary.
Evidence Gathering and Handling	31. Assist law enforcement or the OIG with the collection of evidence. 32. Document all evidence collected and preserved, including compromised systems. 33. Consult and coordinate with the OIG.

TABLE B-4	Office of VA Acquisitions
Role	**Responsibilities**
Preparation	1. In accord with VA Handbook 6500.6, ensure that all contracts in which any VA-owned information, especially PII maintained by contractors 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 B-5	INCIDENT RESPONSE GOVERNANCE BOARD (IRGB)
Role	**Responsibilities**
Preparation	2. Approve goals for implementation and guide integration of incident response with an emphasis on performance metrics. 3. Ensure VA-wide incident response policies are aligned with the Secretary's goals and objectives and support OIT objectives related to IT. 4. Establish and maintain formal and informal incident response communication channels with stakeholders throughout the organization. 5. Set high level compliance doctrines across the organization.
Incident Analysis	6. 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.

TABLE B-6	DATA BREACH CORE TEAM (DBCT)
Role	**Responsibilities**
Oversight	1. Oversee the Data Breach Incident Resolution Process. 2. Adjudicate specific data breaches to determine impact and reporting requirements.
Incident Preparation	3. Provide advance planning, guidance, analysis, and recommendations to the VA Chief Information Officer (VA CIO), Regional Directors, local Directors, and VA senior management to properly address and mitigate incidents involving the loss or compromise of data within VA custody. 4. Draft monthly, quarterly, and ad hoc reports to Congress.
Incident Prevention	5. Ensure that policies and directives regarding data confidentiality and protecting data from the risk of exposure to identity theft are up-to-date.
Incident Prioritization	6. Provide administrative oversight of incident reporting involving the loss or

TABLE B-6	DATA BREACH CORE TEAM (DBCT)
Role	**Responsibilities**
	compromise of data. 7. Has the authority and responsibility to escalate any incident, regardless of the risk assessment.
Incident Notification	8. When required, notify the Secretary, Inspector General, the Office of Management and Budget, the Committees on Veterans' Affairs of the Senate, House of Representatives, and other federal agencies that the Secretary considers appropriate. 9. 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. 10. 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 synopses. These reports will be used to conduct a preliminary data breach analysis in order to make risk-based decisions regarding data breaches, potential identity theft, risk mitigation, and follow-up actions. 11. In the event of a data breach that requires an independent risk analysis, then issue instructions regarding mitigation of associated risk, and concur with, or recommend, corrective actions to prevent a breach recurrence. 12. Teams within the DBCT will assist in analyzing, addressing, and mitigating data 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. 13. Teams within the DBCT are responsible for responding to data breaches and handling notification requirements from a collaborative perspective, whereby responsible parties will work together in formulating plans and sharing best practices. 14. Prepare the Monthly Report and Quarterly Notice to Congress on Data Breaches. This reports the number of incidents involving exposure of SPI categorized by Veterans Health Administration (VHA) Veterans Integrated Service Networks (VISN), Veterans Benefits Administration (VBA) regions, and all others. It also identifies the incidents that do not meet the notification timeframe.
Containment Strategy	15. Coordinate and advise in the execution of the containment strategy and efforts at the national level. 16. Make decisions about containment actions. 17. Determine need for initial notification and credit protection offers to individuals affected by breaches. 18. Coordinate response actions until the incident is resolved. 19. Report to senior VA officials on the status of the incident.

TABLE B-7	RISK MANAGEMENT & INCIDENT RESPONSE (RMIR)
Role	**Responsibilities**
Oversight Support	1. Implement and follow up on decisions of the DBCT. 2. Confer with other VA Senior Management officials and/or external authorities on SPI breaches that have unique circumstances. 3. Report to the IPRM Deputy Assistant Secretary (DAS).
Incident Analysis	4. Perform data breach analysis upon request. 5. Manage contracts for all credit protection services, including data breach analysis and independent risk assessment.

TABLE B-8	CHIEF INFORMATION OFFICERS (CIO)
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 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.
Incident Detection	11. Implement enterprise tools in a timely fashion. 12. Provide consistent monitoring and automated alert implementation. 13. Maintain a strong working relationship with staff to encourage reporting of incidents/suspected incidents.
Incident Analysis	14. Maintain pertinent information including, but not limited to, audit and event logs as well as user account information when appropriate.
Incident Documentation	15. Provide updates to open incidents as directed. 16. Provide input as required in any documentation requested from top management both inside and outside the medical center. 17. Safeguard data and sensitive information related to the incident.

TABLE B-8	CHIEF INFORMATION OFFICERS (CIO)
Role	**Responsibilities**
	18. Ensure that access to incident data is properly restricted.
Containment Strategy	19. Coordinate and advise in the execution of the containment strategy and efforts at the regional and local levels. 20. Make decisions about containment actions. 21. Coordinate response actions until the incident is resolved. 22. Report to senior VA officials on the status of the incident. 23. Work with the OIT staff to assure containment actions are performed in a timely and efficient manner. 24. Safeguard the integrity of involved hardware/software as appropriate.
Evidence Gathering and Handling	25. Preservation of hardware/software as appropriate and requested. 26. Preservation of audit and event logs as appropriate.
Corrective/Mitigation Action	27. Balance mission needs with recommended risk mitigation. 28. Owns the restoration plan. 29. Coordinate with Network ISOs, PO, and staff to implement eradication and remediation actions. 30. Assure response actions are carried out by Local Area Network/Wide Area Network (LAN/WAN) managers. 31. Implement recommendations as appropriate. 32. Maintain a record of costs associated with repair, restoration, business disruption, and labor.
Lessons Learned	33. Participate with the facility incident response staff in a post mortem review of all documentation surrounding the incident/suspected incident. 34. Implement “best practices” as appropriate based on the review.

TABLE B-9	INCIDENT RESOLUTION TEAM (IRT)
Role	**Responsibilities**
Incident Analysis	1. Identify incidents involving data breaches by performing a daily evaluation on incidents from the Incident Tracking Tool (ITT). ITT is the generic term used for VA incident tracking database system. 2. Coordinate and manage activities during incidents involving a data breach. This includes providing credit monitoring service promotion codes within 48 hours of a request from the PO for the code. 3. Produce and maintain an incident communication plan coordinated with Office of Public Intergovernmental Affairs (OPIA), Office of Congressional Legislative Affairs (OCLA), and Office of General Counsel (OGC) as necessary. 4. 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 data breach. 5. Facilitate and participate in incident reviews.

TABLE B-9	INCIDENT RESOLUTION TEAM (IRT)
Role	**Responsibilities**
	6. As necessary, ensure that a non-VA entity conducts an independent risk analysis (IRA) to determine the level of risk for potential misuse of any SPI involved in the data breach. 7. If a reasonable risk exists for the potential misuse of SPI, VA shall provide credit protection services in accordance with regulations prescribed by 38 U.S.C. § 5721-28. 8. Contract for an IRA where warranted. 9. Coordinate with other VA offices, as well as regional and local Incident Resolution Teams to assure the appropriate risk-based, tailored response for identity theft or privacy violation incidents within VA. 10. Work closely with other federal agencies, offices, and teams. 11. 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	12. Maintain records about the status of each incident, along with other pertinent information. 13. Maintain a detailed log of actions, as necessary, taken by all parties working the incident. 14. Produce management information as necessary for breaches that have unique circumstances. 15. Produce incident progress updates, as necessary for breaches that have unique circumstances.

TABLE B-10	PRIVACY OFFICERS (PO)
Role	**Responsibilities**
Incident Preparation	1. Take appropriate privacy and security training. 2. Obtain and maintain an ITT account and develop familiarity with the system. 3. Review VA Handbook 6502.1, ITT. 4. Review Privacy Violation Tracking System 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.
Incident Prevention	9. Implement Departmental and appropriate Administration privacy policies and procedures. 10. Establish an internal privacy audit program. 11. Monitor and report that individuals in their organizations complete the appropriate annual Privacy training program(s). 12. Ensure that privacy issues and concerns are communicated to and coordinated with appropriate parties.

TABLE B-10 PRIVACY OFFICERS (PO)	
Role	**Responsibilities**
	13. Become aware of the systems in their organizations that collect and/or maintain PII. 14. Participate in the filing and updating of Privacy Impact Assessments for systems within the purview of their organizations. 15. 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 contained in an official SOR. 16. Promote activities to foster privacy awareness (e.g. Privacy Day or Information Protection Awareness Week.)
Incident Detection	17. Receive complaints from Veterans or anyone within their organization who believes a privacy incident has occurred. 18. Enter all complaints received into the system allotted for the reporting of privacy events within 1 hour of discovery. 19. Follow guidance provided by the VA Privacy Service in order to record all privacy events in the system allotted for the reporting of privacy complaints or violations. 20. Monitor all privacy violations that they have entered into the system allotted for the reporting of privacy events. 21. Provide updates to the system allotted for the reporting of privacy events, as appropriate.
Incident Documentation	22. Enter updates to the system used for the reporting of privacy/security complaints or violations, as necessary, for any incident with a status of "Open". 23. ISOs and POs receive an e-mail 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. 24. Tickets will be reviewed at least every 72 hours for updates. 25. The POs should immediately update the risk assessment with new information about the incident as soon as it becomes available.
Incident Notification	26. Notify and keep local management and support staff apprised of the incident. 27. Prepare Incident Notification/Credit Monitoring Letters for signature 28. Obtain Promo Codes for Credit Monitoring Letters when applicable
Containment Strategy	29. Participate in initiating containment actions. 30. Suggest alternate containment actions, as necessary.
Restoration	31. Ensure timely closure of incidents.
Evidence Gathering and Handling	32. Direction will be provided by VA-NSOC, law enforcement, or the OIG. 33. Begin fact-finding investigation once initial complaint is logged into PETS/Remedy. 34. Consult with law enforcement or the OIG as necessary. 35. Log all comments and details of their investigation into PETS or the system designated for the reporting of privacy complaints and incidents.

TABLE B-10	PRIVACY OFFICERS (PO)
Role	**Responsibilities**
Lessons Learned	36. Log resolution of incident. 37. Raise user awareness through lessons learned.

TABLE B-11	INFORMATION SECURITY OFFICERS (ISO)
Role	**Responsibilities**
Incident Preparation	1. Obtain and maintain Remedy user accounts and obtain training in Remedy and Risk Assessment. 2. Enter all reported incidents into the ITT within one hour of receiving or identifying an incident. 3. Complete a risk evaluation at the time of reporting the incident and update information on each incident accordingly. 4. Complete appropriate privacy and security training. 5. Become aware of the security laws, regulations, and policies that apply to the organization. 6. Ensure that individuals within the organization know who their ISOs are. 7. Become familiar with and establish a working relationship with the PO, CIO and OIT staff for the organization.
Incident Prevention	8. Advise users on proper security protocols to prevent incidents. 9. Provide training to staff on their roles in preventing, reporting, and handling low-level security incidents. 10. Ensure systems and subsystems affected by incidents are isolated and, if necessary, are restored and/or rebuilt. 11. Provide local organization policy and procedures for reporting and handling incidents. 12. Ensure all users complete the VA Privacy and Security Awareness and Rules of Behavior training annually. 13. Ensure VA National Rules of Behavior are signed annually.
Incident Detection	14. Initiate protective measures when an incident or vulnerability is discovered. 15. Ensure incidents are properly reported, responses are coordinated, and incident updates are provided as required. 16. Coordinate with the PO to determine if a detected or reported security incident is also a privacy incident.
Incident Documentation	17. 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”. 18. ISOs and POs will also receive an e-mail 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. 19. Tickets will 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.
Incident Notification	20. Notify and keep local management and support staff apprised of the incident.

TABLE B-11	INFORMATION SECURITY OFFICERS (ISO)
Role	**Responsibilities**
Containment Strategy	21. Participate in initiating containment actions. 22. Suggest alternate containment actions, as necessary.
Evidence Gathering and Handling	23. Direction will be provided by VA-NSOC, law enforcement, or the OIG. 24. Begin fact-finding investigation once initial complaint is logged into the ITT. 25. Consult with law enforcement or the OIG as necessary. 26. Log all comments and details of their investigation into the ITT or the system designated for the reporting of privacy complaints and incidents.
Lessons Learned	27. Log resolution of incident. 28. Raise user awareness through lessons learned.

TABLE B-12	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 Rules of Behavior (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 all subordinates complete the required Privacy and Information Security Awareness and Rules of Behavior training annually.
Incident Detection	6. Ensure incidents are properly reported, responses are coordinated, and incident updates are provided as required.

TABLE B-13	USERS
Role	**Responsibilities**
Incident Preparation	1. Complete mandatory security training and privacy training on an annual basis. 2. Sign the VA National Rules of Behavior annually.
Incident Prevention	3. Be alert to their surroundings and report any suspected incidents to their respective 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,

TABLE B-13	USERS
Role	**Responsibilities**
	ISO, and supervisor (and VA law enforcement as necessary). After normal business hours, notify the VA-NSOC.

APPENDIX C
INCIDENT RESOLUTION TEAM PROCESS

1. PURPOSE

a. This appendix establishes processes for managing data breaches involving Sensitive Personal Information (SPI) under the ownership of VA, including assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness.

b. The primary goal in managing data breaches is to provide prompt and accurate notification and remediation, if necessary, to those individuals whose SPI may have been, as a result of an incident, accessed, used, or disclosed in a manner not permitted by the applicable confidentiality provisions to whom such access, use, or disclosure poses a risk of financial, reputational, or other harm. Another significant goal is to ensure continued public trust in VA as the guardian of the SPI with which we have been entrusted. Note that SPI includes Protected Health Information (PHI), which is covered under the HIPAA Privacy Rule, as well as certain other types of Personally Identifiable Information (PII).

c. Prompt notification and remediation also involves close coordination, both within VA through the activities of the IRT and with entities outside of VA, such as, the OMB and Congressional committees. This section of the Handbook provides guidelines to enhance coordination efforts for greater efficiency, accuracy, and promptness in communicating with individuals affected by VA data breaches.

2. BACKGROUND

a. OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification, (Sept. 20, 2006), recommended that agencies implement response structures for the prompt response and resolution of incidents potentially leading to identity theft. As a result, VA established a national IRT to support local and regional Data Breach Mitigation teams for the management of VA data breaches.

b. Compliance with the following laws, regulations, and policies is provided through the processes outlined in:

(1) OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Attachment 3: External Breach Notification (May 22, 2007).

(2) Department of Veterans Affairs Information Security Enhancement Act of 2006, Pub. Law 109-461, 120 Stat. 3450, codified at 38 U.S.C. §§ 5721-28, and its implementing regulations, 38 C.F.R. §§ 75.111-119.

(3) HITECH Act, Pub. L. No. 111-5, 123 Stat. 260, codified at 42 U.S.C. § 17932, and the Breach Notification Rule, 45 C.F.R. § 164.400-414.

3. SCOPE

a. These processes apply to all VA offices and personnel, including federal employees, contractors, researchers, students, volunteers and other individuals who use or interface with VA information or

information systems. This Handbook is addressed particularly to the members of the IRT and the staff of the facility experiencing the incident who have the responsibility to respond to, resolve, and follow up on any breach of SPI that impacts VA.

b. This appendix will detail the following process steps that the team uses in managing data breaches:

(1) Incident response

(2) Incident resolution: and

(3) Incident closure/lessons learned

c. These three steps are the last steps of the overall VA incident management process, depicted in Figure C-1.

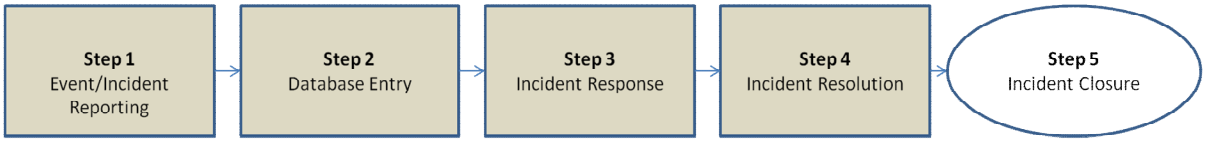

Figure C-1: VA Incident Management Procedure

4. DBCT DATA BREACH INCIDENT PROCESS OVERSIGHT STRUCTURE

a. VA Handbook 6500, *Information Security Program*, describes the responsibilities of VA senior officials, information owners, and information system users in VA incident management. In addition, Appendix B of this document contains the roles and responsibilities of the DBCT, which apply to the DBCT Data Breach Incident Response Oversight process, illustrated in Figure C-2 below.

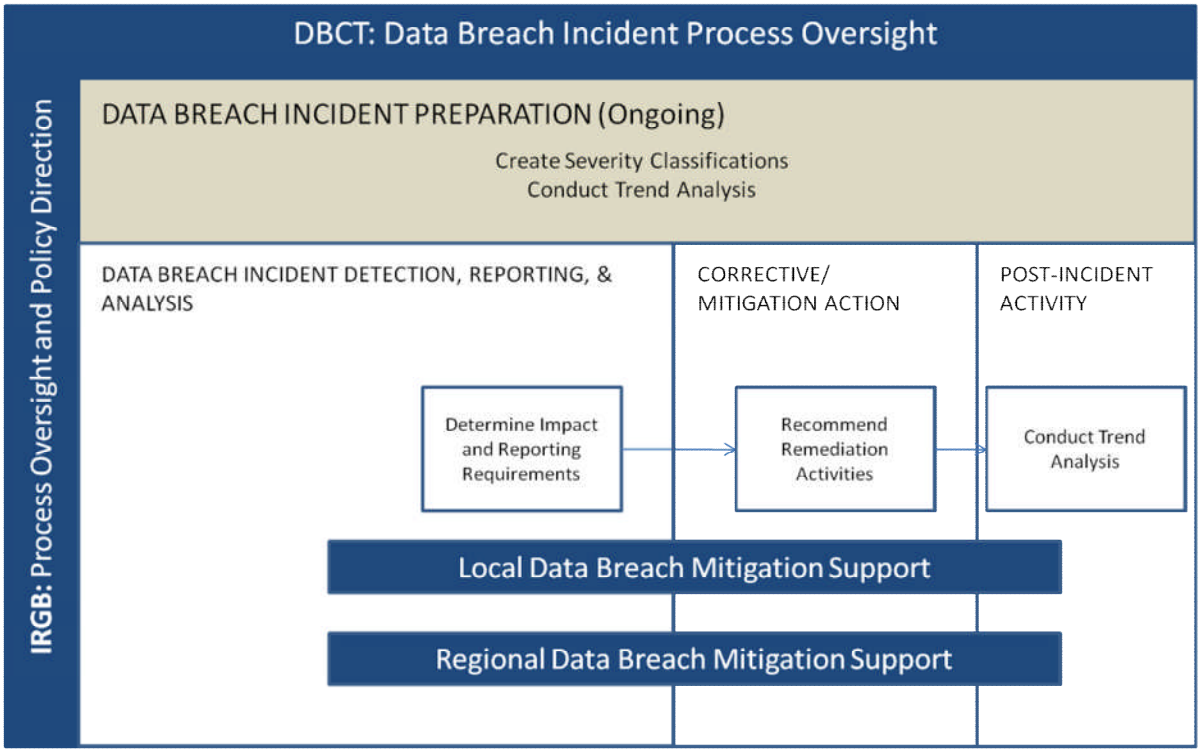

Figure C-2: DBCT Data Breach Incident Process Oversight

b. Laws, policies, and other authorities were developed to establish clear and proper procedures deterring and responding to data breaches. 38 U.S.C. §§ 5721-28 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).

c. 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 data breach:

(1) Notification

(2) Data mining

(3) Fraud alerts

(4) Data breach analysis

(5) Credit monitoring

(6) Identity theft insurance

(7) Credit protection services

5. MANAGEMENT PROCESS

a. **Incident Response**

(1) The VA incident management process begins with local ISOs and POs who verify potential data breach events as incidents, record them in either the VA-NSOC Remedy or PETS databases, as appropriate, and complete the risk assessment. These databases are managed by the VA-NSOC. After these first two steps are completed, the mitigation teams at the local, regional, and national levels manage the response to the incident. Figure C-3 depicts the decision-making process that takes place within the IRT in addressing data breaches.

(2) At the local and regional/VISN levels, mitigation teams may convene any time there is a verified data breach. The chair of the meeting oversees discussion of the breach, based upon the information entered in the VA-NSOC/PETS 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 VA-NSOC/PETS ticket.

b. **Database Incident Review**. The IRT reviews the entries in the VA-NSOC/PETS database daily, evaluate them for clarity and internal consistency, and determining whether or not further action is required to resolve the incident or mitigate potential harm. The DBCT review process is covered in Appendix A. Those entries that warrant the DBCT's attention are reviewed at the weekly DBCT meeting. The DBCT may request follow-up information.

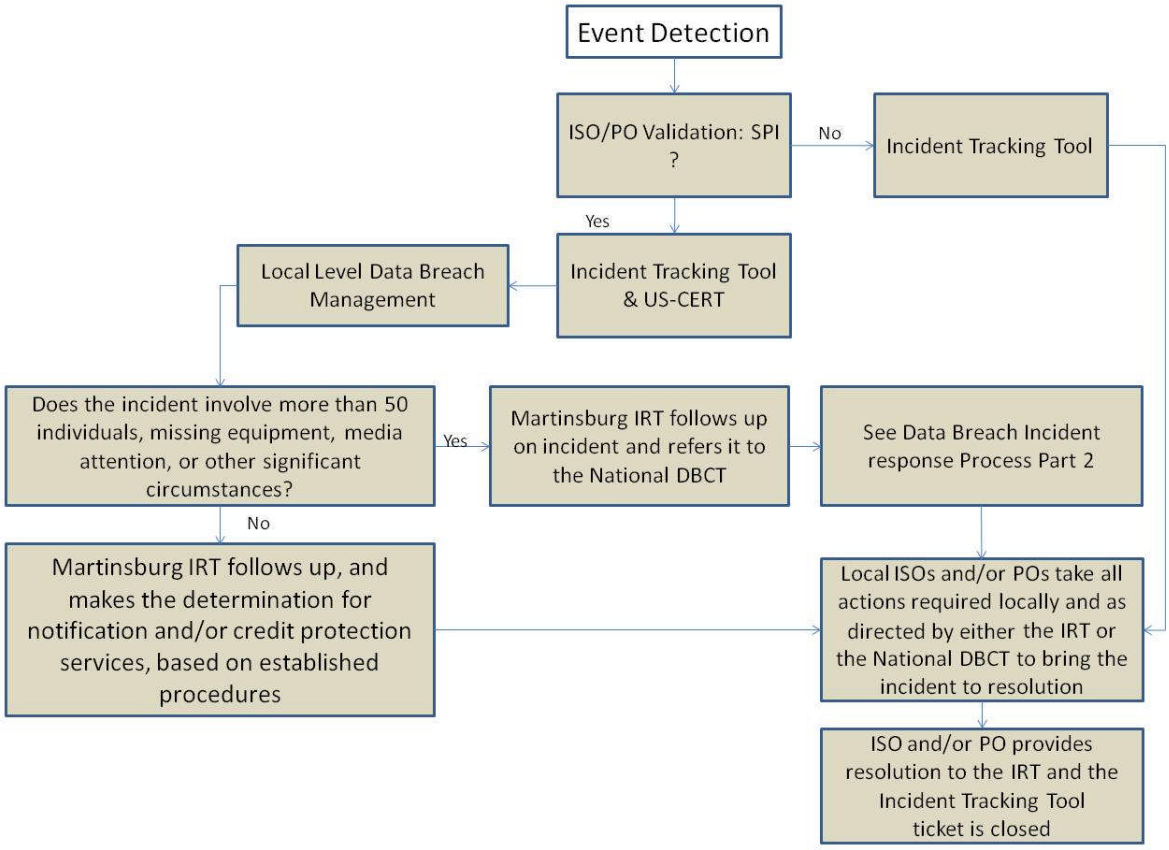

Figure C-3: Data Breach Incident Response Process (Part 1 – IRT)

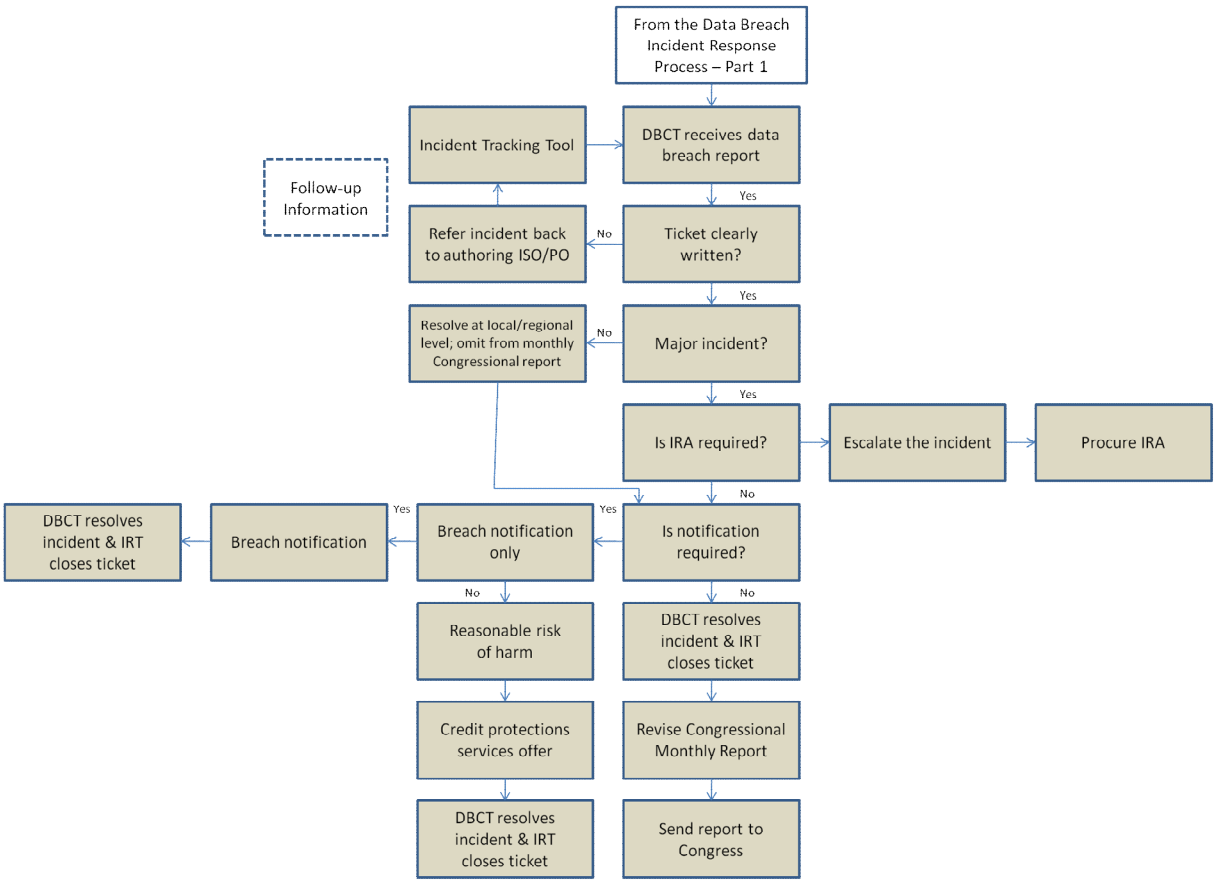

Figure C-4: Data Breach Incident Response Process (Part 2 - DBCT)

c. **Independent Risk Analysis (IRA) Requirement**. The requirement is to review each incident to determine if an IRA is required per 38 U.S.C. § 5724(a).

d. **IRA Waived**. Pursuant to 38 C.F.R. § 75.114, VA may waive an IRA and proceed with offering credit protection service under three circumstances (known as "Accelerated Response").

e. **DBCT Considerations**. If the DBCT (as empowered by the Secretary and VA CIO) determines that there is an "immediate, substantial risk of identity theft of the individuals whose data was the subject of the breach." In determining whether there is such an immediate, substantial risk, the DBCT shall consider:

(1) The nature and content of the lost, stolen or improperly accessed data, *e.g.*, the data elements involved, such as name, social security number, date of birth;

(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 ASCII, or in 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.

f. **Notification.** If a prior IRA conducted for VA on a breach of the same or similar data concluded that credit protection services should be offered; or if a private entity with a similar breach would be required under federal law to provide notification for the individuals affected.

g. **Substitute IRA.** VA may also rely on the results of a prior risk assessment on a breach involving same or similar data or circumstances to conclude that credit protection services are not warranted.

h. **IRA Required**. When an IRA is required, the VA RMIR will obtain an IRA from an independent source (e.g. a contractor, another Federal agency, or VA Office of Inspector General pursuant to 38 U.S.C. § 5724(a)).

i. **Notification Determination**

(1) The IRT will use the Daily Incident to make preliminary assessments of incidents. The DBCT will review each data breach report and make a categorization determination using the criteria in the decision tree categories, which are provided in Appendix A. The result will be a report that the DBCT will use to identify appropriate response activities and determine if notification is required. (See Appendix A).

(2) 38 C.F.R. §§ 75.114 to 75.118 specify the factors that should be addressed in an IRA and the factors that shall be considered when considering notification to individuals external to VA. In determining whether the data breach resulted in a reasonable risk for the potential misuse of the compromised SPI, the DBCT shall consider all factors considered relevant to the decision, including:

(a) The likelihood that the SPI will be or has been made accessible to and usable by unauthorized persons;

(b) Known misuses, if any, of the same or similar SPI;

(c) Any assessment of the potential harm to the affected individuals provided in the risk analysis;

(d) 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;

(e) 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

(f) 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

1. Contents of the notification, pursuant to 38 C.F.R. § 75.117, must include:

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

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

c 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;

d What steps individuals should take to protect themselves from potential harm, if any

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

2. Contact procedures for those wishing to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, web site, and/or postal address; and

a 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 instruction for obtaining other credit protection services offered under this subpart.

3. In addition to notification of a breach the DBCT may find that other protection services, such as the following, should be provided:

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

b. Data breach analysis

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

d. One year of identity theft insurance.

e. 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.

(3) The DBCT will log, track, and close (when complete) routine incidents with established remediation processes. The DBCT will report (escalate) non-routine incidents requiring senior leader involvement to the appropriate Administration for review, action, and follow-up reporting.

j. **Type of Notification Determination.** If notification is required, the DBCT determines what the notification should contain and the method of delivery pursuant to the requirements of 38 C.F.R. § 75.117. (See Appendix A, DBCT Review Process, and Appendix D, VA Process for Compliance with HITECH Act.)

k. **Monthly Report to Congress on Data Breaches**. The IRT prepares the Monthly Report to Congress on Data Breaches for submission to Congress (see below, Communicating with Congress). The following types of data breaches are examples of what should be retained on this report:

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

(2) 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;

(3) Incidents involving 50 or more individuals.

l. **Incident Resolution:** Incident resolution is the process of implementing action items to resolve information breaches, mitigate potential harm, institute corrective actions, and ensure the public's continued trust in VA. Much of incident resolution involves proactive external communication ~ first to the people whose information was involved in the incident then to Congress and the public. In addition to communication, prompt remediation actions, such as offering credit protection services for affected individuals, are critical.

(1) Obtaining Contact Information

(a) It is the responsibility of local sites to contact the individuals affected and to report out when completed. The PO can look for individuals contact information in the system of records. PO shall not go to next of kin for the information.

(b) 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.

(c) VBA uses SHARE and the contact information is cross referenced with the Social Security and/or CAPRI databases to check accuracy. In some cases, the Veteran's banking institution needs to be contacted to validate current address information.

(d) 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. Addresses of Veterans are collected to ensure NCA is providing service within 75 miles of 75% of the Veteran population. The contact information is kept in readable format and is retrievable from the BOSS/AMAS system.

(e) VHA uses their applications such as CPRS for obtaining, storing, and maintaining Veterans' contact information. The information is verified each time Veterans receive services from VHA.

(f) In those instances where there is insufficient or out-of-date contact information that precludes direct written notification to an individual subject to a data breach, 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 affected individuals likely reside. Such a notice must include a toll-free phone number where an individual can learn whether or not his or her personal information might have been involved in the data breach. See 38 C.F.R. § 75.117(b).

(2) External Communications

(a) Communicating with Individuals. Communication with individuals directly affected by an incident 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 and prepared by the PO or a Facility Director's designee with guidance from the IRT.

(b) All communication with Congress should take place through the Office of Congressional and Legislative Affairs.

m. **Communicating with the General Public.**

(1) In accordance with the HITECH Breach Notification Rule, and to achieve greater transparency, several data breach reporting measures have been adopted for incidents involving individually identifiable health information maintained by VHA to complement existing procedures.

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

(b) A toll free phone number will be established for data breach incidents potentially involving more than 500 individuals. When one occurs the number is activated and posted, along with notification to the media as required by HITECH, on the VA Notices web page. Interested/concerned parties can go to the web page and call to ask questions relating to the media notification.

(2) Media communications with the public concerning incidents are coordinated through the associated VA Office of Public and Intergovernmental Affairs (OPIA). VA staff and contractors should not speak directly to members of the press about any data breaches but refer all inquiries to OPIA.

n. **Procurement of Remediation (Credit Protection) Services**

(1) VA RMIR 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.

(2) When the DBCT determines that a notification letter or an offer of credit protection services is needed the local facilities' PO or Facility Director Designee, 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 redacted copy will be attached in the tracking system, mailto: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 Remedy. 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 30-day turnaround time for notifying Veterans.

(3) The template letters are available on the RMIR Incident Response Webpage. Letters must be mailed within 30 days from the date the incident occurred.

(4) The VA OIT 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.

(5) Codes are requested by the PO by sending an e-mail to *VA Identity Safety* (vaidentitysafety@va.gov). *VA Identity Safety* provides codes to the PO. The following information must be included on the e-mail request for codes:

(a) Number of codes needed (based on the total number of living individuals impacted by the incident

(b) Facility responsible for the incident

(c) The SOC ticket number of the incident

(6) Additional information about a given incident may become available after the DBCT has made a decision on the incident. In such a case, the person responsible for the incident ticket may appeal the decision by e-mailing (mailto:VAIRCTMailbox@va.gov) Appeals must be made within 10 days of the

DBCT's initial decision using the Appeals Request form which can be found on the RMIR Webpage. The DBCT will review the appeal and VA-NSOC will notify the requester of the decision.

o. Incident Closure. The DBCT make the final determination that an incident is closed and IRT staff notes the closure in the VA-NSOC/PETS database. Generally, an incident may be considered closed when either 1) the DBCT determines that no further action is needed, or 2) all affected individuals have been notified and/or offered remediation in response to the DBCT's decision on the incident, and the responsible facility official has sent a copy of the redacted letter to the DBCT mailbox.

APPENDIX D

VA Process for Compliance with HITECH Act

1. VA HITECH Compliance Overview

a. HITECH stands for the Health Information Technology for Economic and Clinical Health Act. The Act is part of The American Recovery and Reinvestment Act (ARRA) of 2009. The breach notification rule implementing provisions of the HITECH Act include certain requirements for covered entities and business associates regarding the handling of data breaches, such as issuing a local news release and submitting information to HHS for its Web posting in certain incidents. The HITECH Breach Notification Rule applies only to HIPAA-covered entities, such as VHA, and its business associates, but VHA's response to data breaches under the Rule is coordinated by the DBCT and the IRT, which have been designated by the VA CIO to work closely with VHA and its business associates in taking actions necessary to comply with the Rule.

b. A toll free phone number will be established for data breach incidents potentially involving a large (500+) number of individuals. When one occurs the number is activated and posted, along with a HITECH Press Release, on the VA Notices web page http://www.va.gov/about_va/va_notices.asp. Interested/concerned parties can go to the Web page and call to ask questions relating to the incident.

c. Approved letter templates and press release templates are available to Privacy Officers (PO) and Public Affairs Officers (PAO) at the RMIR Webpage.

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. The local media do not have to publish; however, VHA must provide it to them for publication.

e. If there is an incident involving 500 or more individuals, the IRT must notify the Office of Congressional and Legislative Affairs (OCLA) as soon as possible, so it can notify the Committees on Veterans' Affairs of the House and the Senate within 72 hours. Also, VHA executives inside these distribution lists have requested the same level of notification: VHA 10N Action, VHA 10A Action, VHA Hot Media, VHA 10B, VHA 19 Privacy Issues, VHA HITECH Press.

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

2. Individual, Media and Health & Human Services (HHS) Data Breach Reporting Process

a. The following defines the process within VA for reporting data breaches to the individual, the media, and HHS to meet HITECH requirements, which apply only to unsecured VHA Protected Health Information (PHI) covered by the HIPAA Privacy and Security Rules. Only breaches that expose the individual to significant risk of financial, reputational, or other harm and do not fall under one of the enumerated exceptions require notice under HITECH.

b. Unsecured protected health information is protected health information 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 Health and Human Services (HHS) in guidance. This guidance will be updated annually and available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

c. To comply fully with the HITECH Act and the Breach Notification Rule, in addition to notice to the subjects of the breach, HHS must be notified about significant breaches involving VHA unsecured PHI. In certain circumstances, media outlets must be notified, and information must be posted on the VA web page.

d. The process for notifying individuals, pursuant to 45 C.F.R. § 164.404, is located on the RMIR Webpage.

e. **Required Notification Elements.** The 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;

(2) description of the types of information that were involved in the breach;

(3) steps affected individuals should take to protect themselves from potential harm;

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

(5) contact information for the covered entity.

f. **Substitute Notice to Individuals.** If VA cannot find a valid, current address for individuals whose unsecured PHI is involved in a data breach, VA must provide substitute notice to them. If VA does not have valid, current addresses for fewer than ten individuals involved in the breach, VA may provide an alternative form of written notice, or notice by telephone or other means. If VA does not have valid, current addresses for ten or more individuals, VA has to 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, VA also has to provide a toll-free number for at least 90 days, so the individual can learn whether his or her data was the subject of the data breach.

g. **Notification to HHS**. HHS must be notified of any data breach involving the 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 data breaches is posted on the HHS web site. For breaches involving fewer than 500 individuals VA 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.)

h. **Notification to the Media**. If the data breach involves unsecured PHI of 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.

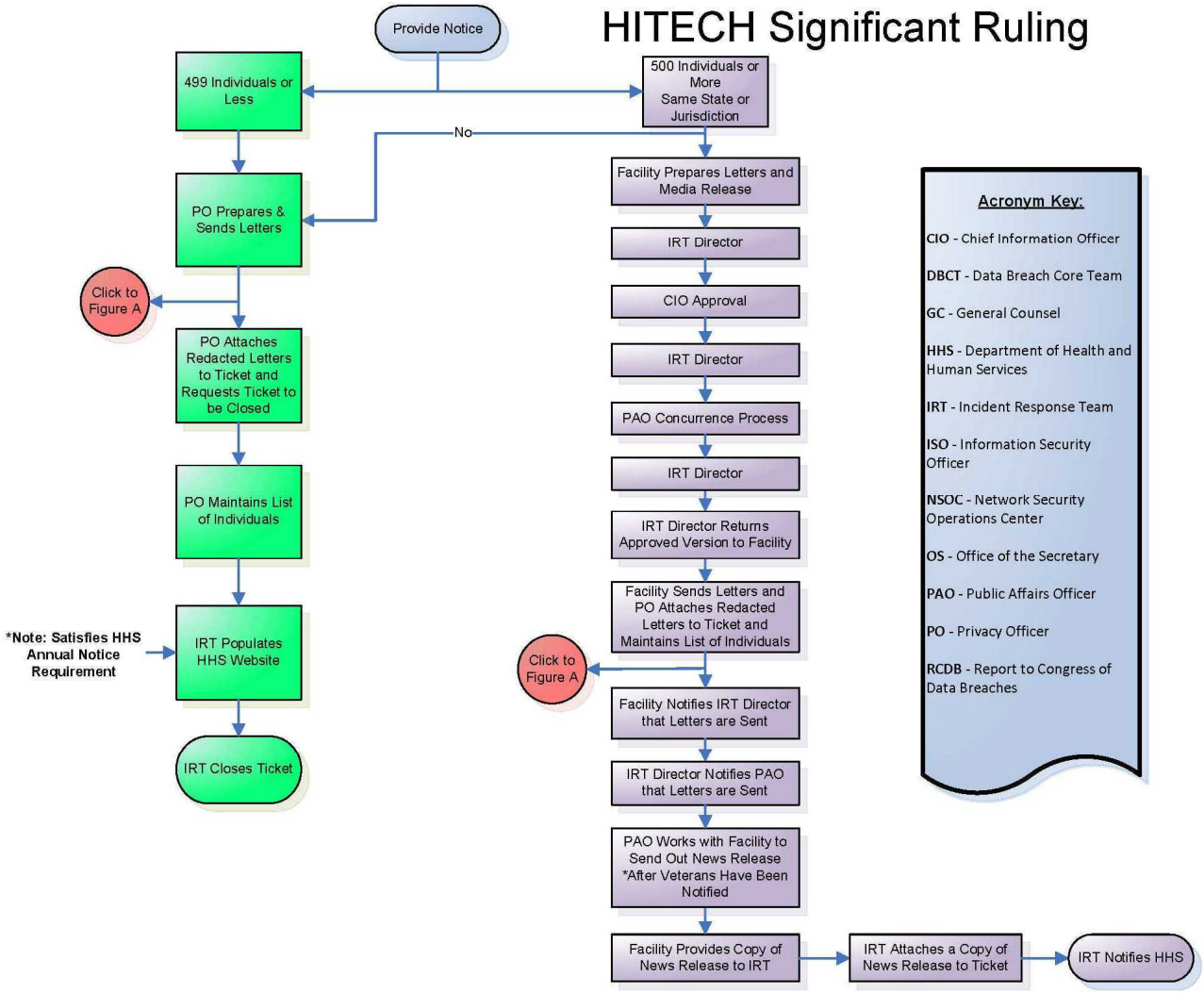

Figure D-1: HITECH Significant Ruling Flow Chart

3. HITECH Significant Ruling Notification Process

a. **The HITECH Significant Ruling process.** This identifies the notification procedure that is followed when an incident has been determined to involve PHI. The narrative breaks out the process into 4 distinct areas:

(1) Those incidents involving fewer than five hundred (500) individuals and for those involving five hundred (500) or more individuals who are not in the same state or jurisdiction. This is the section of the flowchart colored in green (Figure D-1).

(2) Those incidents involving five hundred (500) or more individuals located in the same state or jurisdiction. This is the section of the flowchart colored in light purple (Figure D-1).

(3) The Conspicuous Posting / Substitute Notice area which is colored in red (Figure D-2).

(4) The non-HITECH section which is colored in blue (Figure D-3).

b. **Individual Notification of fewer than 500 individuals.** Figure D-1 demonstrates the process used when immediate notification to HHS is not required. These incidents are reported as part of the annual report to HHS.

(1) The local PO completes and mails notification letters, using the DBCT-provided template letter, to the individuals affected by the breach.

(2) A redacted letter is attached to the ITT for archival purposes, along with mitigating and corrective actions taken.

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

(4) Entering the incident on the HHS website satisfies the requirement for annual reporting under HITECH to Health & Human Services (HHS). The annual method of reporting requires that all breaches from the prior year are entered into the HHS website by 1 March of the current year. The reporting may be made annually or on a rolling basis. For incidents involving fewer than 500 individuals, NSOC will submit the information to HHS when the redacted letters are received and then will close out the ITT ticket.

c. **Individual Notification of 500 or more individuals.** Figure D-1 illustrates the process used when the incident affects five hundred (500) or more individuals. If the incident affects five hundred (500) or more individuals, notice to HHS must be provided when it provides notice to individuals. If the five hundred (500) or more affected individuals are within the same state or jurisdiction, VA must 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 and mail the Notification Letter(s), using the DBCT provided template letter, to the individuals affected by the breach (reference 1a). The facility Director, or their designee, signs the letter.

(a) The local PAO will prepare a news release using the OPIA news release template, 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 IRT/DBCT and VACO approval channels for processing.

(c) Once the package is approved, the local PAO will send out the news release and will 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.

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

(3) The local PO will email the news release to the IRT, and IRT will add it to the ITT ticket for archiving.

(4) IRT will submit the report to HHS, for incidents involving more than 500 individuals, within 60 days of the date that the incident occurred, but no later than when the individuals are notified, whichever is sooner.

(5) If law enforcement, including OIG, requests in writing a delay in notifications, then IRT will delay providing the notice for the time period specified by their request. Notification will be delayed for 30 days if the request is provided verbally. Documentation of written or verbal requests will be added to the Remedy ticket.

d. **Substitute Notice for fewer than 10 individuals without a valid current address.**

(1) Figure D-2 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 VHA Privacy.

(3) If there are fewer than 10 individuals without a valid current address, including those for whom letters were returned as undeliverable, a substitute notice will be provided.

(4) The substitute notice may be provided by an alternative form of written notice, telephone, or other means.

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

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

e. **Substitute Notice for 10 or more individuals without a valid current address.**

(1) Figure D-2 illustrates the process followed when substitute notice must be provided 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 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 the individual can learn whether their data was the subject of the data 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 VHA Privacy.

(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 website Webmaster.

(5) The VA Webmaster will post the summary write-up and notice on the VA department website. It will remain on the website for 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 IRT, and IRT will add the write-up and notices to the ITT ticket for archival purposes.

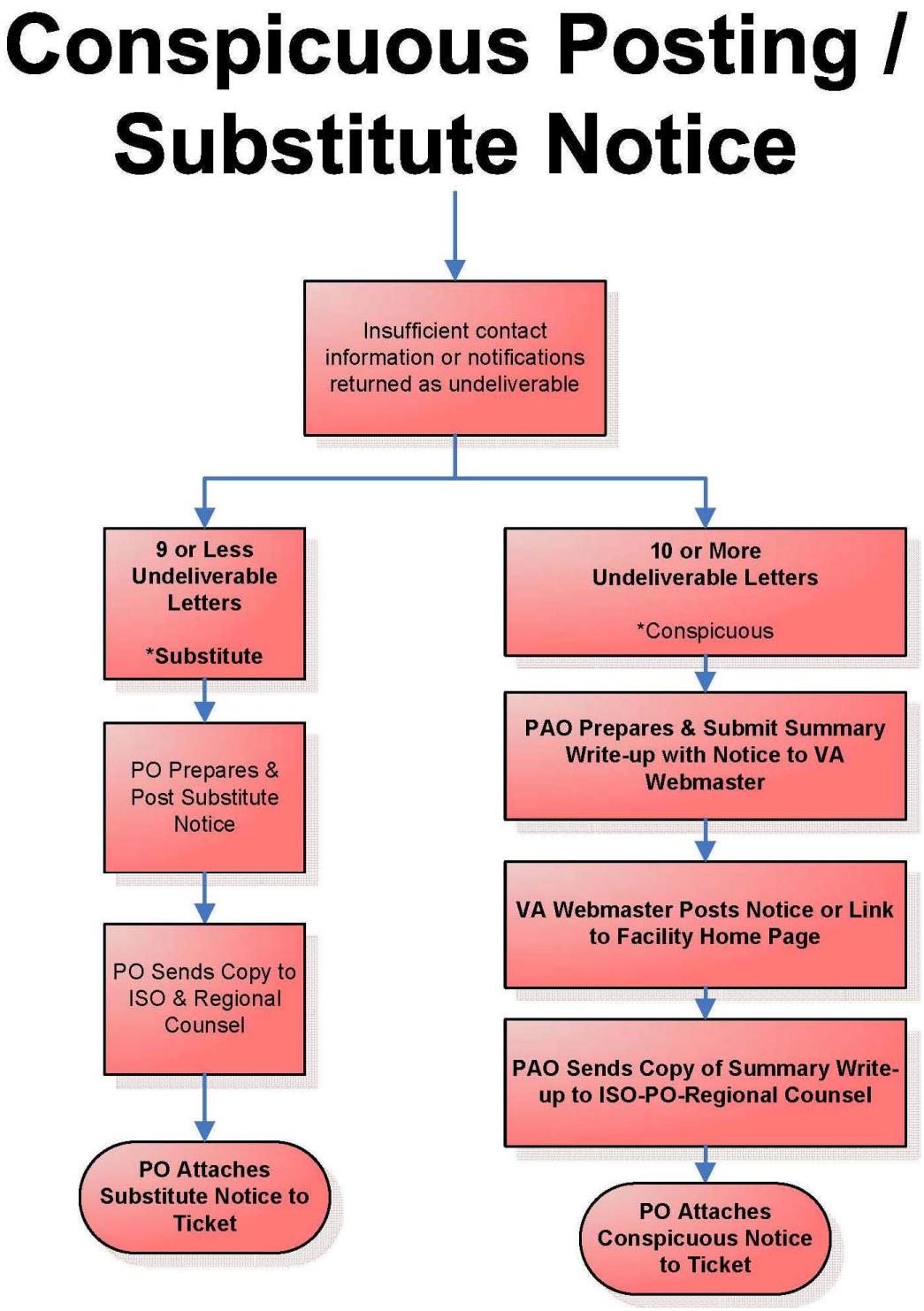

Figure D-2: Conspicuous Posting / Substitute Notice Flow Chart

f. **Non-HITECH Incidents** (See also Appendix A, Data Breach Core Team Review Process).

(1) The flowchart (Figure D-3) is the process used for those incidents that do not meet the standard for reporting under HITECH but have the potential to compromise the PII of individuals.

(2) The local PO completes and mails letters using the DBCT provided letter template to the individuals affected by the breach.

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

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

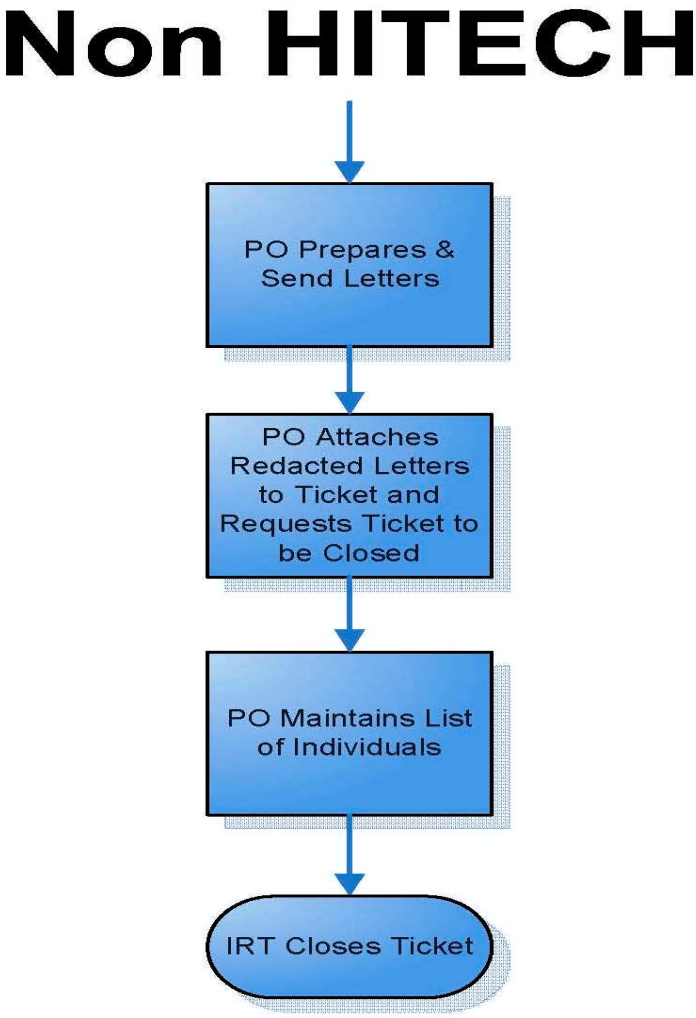

Figure D-3: Non-HITECH Process Flow Chart

4

. Breach Notification and the VHA PAO

a. HITECH requires sending a local news release and information to HHS for Web posting within 60 days if 500 or more people within a state or local jurisdiction are potentially exposed to a breach of their health information. 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 RMIR Incident Response Webpage. Sample news releases are available from OPA regional offices.

c. PAOs required to prepare a news release will receive one of two types of sample releases 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 information the law requires to be in individual letters of 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., full name, SSN, date of birth, address);

(3) Steps 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 at the facility where the incident occurred and who to contact for 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 OIT's IRT. 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 OGC, OIT, OCLA, OPIA, and OS/StratComm. When the news release has been approved and sent out, the PAO must give a copy to the facility privacy officer and identify the media outlet(s), to which it was sent. The PO sends it to the DBCT staff, which notifies HHS of the incident.

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

5. 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. 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. 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 qualifying written request to delay is received during that time.

APPENDIX E
REFERENCES

1. Statutes

a. 38 U.S.C. §§ 5721-28, Information Security.

b. Sections 13400-402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. Law No. 111-5, 123 STAT. 226, 260 (2009), codified at 42 U.S.C. § 17932.

c. 44 U.S.C. §§ 3541-49, Federal Information Security Management Act (FISMA) of 2002.

d. 5 U.S.C. § 552a, The Privacy Act.

e. 38 U.S.C. § 5701, Confidential Nature of Claims.

f. 38 U.S.C. § 5705, Confidentiality of Medical Assurance Records.

g. 38 U.S.C. § 7332, Confidentiality of Certain Medical Records.

2. Regulations

a. 38 C.F.R. §§ 75.111-.119, Data Breaches.

b. 45 C.F.R. Part 164, particularly §§ 164.400-.414, Notification in the Case of Breach of Unsecured Protected Health Information.

3. Office of Management and Budget Publications

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

b. Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006).

4. National Institute of Standards and Technology Publications

a. Special Publication 800-61, revision 1 (March 2008), Computer Security Incident Handling Guide.

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

5. Other References

a. Interim Final Rule for Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (Aug. 24, 2009).

b. 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 (April 27, 2009).

c. VA Directive and Handbook 6500, Information Security Program.

d. VA Directive 6502, Privacy Program.

e. VA Handbook 6502.1, Privacy Event Tracking System (PETS).

f. VA Directive 6509, Duties of Privacy Officers.

APPENDIX F
ACRONYMS

1. **CFR** – Code of Federal Regulations
2. **CIO** – Chief Information Officer
3. **DBCT** – Data Breach Core Team
4. **FIPS** – Federal Information Processing Standard
5. **HIPAA –** Health Insurance Portability and Accountability Act of 1996
6. **HITECH Act** – Health Information Technology for Economic and Clinical Health Act
7. **IRA** – Independent Risk Analysis
8. **IRGB** – Incident Response Governance Board
9. **IRT** – National VA Incident Resolution Team
10. **ISO** – Information Security Officer
11. **IT** – Information Technology
12. **ITIL®** – IT Infrastructure Library
13. **ITT** – Incident Tracking Tool
14. **LAN** – Local Area Network
15. **NCA** – National Cemetery Administration
16. **NCIO –** Network Chief Information Officer
17. **NIST** – National Institute of Standards and Technology
18. **NSOC** – Network and Security Operations Center
19. **OCLA** – Office of Congressional and Legislative Affairs
20. **OCS –** Office of Cyber Security

21. **OGC** – Office of General Counsel

22. **OIG** – Office of Inspector General

23. **OIT** – Office of the Assistant Secretary for Information and Technology

24. **OMB** – Office of Management and Budget

25. **OPIA** – Office of Public and Intergovernmental Affairs

26. **PAO** – Public Affairs Officer

27. **PETS –** Privacy Event Tracking System

28. **PHI** – Protected Health Information

29. **PII** – Personally Identifiable Information

30. **PO** – Privacy Officer

31. **RMIR** – Risk Management and Incident Response

32. **SDCT** – Service Disruption Core Team

33. **SPI** – Sensitive Personal Information

34. **SP –** Special Publication

35. **SPI –** Sensitive Personal Information

36. **SSN –** Social Security Number

37. **US-CERT** – United States Computer Emergency Readiness Team

38. **USC** – United States Code

39. **VA CIO** – VA Chief Information Officer

40. **VA-NSOC** – Veterans Affairs Network and Security Operations Center

41. **VA-RMIR** – VA Office of Risk Management and Incident Response

42. **VACO** –VA Central Office

43. VBA – Veterans Benefits Administration

44. VHA – Veterans Health Administration

APPENDIX G
GLOSSARY OF TERMS

1. USE: This glossary is the primary reference for terms used in the Handbook and its appendices.

2. SOURCES: Terms in this glossary incorporate, or are based upon, terms contained in the references listed in Appendix E and the Glossary of Terms for Notifications-Escalation ROAR Team (Oct 24, 2007). Wherever possible, IT Infrastructure Library (ITIL®) definitions are used with appropriate modifications to reflect the VA enterprise and US terminology. References and copyright acknowledgements as cited.

3. CONTACT: Forward all questions and suggestions concerning terms in the glossary to the VA Incident Resolution Team (Martinsburg, WV), RMIR.

4. TERMS

a. **Breach (of PHI under HITECH)**: The unauthorized acquisition, access, use, or disclosure of protected health information (PHI) in violation of the HIPAA Privacy Rule which compromises the security or privacy of such information by posing a significant risk of financial, reputational, or other harm to the individual, except:

(1) Any unintentional acquisition, access, or use of PHI by an employee, contractor, or other person acting under the authority of a covered entity or a business associate, 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 violation of the HIPAA Privacy Rule;

(2) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or a business associate to another person authorized to access PHI at the same covered entity or business associate, if the information received is not further used or disclosed in violation of the HIPAA Privacy Rule; or

(3) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

See 45 C.F.R. § 164.402. Is a subset of Data Breach under title 38.

b. **Business**: (Service Strategy) An IT Service Provider provides IT Services to a Customer within a Business. [ITIL®, v3 - abbreviated]

(1) Within VA, the term business is used in referring to both the operational business lines (i.e., VHA, VBA, and NCA) and the back office businesses (e.g., time and attendance,

contracting). It is important to identify clearly which business organization or function is meant as this will impact priority of response and resource allocation decisions.

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

(1) A health care provider that conducts certain transactions in electronic form,

(2) A health care clearinghouse, or

(3) A health insurance plan.

d. **Data (or Information) Breach (under title 38)**: The loss, theft, or other 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. See 38 U.S.C. § 5727. May or may not be a breach under HITECH.

e. **Data Breach Analysis**: The process used to determine if a data breach has resulted in the misuse of sensitive personal information.

f. **Data Breach Core Team**: The DBCT is the arm of the IRGB that has oversight responsibilities for data breaches. It adjudicates specific data breaches to determine impact and reporting requirements. It is a matrix structure from the local to the national level that operates both vertically and horizontally.

g. **Identity Theft**: A fraud committed using the identifying information of another person.

h. **Impact**: The effect of an IT incident on an organization. The level of effect is usually relative to the size of the organization and its resilience. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact. [Business Continuity Institute, *Glossary of General Business Continuity Management Terms*]

i. **Incident**: A discrete event in which VA SPI was the subject of a data breach as defined in this glossary.

j. **Incident Management**: (Service Operation) the Process responsible for managing the Lifecycle of all Incidents.

k. **Independent Risk Analysis:** an analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any VA sensitive personal information involved in the data breach.

l. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

m. **IT (VA)**: Within VA OIT

n. **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, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (See Sensitive Personal Information, below)

o. **Priority**: A Category used to identify the relative importance of an Incident, Problem, or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken. For example, the [*SLR*] may state that [*Incidents with a specific priority*] must be resolved within 12 hours. [ITIL®, v3 – modified] *See Impact, Urgency*

p. **Prioritization**: The ordering of critical activities and their dependencies are established during incident handling based on priority. The business continuity plans will be implemented in the order necessary at the time of the event. [Disaster Recovery Institute International, *DRJ Glossary* - modified] *See Impact, Urgency*

q. **Process Violation**: The proximate cause of a data breach was a breakdown of process under circumstances for which it is inappropriate to hold an individual directly responsible for the data breach. Individual training, informal counseling, and system improvement activities are normal responses to a determination that an actual or attempted data breach was the result of a process violation.

r. **Protected Health Information (PHI)**: Information that:

(1) Is maintained by a covered entity, such as a health care provider or a health plan;

(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) Identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

s. **Risk Assessment**: An analysis to determine the scope, likelihood, and severity of the results of a SPI breach, to determine its resolution at a local or regional level.

t. **Sensitive Personal Information (SPI)**: Information that:

(1) Is maintained by an agency;

(2) Is about an individual, such as education, financial transactions, medical history, protected health information, and criminal or employment history, and information that can be used to distinguish or trace the individual's identity (Personally Identifying Information – PII), including name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and

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

Includes records about individuals requiring protection under applicable confidentiality provisions.