MANAGEMENT OF BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION

1. **REASON FOR ISSUE:** This handbook provides revised policy and procedural guidance on the VA management of breaches involving VA Sensitive Personal Information (SPI). It implements the Privacy Act of 1974, 5 U.S.C. § 552a; 38 U.S.C. §§ 5721-28 and 38 C.F.R. §§ 75.111-119; section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (codified at 42 U.S.C. § 17932) and the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule at 45 C.F.R. §§ 164.400-414; Office of Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information; OMB Memorandum M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements; and Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.

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

   a. Establishes procedures for managing breaches and updates the criteria used to determine whether a reported incident is a breach involving VA SPI. Contains updated criteria used to determine whether VA should notify or offer credit monitoring services to individuals whose VA SPI is involved in a breach.

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

   c. Describes the processes VA has implemented to comply with all relevant breach response laws, regulations and policies, simultaneously with the most stringent provisions used, when applicable.

3. **RESPONSIBLE OFFICE:** Office of the Assistant Secretary for Information and Technology (005), Office of Compliance, Risk & Remediation (005X), Data Breach Response Service (005X6C) is responsible for the content of this handbook.

4. **RELATED DIRECTIVE/HANDBOOK:** VA Directive 6500, VA Cybersecurity Program; VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program.

5. **RESCISSIONS:** VA Handbook 6500.2, Management of Security and Privacy Incidents, dated March 12, 2019 and VA Handbook 6502.1, Privacy Event Tracking dated February 18, 2011, are rescinded.

Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6500.2
Transmittal Sheet
June 30, 2023

CERTIFIED BY:

/s/
Shana Love-Holmon
Acting Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt D. DelBene
Assistant Secretary for
Information Technology and
Chief Information Officer.

DISTRIBUTION: Electronic Only

MANAGEMENT OF BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION

TABLE OF CONTENTS

1. PURPOSE. 4
2. SCOPE. 4
3. BACKGROUND/OVERVIEW. 5
4. RESPONSIBILITIES. 7
5. BREACH MANAGEMENT PROCESS AND OVERSIGHT STRUCTURE. 22
6. VA CRITERIA FOR BREACH AND RISK ASSESSMENT 26
7. TABLETOP EXERCISE AND ANNUAL PLAN REVIEW 28
8. REFERENCES. 29
9. TERMS AND DEFINITIONS. 31
APPENDIX A - STANDARD RISK ASSESSMENT MATRICES 34
APPENDIX B – BREACH NOTIFICATION 44
APPENDIX C – HIPAA BREACH NOTIFICATION 50

MANAGEMENT OF BREACHES INVOLVING SENSITIVE PERSONAL INFORMATION

1. PURPOSE.

a. Updates VA Handbook 6500.2 to align with VA policy in VA Directive 6500, VA Cybersecurity Program and VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program.

b. Establishes associated breach management policies and assigns responsibilities for the oversight, management and reporting procedures to ensure appropriate and expeditious managing of breaches involving Sensitive Personal Information (SPI).

c. Provides the criteria used by Data Breach Response Service (DBRS) and the Data Breach Core Team (DBCT) to determine whether a reported incident is a breach involving SPI and whether the VA should notify or offer credit monitoring services to the record subjects.

d. Provides procedural guidance to Privacy Officers (PO), Information System Security Officers (ISSO) and others involved with the management of privacy and information security incidents. It does not contain the criteria used by the ISSO to report cyber security incidents unless SPI is involved.

2. SCOPE.

a. This handbook applies to all VA Sensitive Information (VASI), SPI, Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Federal Tax Information (FTI) and other Personally Identifiable Information (PII), subject to protection under the Privacy Act, title 38 confidentiality statutes and the HIPAA Privacy and Security Rules.

b. This handbook satisfies the Federal and statutorily requirements of:

(1) The Privacy Act, 5 U.S.C. § 552a, implemented at 38 C.F.R. §§ 1.575-1.582;

(2) 38 U.S.C. §§ 5721-28, implemented at 38 C.F.R., §§ 75.111-119;

(3) The HITECH Act § 13402 (codified at 42 U.S.C. § 17932);

(4) The HIPAA Breach Notification Rule, 45 C.F.R., §§ 164.400-414;

(5) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information;

(6) OMB Memorandum M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements;

(7) Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.

3. BACKGROUND/OVERVIEW.

a. This handbook applies to all VA employees, contractors, volunteers, trainees and students with access to VA information or information systems in order to perform their duties ("VA personnel"), as well as Veteran Service Organizations (VSOs), union officials and other non-VA individuals to whom such access is provided to support their representation of Veterans or employees with access to VA information or information systems in order to perform a VA-authorized activity ("trusted entities"). This handbook does not address VA's response to a data breach involving other VA sensitive data (not SPI), such as embargoed budget data.

b. VA has established breach management through prompt risk identification, subject notification and remediation for those individuals whose SPI may have been inappropriately accessed, used, or disclosed in a manner not permitted by applicable confidentiality provisions and to ensure continued public trust in VA as the guardian of SPI.

c. VA has established an approach to enhance coordination efforts for greater efficiency, accuracy and promptness in communicating within VA through the activities of the DBRS and the DBCT and with entities outside of VA, such as the Cybersecurity and Infrastructure Security Agency (CISA)/United States Computer Emergency Readiness Team (US-CERT), OMB and Congressional committees.

d. VA's DBRS tailors a response to a breach based on the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals. This handbook serves as the breach response plan for VA. The VA DBRS and the DBCT are authorized by the Secretary to respond to breaches involving SPI. The DBRS supports regional and local incident response teams for the management of VA breaches.

e. VA's breach management process incorporates compliance with all relevant breach response laws, regulations and policies, simultaneously with the most stringent provisions used when applicable, as explained below:

(1) 38 U.S.C § 5721-28 established information technology (IT) security requirements for VA SPI. The Act mandates procedures for detecting, immediately reporting and responding to security incidents, notifying Congress of any significant data breaches involving SPI and providing credit monitoring services to those individuals whose SPI may have been involved.

(a) 38 U.S.C. § 5724(b) prescribed regulations at 38 C.F.R. §§ 75.111-119, for the provision of credit monitoring services after the DBRS determines there is at least a reasonable risk of potential misuse of SPI involved in a breach.

NOTE: In the event of an incident, the DBRS may, as a matter of discretion, offer credit monitoring services even if no determination

has been made that it is legally required. The decision to provide credit monitoring services following a particular incident does not indicate VA has determined a reasonable risk exists for the potential misuse of the SPI involved in the incident and therefore a reasonable risk of harm to the affected party.

(b) 38 U.S.C. § 5724(c) requires the Department to prepare and submit a quarterly report to Congress regarding all data breaches involving SPI. The DBRS prepares and submits a quarterly report to Congress regarding all data breaches involving SPI.

(2) The HITECH Act §13402 (codified at 42 U.S.C. §17932) and the HIPAA Breach Notification Rule specified in 45 C.F.R. §§ 164.400- 414 require covered entities (CEs) and their business associates (BAs) to notify individuals of breaches involving their unsecured PHI. The VA DBRS provides breach incident response on behalf of Office of Information Technology (OIT), a BA of the Veterans Health Administration (VHA), the CE under the HIPAA rules.

(3) The Privacy Act, 5 U.S.C. § 552a, implemented by VA at 38 C.F.R. §§ 1.575-1.582, prohibits the disclosure of records about individuals without their authorization or some other exception and requires the safeguarding of an individual against an invasion of personal privacy. The DBRS reviews disclosure authority under the Privacy Act as part of the breach determination process.

(4) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, sets forth the policy for Federal agencies to plan for and respond to a breach of SPI, as well as guidance on whether and how to provide notification and credit monitoring services to those individuals. This handbook serves as the breach response plan for VA. The DBRS supports regional and local incident response teams for the management of VA breaches.

(5) OMB Memorandum M-22-05, Guidance on Federal Information Security and Privacy Management Requirements provides reporting guidance deadlines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The VA DBRS is the designated incident response service for breaches of VA information involving SPI.

(6) Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies provides guidance, as a condition of receiving FTI, requiring VA to establish and maintain, to the satisfaction of the IRS, certain safeguards designed to prevent unauthorized uses of FTI and to protect the confidentiality of the information. Upon discovering a possible improper inspection or disclosure of FTI, to include breaches or security incidents, VA personnel identified by the DBRS shall follow VA incident reporting procedures and contact the appropriate special-agent-in-charge, Inspector General for Tax

Administration (TIGTA) immediately, but no later than 24 hours, after identification of a possible issue involving FTI in accordance with IRS Publication 1075.

(a) An incident, as defined in OMB M-17-12, is any occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies.

(b) A breach, as defined in OMB M-17-12, is a loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

4. RESPONSIBILITIES.

a. **Under Secretaries, Assistant Secretaries and Other Key Officials.** The Under Secretaries, Assistant Secretaries and Other Key Officials have responsibilities under the incident preparation and incident prevention roles. The Under Secretaries, Assistant Secretaries and Key Officials shall:

(1) Implement and comply with all VA policies, directives, handbooks on information security, privacy and records management regarding the use, disclosure, storage, transmission and protection of VA information in their organization;

(2) Ensure VA policies, directives and handbooks related to data confidentiality and protecting data from the risk of exposure to identify theft meet all Federal requirements;

(3) Ensure regional and local Incident Response Teams (IRTs) are established within each organization in the event of a breach;

(4) Ensure users support and comply with the incident response process; and

(5) Ensure VA personnel using VA information or information systems take annual security and privacy training in accordance with VA policies.

b. **Senior Agency Official for Privacy and Chief Privacy Officer.** The Senior Agency Official for Privacy (SAOP) and the Chief Privacy Officer (CPO) have responsibilities under the incident preparation and incident prevention roles. The SAOP and CPO shall:

(1) Ensure oversight, coordination and facilitation of VA’s privacy compliance efforts;

(2) Ensure all VA Privacy Act System of Records Notices (SORNs) include routine uses for the disclosure of information necessary to respond to a breach;

(3) In coordination with the Head of Contracting Activity, ensure contract provisions to assist with the response to a breach are uniform and consistently included in VA contracts;

(4) Ensure VA's breach response plan and system security authorization documentation clearly define roles and responsibilities, to include contractors operating information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of SPI on behalf of VA;

(5) Identify logistical support to respond to a breach, including other Federal agencies that may support VA in the event of a breach;

(6) Ensures breach response team(s) assess the risk of harm for suspected or confirmed breaches;

(7) Ensure the development, implementation and review of VA's breach response plan and designation of VA's breach response team;

(8) Ensure personnel staffing the agency's security operations center are properly trained to identify a breach and that appropriate subject matter experts who can identify reporting requirements are part of the breach response team;

(9) Coordinate with identified agency officials to ensure law enforcement authorities (e.g., Office of Inspector General (OIG) and the Office of General Counsel (OGC) receive timely notification as appropriate;

(10) Review reports detailing the status of breaches, validate accuracy, identify lessons learned, implement specific, preventative actions reported and ensure documentation of changes and any challenges preventing VA from remedial measures; and

(11) Ensure documented review of VA's breach response plan confirms the plan is current, accurate and reflects applicable changes in law, guidance, standards, policies, procedures, staffing, or technology is included in applicable annual FISMA reporting.

c. **Director of the Data Breach Response Service (DBRS).** The Director of the DBRS has responsibilities under the oversight support, incident preparation, incident prevention, incident analysis, incident documentation and incident notification strategy roles. The Director of the DBRS shall:

(1) Ensure VA-wide incident response policies are aligned with applicable Federal law and guidance as well as the Secretary's and OIT's goals and objectives;

(2) Perform daily incident and breach analysis using the Privacy and Security Event Tracking System (PSETS);

(3) Implement and follow-up on decisions made by the DBCT;

(4) Report breaches involving VHA PHI to the Department of Health and Human Services (HHS);

(5) Provide advanced planning, guidance, analysis and recommendations to Key Officials, VA senior management officials, the SAOP, the CPO and external authorities to properly address and mitigate incidents and breaches;

(6) Establish and maintain formal and informal incident response communication channels with stakeholders throughout the Department;

(7) Draft quarterly and ad hoc reports to internal and external stakeholders, including Congress;

(8) Notify appropriate individuals within VHA when approaching the 60-calendar day notification turnaround time after a breach involving PHI;

(9) Respond to and address incident response issues and provide feedback on remediation strategy;

(10) Manage contracts for all VA credit monitoring services;

(11) Provide appropriate notification templates and credit monitoring service promotion codes, where applicable, within two business days from the date requested by the PO;

(12) Arrange for and manage an Independent Risk Analysis (IRA) when necessary, by a non-VA entity to determine the level of risk for a potential misuse of any SPI involved in a breach;

(13) Coordinate with other VA offices, as well as regional and local IRTs to ensure the appropriate risk-based, tailored response for breaches;

(14) Ensure internal stakeholders are aware of the appeal process for requesting reconsideration from the DBRS when they obtain new information about an incident;

(15) Ensure PSETS system captures a record of each incident to include status, detailed log of actions and all relevant information for each incident and maintain the record according to the appropriate records control schedule;

(16) Serve as liaison between functional areas affected to include VA organizations and certain non-VA entities such as OMB, the Government Accountability Office (GAO) and Congress;

(17) Issue instructions regarding mitigation of associated risk and concur with, or recommend, corrective actions to prevent a breach recurrence;

(18) Coordinate with the DBCT in analyzing, addressing and mitigating breaches to ensure timeliness, uniformity and visibility of VA responses;

(19) Collaborate and coordinate with the DBCT to respond to breaches and address notification requirements;

(20) Report to Congress on data breaches to include the number of involving exposure of SPI categorized by VHA Veterans Integrated Service Networks (VISNs), Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA) districts and all others;

(21) Annotate events as unable to notify or contact when there are circumstances where the Veteran's identity is not known or where all methods of contacting the Veteran have been exhausted and substitute notice is not warranted or would cause undue concern.

d. **Data Breach Core Team (DBCT).** The DBCT has responsibilities under the oversight, incident prioritization, incident notification and containment strategy roles. The DBCT shall:

(1) Be chaired by the Director of the DBRS and meet weekly at a minimum or as directed by the Chair;

(2) Provide guidance to the DBRS to ensure timeliness, uniformity and visibility of VA responses;

(3) Advise the DBRS in determining whether an incident has resulted in a breach, responding to a breach by providing notification or credit monitoring to affected individuals and collaborating with POs, ISSOs and program offices on response actions until the incident is resolved;

(4) Adjudicate appeals by program offices of breach determinations; and

(5) Escalate any incident to VA leadership, regardless of the risk assessment.

e. **VA-Cyber Security Operations Center (VA-CSOC).** The VA-CSOC has responsibilities under the incident prioritization, incident prevention, incident detection, incident analysis, incident documentation, incident notification, containment strategy and evidence gathering and management roles. VA-CSOC shall:

(1) Maintain contact information for stakeholders within and outside VA, such as OIG and other law enforcement entities;

(2) Ensure the field has appropriate incident response mechanisms, such as phone numbers, email addresses and tools available to report suspected incidents;

(3) Ensure VA-CSOC staff is adequately trained to prioritize incidents and to assist the field;

(4) Provide the necessary evidence collection, forensics, or containment actions as applicable;

(5) Ensure reporting and alerts are proactive and effective in bringing abnormal conditions to the attention of the right people in a timely manner;

(6) Collaborate with organizational stakeholders to develop an after-action report process to review root cause and future prevention mechanisms;

(7) Ensure incident escalation procedures are in place for reported events;

(8) Ensure processes are clearly written and updated on a regular basis as conditions or changes occur in strategies, organizations, people, or devices;

(9) Collaborate with Information Technology Development, Security and Operations (DevSecOps) to ensure only certified devices are placed into the operational enterprise and configurations are properly maintained to minimize potential compromise or other adverse events which could expose SPI to unacceptable risks;

(10) Perform scans as necessary;

(11) Provide incident detection capabilities, systems, procedures and expertise;

(12) Configure and maintain monitoring capabilities of enterprise security systems;

(13) Provide a central response coordination and incident management function for all incidents affecting the VA enterprise;

(14) Validate the occurrence of a breach involving a cybersecurity base event is an incident. VA-CSOC will attempt to validate all reported IT- based events to eliminate false positives. Validation will be via an investigative process. VA-CSOC may request additional logs and other information to further validate the event;

(15) Ensure a PSETS event is created for confirmed cybersecurity related incidents within one (1) hour of discovery by the PO or ISSO, as provided in Appendix D and notify the DBRS if an event is determined to be an incident involving an IT-based breach of VA SPI;

(16) Collaborate with POs and ISSOs, as necessary, to track the progress of response activity via PSETS. If the IT-based systems event is determined to be a breach, perform all necessary documentation of an incident’s progress;

(17) Update records about the status of IT-based system incidents, along with other relevant information;

(18) Alert affected Information System Security Managers (ISSMs) at the network/territory level, area ISSOs, POs, technical points of contact, Network Operations Manager and others as appropriate (e.g., US-CERT) about the potential or actual incident in a timely manner;

(19) Notify US-CERT and OIG of incidents involving IT-based systems;

(20) Direct a remediation strategy;

(21) Coordinate the response efforts with DBRS;

(22) Coordinate with ISSMs at the network/territory level, area ISSOs and as appropriate (e.g., US-CERT, OIG and law enforcement);

(23) Prepare situation updates on status throughout response efforts;

(24) Recommend and coordinate containment actions with appropriate staff;

(25) Coordinate and assist law enforcement or the OIG with the collection of evidence; and

(26) Document all evidence collected and preserved, including affected systems.

f. **Head of Contracting Activity.** The Head of Contracting activity has a responsibility under the incident preparation role. The Head of Contracting shall: Ensure all contracts involving contractor access to VA-owned information or information systems, especially VA SPI, contain the appropriate security and privacy clauses as required by Federal and VA Acquisition Regulations in accordance with VA Handbook 6500.6, Contract Security.

g. **End User Operations Manager.** The End User Operations Manager has responsibilities under the incident preparation, incident detection, incident analysis, incident documentation, containment strategy, evidence gathering and management, mitigation/corrective action and lessons learned roles. The End User Operations Manager shall:

(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 all users of VA information and information systems under their responsibility take annual privacy and information security training;

(4) Work closely with the ISSO to maintain continuity of service;

(5) Ensure all users of VA information and information systems under their responsibility take ownership/responsibility for the data at their disposal;

(6) Adhere to VA configuration standards to ensure appropriate workstations and servers include installation and maintenance of patches for hardware and software, to include anti-virus;

(7) Ensure the appropriate user awareness and training programs on privacy procedures are available;

(8) Ensure users are aware of the reporting procedures and the policies for protecting VA information and information systems;

(9) Maintain a strong working relationship with the ISSO and PO;

(10) Ensure systems and subsystems affected by incidents are isolated as quickly as possible and if necessary, are restored or rebuilt;

(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;

(14) Maintain pertinent information including, but not limited to, audit and event logs as well as user account information when appropriate;

(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 facility;

(17) Safeguard data and sensitive information related to an incident;

(18) Ensure access to incident data is properly restricted;

(19) Coordinate and advise in the execution of the containment strategy and effort at the district 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 ensure containment actions are performed in a timely and efficient manner;

(24) Safeguard the integrity of involved hardware/software as appropriate; Preserve hardware/software as appropriate and requested;

(25) Preserve audit and event logs as appropriate;

(26) Balance mission needs with recommended risk mitigation;

(27) Coordinate with ISSOs, POs and staff to implement eradication and remediation actions;

(28) Ensure response actions are carried out by Local Area Network/Wide Area Network (LAN/WAN) managers;

(29) Implement recommendations as appropriate;

(30) Maintain a record of costs associated with repair, restoration, business disruptions and labor;

(31) Participate with the facility IRT staff in post-mortem review of all documentation surrounding the incident/suspected incident; and

(32) Implement “best practices” as appropriate based on the review.

h. **Privacy Officer (PO).** The PO has responsibilities under the incident preparation, incident prevention, incident detection, incident documentation, incident notification, containment strategy, restoration, evidence gathering and management and lessons learned roles. The PO shall:

(1) Maintain a PSETS account and ensure familiarity with the system;

(2) Maintain awareness of the privacy laws, regulations and VA policies affecting their organizations;

(3) Ensure awareness of the processes and systems in their organizations that collect and/or maintain SPI (e.g., PHI, PII FTI);

(4) Establish a working relationship with the ISSO(s) for the organizations and/or systems for which they are responsible;

(5) Execute directions provided by the DBRS, law enforcement, or OIG;

(6) Ensure VA personnel have appropriate incident response mechanisms to include:

(a) Conduct appropriate training to identify, contain and report suspected or confirmed privacy events; and

(b) Identity and contact information for PO, alternate PO, or other designated individuals as directed by local policy or procedures.

(7) Enter all suspected or confirmed complaints and incidents into PSETS within one hour of discovery, as provided in Appendix D;

(a) Ensure all discovery and risk evaluation fields are completed to include the date and time the event occurred and the date and time the event was identified, or notification of the event was received and acknowledged; and

(b) Notify and keep local management and support staff apprised of the event.

(8) Conduct or continue investigations of events not in a "closed" status update the PSETS event and document the progress in PSETS as appropriate;

(9) Request current templates for incident notification/credit monitoring and promotional (promo) codes as necessary, for each event when notified by the DBRS a breach of SPI has occurred;

(a) Complete all editable fields when drafting letters using the notification/credit monitoring letter templates provided by the DBRS to include:

i Pertinent facility information to include the facility name, address and other contact information;

ii Date letter is drafted or signed;

iii Description of the incident including the date of the incident (if known), the date of the discovery of the incident and the types of information involved (e.g., name, address); and

iv Description of what was done to investigate the incident, what was done to mitigate harm to individuals and what was done to prevent such incidents from recurring.

(b) Ensure no other templated language is changed unless directed by the DBRS.

(10) Coordinate with Public Affairs for drafting and DBRS for guidance and approval of news releases when required; Work with facility Public Affairs to ensure the news release and notification letters contain identical descriptions of the incident.

(11) Ensure timely closure of complaints and incidents, as follows:

(a) Update mitigation/corrective action fields in PSETS with description of what was done to investigate the event, what was done to mitigate harm to individuals and what was done to prevent such events from recurring as appropriate;

(b) Ensure REDACTED copies of pertinent external communications from investigation (e.g., correspondence, press releases) have been attached to the PSETS event;

(c) Ensure REDACTED complaint response letter has been attached to any PSETS complaint;

(d) Ensure REDACTED copies of notification or credit monitoring letters are attached to PSETS events as appropriate for any incident:

(12) For incidents with more than one letter type or more than one individual impacted, attach one representative REDACTED copy of letter type to PSETS.

(a) Close complaints; and

(b) Request the DBRS close incidents via PSETS.

(13) Ensure an after-action report process is in place to look at root causes and future prevention mechanisms, including reviewing privacy compliance documentation; Raise user awareness through lessons learned.

i. **Information System Security Officer (ISSO).** The ISSO has responsibilities under the incident preparation, incident prevention, incident detection, incident analysis, incident documentation, incident notification, containment strategy, restoration, evidence gathering and management and lessons learned roles. The ISSO shall:

(1) Maintain a PSETS account and ensure familiarity with the system;

(2) Maintain awareness of the security laws, regulations and VA policies affecting their organizations;

(3) Ensure awareness of the processes and systems in their organizations that collect or maintain SPI (e.g., PHI, PII, FTI);

(4) Establish familiarity and working relationships with the PO, End User Operations Manager and OIT staff for their organization;

(5) Execute directions provided by the DBRS, VA-CSOC, law enforcement, or OIG;

(6) Ensure VA personnel have appropriate incident response mechanisms to include:

(a) Appropriate training to identify, contain and report suspected or confirmed security events; and

(b) Identity and maintain contact information for ISSOs, or other designated individuals as directed by OIT policy or procedures.

(7) Enter all suspected or confirmed incidents into PSETS within one hour of discovery, as provided in Appendix D;

(a) Ensure all discovery and risk evaluation fields are completed to include the date and time the event occurred and the date and time the event was identified, or notification of the event was received and acknowledged;

(b) Coordinate with the PO to determine if a detected or reported security incident is also a privacy incident; and

(c) Notify and keep management and support staff apprised of the incident as appropriate.

(8) Conduct or continue investigations of events not in a “closed” status, update the PSETS event and document the progress in PSETS as appropriate, as follows:

(a) Initiate protective measures when an incident or vulnerability is discovered; and

(b) Verify with OIT the systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored or rebuilt as directed by VA-CSOC.

(9) Ensure timely closure of incidents, as follows:

(a) Update mitigation/corrective action fields in PSETS with description of what was done to investigate the incident, what was done to mitigate harm to individuals and what was done to prevent such events from recurring as appropriate;

(b) Ensure REDACTED copies of pertinent communications from investigation (e.g., emails, scans, log files) have been attached to the PSETS event as appropriate;

(c) Ensure that incidents initiated by VA-CSOC include a statement that closure is approved; and

(d) Request the DBRS close incidents via PSETS.

(10) Ensure an after-action report process is in place to look at root causes and future prevention mechanisms, including reviewing privacy compliance documentation; Raise user awareness through lessons learned.

j. **Public Affairs Officer.** The Public Affairs Officer has responsibilities under the incident notification and incident follow-up roles. The Public Affairs Officer shall:

(1) Prepare a news release, if required, using a previous news release provided by the DBRS as a sample;

(2) Draft news release to include all information the HIPAA Breach Notification Rule requires, as necessary;

(3) Coordinate with Office of Public and Intergovernmental Affairs (OPIA) as appropriate;

(4) Provide draft news release to facility PO, who will send it to DBRS for approval;

(5) Work with facility POs to ensure the news release and notification letters contain identical descriptions of the incident;

(6) Arrange for the publication of the news release by media outlets within two business days after the mailing of all notification letters;

(7) Provide a copy of the news release and list of media outlets to the PO for uploading to the PSETS event. Provide a copy of the news release to OGC and OIG as appropriate;

(8) Provide substitute notification when required if the agency does not have sufficient contact information to provide notification and as supplemental notification for any breach to keep potentially affected individuals informed; and

(9) Be prepared to say what the facility has done or is about to do to prevent a recurrence when/if contacted by the news media.

k. **Supervisors.** The Supervisor has responsibilities under the incident preparation, incident prevention and incident detection roles. The Supervisor shall:

(1) Ensure all subordinates can identify and know how to contact their PO and ISSO;

(2) Provide an inventory of the affected software, documents, etc., with an operational impact assessment of the potential data compromise and to assist with investigations; and

(3) Ensure privacy and security events are properly reported, responses are coordinated and updates are provided as required.

l. **Users of VA Information and Information Systems.** The Users of VA Information and Information Systems have responsibilities under the incident preparation, incident prevention and incident detection roles. Users of VA information and information systems shall:

(1) Ensure alertness to their surroundings and report any suspected incidents via local established reporting procedures to their ISSO, PO, appropriate designee, or supervisor immediately;

(2) Ensure vigilance in watching for unusual system behavior that may indicate a security incident in progress;

(3) Comply with all VA directives and policies on the appropriate use and security of VA IT resources and information;

(4) Observe their physical surroundings and make sure no SPI is left unsecured or otherwise at risk;

(5) Report any anomaly they notice with their applications and computers to their ISSO upon discovery; and

(6) Report any suspicion of inappropriate privacy or security practices tothe PO, ISSO and supervisor, as well as to VA law enforcement as appropriate, immediately upon discovery.

m. **Incident Management Process**.

(1) Introduction. The incident management process contains four main areas;

(2) Incident preparation;

(3) Incident detection, reporting and analysis;

(4) Incident mitigation/corrective action; and

(5) Post-incident activity.

n. **Incident Preparation.** Incident preparation requires the establishment of an incident response capability to ensure VA is responsive to incidents and prevents incidents by ensuring systems, networks and applications are sufficiently secure.

(1) Incident preparation begins with assigning roles and responsibilities across VA to manage and prevent incidents.

(2) Incident prevention is part of incident preparation, whereby security and privacy policies and training and system security controls are the primary mechanisms for preventing and reducing the number of incidents and breaches. OIS and DevSecOps ensure appropriate policies and controls exist to protect SPI and VA information systems using, storing and transmitting SPI.

o. **Incident Detection, Reporting and Analysis.** Incident detection and reporting occurs either through technical detection or reporting of an incident. Once reported, the incident will be analyzed, documented, prioritized and, if warranted, incident notification will be initiated.

(1) A user must immediately report to their VA supervisor, PO, or ISSO any actual or suspected incident involving the possible compromise or loss of any VA sensitive information in accordance with locally published reporting procedures.

(2) The PO or ISSO will promptly report the incident via PSETS within one hour of discovery, as provided in Appendix D in accordance with OIT Incident Management procedures.

(3) After an incident has been detected and reported, the PO or ISSO will investigate the privacy or security incident and provide feedback to the DBRS via PSETS. During investigation, if evidence of larceny, fraud, identity theft or other possible criminal activity is discovered, the PO or ISSO will coordinate with local leadership, law enforcement and OIG as appropriate.

(4) The DBRS, will determine whether a breach has occurred, based on the available facts presented.

(a) If a breach has occurred, the DBRS will follow the breach management process and notify the PO whether notification or credit monitoring services are warranted.

(b) If a breach has not occurred, the DBRS will render a DBRS decision and place the event in a pending resolution status.

(5) If the incident involves FTI, VBA Veterans Service Center (VSC) and Pension Management Center (PMC) personnel will follow standard VA reporting procedures and will:

(a) Report suspected security incidents pertaining to FTI to the VA incident response resources upon discovery of the incident, and;

(b) Contact the appropriate Field Division Office of TIGTA, OIG, and the IRS Office of Safeguards immediately, but no later than 24 hours after identification of a possible incident involving FTI.

NOTE: Reporting personnel shall review IRS Publication 1075, Section 1.8, Reporting Improper Inspections or Disclosures.

p. **Incident Mitigation/Corrective Action.** Depending on the results of the incident analysis, mitigation or corrective actions may include re-training VA personnel on applicable policy and proper procedures, revising policy or procedures to prevent a recurrence and providing notifications or credit monitoring services to individuals whose SPI was involved in a breach in accordance with VA policy and Federal law. While engaging in these activities, VA officials will also collect evidence to support any potential legal proceedings if warranted. Prior to requesting closure of the PSETS event, the PO or ISSO will promptly enter what actions have been taken to remediate any loss that may have occurred and what actions are being taken to prevent a future occurrence of this type of incident via PSETS in accordance with OIT Incident Management procedures.

q. **Post-Incident Activity.** Post-incident activity involves reviewing lessons learned, using collected incident data and evidence retention. Incident response personnel including DBRS, POs, ISSOs and other stakeholders will conduct the following post-incident activities:

(1) Review incidents from beginning to end, to include evaluating how well staff and management responded.

(2) Confirm incidents are closed by addressing the incident in writing and achieving closure in PSETS.

(3) Use collected incident information to remediate weaknesses, improve processes, or justify additional resources.

(4) Retain all evidence in any format related to an actual or suspected incident or breach in accordance with Records Control Schedule 10-1, 6000.6 Electronic Tracking System Files.

(a) For VA systems retaining FTI, post-incident activity, including audit logs must be maintained for seven years “to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements”. **NOTE:** Reporting personnel (i.e., VBA Pension and Fiduciary personnel) shall review IRS Publication 1075, Section AU-11, Audit Record Retention.

(b) DBRS or DBCT decisions for breach determination may be appealed.

(c) POs may appeal a decision within 10 days of the DBRS or DBCTs initial decision using the appeal request function within PSETS.

i POs must indicate in the appeal what has changed since the DBRS decision was made (e.g., PO learned new information that may change the incident outcome or new information regarding the ability to notify the subject of a breach).

ii In the event breach notification is required and the record subject’s identity is not known, they are deceased and have no next of kin on file, or when all methods of contacting those affected are exhausted, the DBRS may modify the decision to reflect a breach occurred, but unable to identify. In those instances, regarding PHI where there is insufficient or out of date contact information preventing direct written notification, a substitute form of notice may be provided. Substitute notices for PHI are covered in Appendix B.

(d) Upon receipt of the appeal, the DBRS reviews the appeal and determines if the new information provided is sufficient to render an immediate appeal decision, or whether the appeal will be presented to the DBCT.

i The DBRS or DBCT may modify their previous decision if new facts are presented that demonstrate an incident may be demoted from a breach or elevated to a breach.

ii The DBRS will notify the appeal requestor of the decision to sustain or reverse the breach determination.

5. BREACH MANAGEMENT PROCESS AND OVERSIGHT STRUCTURE.

a. **Introduction.** Breach management is part of the overarching incident management process designed to mitigate risk. The breach management process includes defining a breach, initiating a breach response team when necessary, conducting internal breach investigation, mitigating a breach to reporting requirements are met.

b. **Breach Definitions.** The terms incident, violation and breach are often used interchangeably but VA considers these terms to have their own distinct meaning. See Appendix D. Exclusions, a standard risk assessment, or a detailed risk assessment are applied by the DBRS when needed, to determine the risk of harm for breaches involving SPI to determine if notification or credit monitoring services are warranted.

c. **Breach Response Team.** The DBRS serves as the overarching breach response team for VA on behalf of the Secretary, the SAOP and the CPO. The DBCT is established and convenes to review incidents meeting specific criteria or for an appealed DBRS decision. The DBRS and the DBCT consult with other VA personnel who may be necessary according to specific agency missions, authorities, circumstances and identified risks as appropriate.

(1) The DBRS, as VA's breach response team, is comprised of personnel with the skills and expertise required to respond to breaches involving SPI effectively and efficiently.

(a) The DBRS coordinates and maintains all credit monitoring services provided by VA through a national contract. **NOTE**: Only the DBRS is authorized to procure credit monitoring services on behalf of VA.

(b) The DBRS maintains and provides all promotional codes, notification and enrollment templates. When notification or credit monitoring services are warranted for breaches involving SPI, the PO requests promotional codes and templates from the DBRS. NOTE: Only the DBRS is authorized to draft and disseminate promotional codes, notification templates and credit monitoring services enrollment instructions on behalf of VA.

(c) At the staff level, the DBRS reviews all suspected breaches reported as incidents and confirmed breaches daily.

(d) The DBRS uses prescribed exclusions, standard risk assessments and if needed, uses detailed risk assessments, or convenes the DBCT for assistance in making breach determinations.

(e) The DBRS notifies POs and ISSOs of DBRS decisions.

(2) The DBCT shall meet weekly at a minimum, or as required by the Director of the DBRS, to review specific incidents and advise the DBRS in determining type of event, impact and reporting requirements.

(a) The DBCT is comprised of the DBRS, members from VHA,VBA and NCA. Other members include the SAOP, CPO, CIO, CISO, OGC, Office of Congressional and Legislative Affairs (OCLA), Office of Human Resources Administration (OHRA), and OPIA. Optional attendees may include other VA personnel who may be necessary according to specific agency missions, authorities, circumstances and identified risks as appropriate.

(b) The DBCT reviews major or complex incidents to include incidents with Congressional or media interest and appeals of DBRS decisions.

(c) The findings of the DBCT regarding adjudication, type of event, impact and reporting requirements are made through collaboration, however the SAOP has the authority to overrule DBCT recommendations.

(d) The DBCT has the authority to escalate any incident to VA leadership, regardless of the risk assessment outcome.

(3) Regional or local breach/incident response teams may be convened in response to a major breach/incident.

(a) Regional or local breach/incident response teams may be called upon to identify applicable privacy compliance documentation (e.g., SORNs, PIAs or privacy notices applying to potentially comprised SPI).

(b) Regional or local breach/incident response teams may need to consult with regional/local VA personnel who may be necessary according to specific agency missions, authorities, circumstances and identified risks as appropriate.

(c) Regional or local breach/incident response teams may escalate breaches/incidents through regional and or local executive leadership.

d. **Breach Investigation.** Not all incidents may rise to the level of a breach. The breach investigation process is a systematic approach to determining whether an unauthorized use or disclosure of VA information or information system has taken place and the risk of harm that result from the incident.

(1) The DBRS reviews all incidents, either detected or reported, using the VA developed breach criteria in Appendix A for determining when an incident is a breach.

(2) The DBRS may direct POs or ISSOs to investigate incidents further, provide additional information and update PSETS accordingly.

(3) If the DBRS determines a breach has occurred, the DBRS will follow the breach management process and notify the PO whether notifications or credit monitoring services are warranted.

e. **Breach Mitigation.** When an incident is determined to be a breach, mitigation is required. Breach mitigation often includes timely and accurate communication with individuals whose SPI was involved in a breach.

(1) Mitigation of breaches requires a series of actions or processes assisting in the identification of the root cause(s) of the breach, to understand how the breach occurred and prevent future occurrences.

(2) The DBRS directs the PO when and how to notify affected individuals of the breach and if warranted, provides promotional codes and enrollment instructions for credit monitoring services.

(a) Notification to the affected individuals must be made within 60 calendar days from the date the incident occurred, if known, or was discovered if the date of the incident is unknown.

(b) The DBRS provides, as appropriate, a weekly report of incidents requiring notification to Administrations and Staff Offices to assist them in meeting the 60-calendar day timeframe.

(c) Breaches involving PHI, or breaches involving more than 500 individuals may have additional notification processes. The HIPAA breach notification process is outlined in Appendix C.

(d) The PO must ensure they are using the most up-to-date templates for notification and specific promotional codes by requesting them from the DBRS for each breach occurrence.

NOTE: At no time shall POs reuse previously saved notification templates or promotional codes.

(e) VA maintains accurate and up-to-date contact information gathered when an individual registers for healthcare or benefits.

i If the DBRS determines that notification is warranted, it is the responsibility of each facility, through the PO, to contact individuals whose SPI was involved in a breach.

ii Contact information for individuals may be found in the Veterans Affairs Profile (VA Profile) (192VA30) system of records and should not be requested of the next of kin.

iii Veterans experiencing homelessness are encouraged to provide contact information of a relative or another person who is able to contact them.

iv . In those instances where there is insufficient or out-of-date contact information preventing direct written notification, a substitute form of notice may be provided. Substitute notice details are provided in Appendix B.

(f) The responsible PO will draft letters on official VA letterhead, using letter templates provided by the DBRS and will ensure mailing of the letters to the individuals affected by the breach. The facility Director, or their designee, will sign the letter.

i A redacted copy of each letter type sent for a breach will be attached by the PO to the PSETS event, prior to requesting closure. For more information on breach letter types, review Appendix B.

ii The responsible PO will maintain a copy of each letter sent for a breach in their local privacy event folders, maintained and retrieved by the PSETS event (ticket) number or by the date of the event, never by the complainant's name or other unique identifier.

(g) When requesting closure of the breach, the PO will promptly enter what actions have been taken to remediate any loss that may have occurred and what actions are being taken to prevent a future occurrence of this type of breach via PSETS in accordance with OIT Incident Management procedures.

(h) The DBRS will review each request for closure of a breach to ensure the facility has uploaded appropriate redacted letter(s) and entered appropriate mitigation/corrective action in PSETS.

f. **Breach Reporting.** The DBRS coordinates the reporting of breaches both internally and externally as appropriate. The DBRS or the DBCT may escalate breaches to VA leadership, through the CPO or SAOP. The DBRS ensures external reporting requirements are met, including notification to the general public.

(1) The VA-CSOC, as VA's principal security operations center, notifies the US-CERT of a breach consistent with US-CERT notification guidelines.

(2) For those breaches requiring reporting to law enforcement, OIG or OGC, the DBRS ensures the facility responsible for the breach reports breaches promptly, even if the breach is unconfirmed, or the circumstances are still unclear.

(3) For those breaches requiring reporting to Congress, the DBRS through OCLA ensures the appropriate Congressional Committee(s) are notified.

(a) Congressional Committees must be notified no later than seven days after the date on which there is a reasonable basis to conclude a

breach constitutes a major incident, in accordance with FISMA and OMB M-22-05.

(b) A major incident involves an unauthorized modification of unauthorized deletion of unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more individuals.

(c) For major incidents, VA will supplement the initial seven day notification with a report no later than 30 days after discovery of the breach.

(d) All breaches of SPI are reported to Congress quarterly. The DBRS prepares the report and provides it to OCLA for distribution.

i Once the report of all breaches involving SPI is reported to Congress, the DBRS publishes the report on a publicly accessible VA website.

ii OIT personnel shall not speak directly to members of the press about any breaches but shall refer all inquiries to OPIA.

iii For those breaches requiring reporting to HHS in accordance with the HIPAA Breach Notification Rule, review Appendix C.

6. VA CRITERIA FOR BREACH AND RISK ASSESSMENT

a. **Introduction to VA Breach Criteria.** For purposes of simplifying and standardizing the breach management process, VA developed breach criteria for determining when an incident is a breach. The VA-developed breach criteria include reviewing standard breach exclusions, applying the standard risk assessment matrices, or using a detailed VA Breach Risk Assessment Tool (VABRAT) for breaches with unusual circumstances.

(1) The VA DBRS uses the breach criteria and risk assessment in determining whether the reported event constitutes a breach and whether VA should notify the record subjects of the event or offer them credit monitoring services.

(2) The VA DBRS reviews each breach to determine when an IRA is necessary in accordance with 38 U.S.C. § 5724(a).

(a) When an IRA is required, the DBRS will arrange for and manage an IRA by a non-VA entity to determine the level of risk for a potential misuse of any SPI involved in a breach.

(b) VA may rely on the results of prior IRAs for similar incidents for breach and notification determinations.

b. **Breach Exclusions.** A breach excludes:

(1) Any unintentional acquisition, access, or use of SPI by VA personnel or person acting under the authority of VA or its contractors or other agents (e.g., BAs), if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in the further use or disclosure in a manner not permitted by law or VA policy.

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

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

c. **Standard Risk Assessment Matrices.** After reviewing the standard breach exclusions, the DBRS uses the standard risk assessment matrices in Appendix A to determine whether notification or credit monitoring are warranted.

(1) Except for the standard breach exclusions listed above, an unauthorized acquisition, access, use, or disclosure of SPI is presumed to be a breach, unless VA demonstrates there is a low probability the SPI has been compromised based on the standard risk assessment of factors including the following:

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

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

(c) The likelihood that the SPI was acquired or viewed; and

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

d. **Detailed VA Breach Risk Assessment Tool.** After reviewing the standard breach exclusions, assuming the incident is a breach and applying the standard risk assessment and matrices, if further review is necessary, the DBRS will use a detailed risk assessment tool.

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

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

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

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

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

(e) Likelihood that the SPI was the target of, rather than incidental to, the unauthorized acquisition, access, use, or disclosure; and

(f) The likelihood that the credit monitoring services will assist the individuals in avoiding or mitigating any harm resulting from the breach.

(2) Based on the results, the DBRS will determine if detailed risk assessments need to be provided to the DBCT.

(a) The DBCT will determine whether there is a low probability of risk of compromise of the involved SPI. In accordance with 38 C.F.R. § 75.115, compromise means made accessible to and usable by unauthorized persons.

(b) If, upon review of the available information, the DBCT finds more information is necessary to determine if there is more thana low probability of risk of compromise to the SPI of the recordsubjects, the DBRS may ask the involved VA personnel to provide such additional information.

7. TABLETOP EXERCISE AND ANNUAL PLAN REVIEW.

a. Tabletop Exercise. Testing breach response plans is an essential part of risk management and breach response preparation. On the second Tuesday in each October, the DBRS shall convene the DBCT, as the agency's breach response team to hold a tabletop exercise. The DBRS shall document the review of this breach response tabletop exercise as part of annual FISMA reporting. The purpose of the exercise is to test the breach response plan as presented in this handbook and ensure members of the breach response team familiar with the plan and understand their specific roles. Tabletop exercises are conducted to ensure coordinated responses to breaches, to further refine and validate this breach response plan and identify potential weaknesses in response capabilities.

b. Annual Plan Review. At the end of each fiscal year, the SAOP and CPO shall review reports detailing the status reported breaches to determine if VA should update the breach response plan, develop and implement new or revise existing policies or training, or modify information sharing arrangements. The SAOP shall document the review of this breach response plan as part of annual FISMA reporting.

8. REFERENCES.

a. 38 U.S.C. §§ 5721-28, Department of Veterans Affairs Information Security Enhancement Act of 2006.

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

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

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

e. 38 U.S.C. § 5701, VA Claims Confidentiality Statute.

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

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

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

i. 45 C.F.R. §§ 160 and 164, HIPAA Privacy, Security and Breach Notification Rules.

j. OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, (January 3, 2017).

k. OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements, (December 6, 2021).

l. Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide) (August 6, 2012).

m. Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 6, 2010).

n. Special Publication 800-66 Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability Act (HIPAA) Security Rule (October 23, 2008).

o. VA Directive 6500, VA Cybersecurity Program VA Information Security Program. (February 24, 2021).

p. VA Directive 6502, VA Enterprise Privacy Program (May 5, 2008).

q. VA Directive 6509, Duties of Privacy Officers (July 30, 2015).

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

s. VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program (February 24, 2021).

t. VA Handbook 6500.6, Contract Security (March 12, 2010).

u. VHA Directive 1605, VHA Privacy Program (September 1, 2017).

v. VHA Directive 1605.05, Business Associate Agreements (November 17, 2020).

w. VHA Directive 1605.01, Privacy and Release of Information (August 31, 2016).

x. VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosures and Requests for Protected Health Information (April 4, 2019).

y. VHA Directive 1606.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation (November 20, 2020).

z. VHA Directive 1907.08, Health Care Information Security Policy and Requirements (April 30, 2019)

aa. Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies. (December 10, 2021).

9. TERMS AND DEFINITIONS.

a. **Breach.** A loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. A breach shall be treated as discovered as of the moment such breach is known to the individual or, by exercising reasonable diligence, would have been known to that individual.

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

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

d. **Credit Monitoring Services.** All the services listed in 38 U.S.C. § 5724 (b) and 38 C.F.R. § 75.118 provided to those individuals impacted by a breach of VA SPI, to include but not limited to internet and dark web monitoring, database source monitoring, identity theft insurance and identity restoration services.

e. **Data Elements**. A combination of characters, words, or phrases referring to one separate item of information. Examples are name, full SSN, last name, last four of SSN, DOB, Address, Service Number, or other identifying terms or words.

f. **Federal Tax Information (FTI).** Tax return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.

g. **Incident.** Any occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. An incident shall be treated as discovered as of the moment such incident is known to the individual or, by exercising reasonable diligence, would have been known to that individual.

h. **Individually Identifiable Health Information (IIHI).** As defined by the HIPAA Privacy Rule, information that: is created or received by a health care provider,

health plan, or health care clearinghouse; relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (3)(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

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

j. **Personally Identifiable Information (PII).** Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII elements include but are not limited to name, SSN, biometric records, etc. alone, or when combined with other personal identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

k. **Protected Health Information (PHI).** As defined by the HIPAA Privacy Rule, PHI is IIHI that is transmitted by electronic media, maintained in or by electronic media, or transmitted or maintained in any other form or medium, excluding IIHI in (i) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) records described 20 U.S.C. § 1232g(a)(4)(B), (iii) employment records held by a CE in its role as employer; and (iv) records regarding a person who has been deceased for more than 50 years.

l. **Sensitive Personal Information (SPI)**. SPI, with respect to an individual, means any information about the individual maintained by an agency, including the following:

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

(2) Information that can be used to distinguish or trace the individual's identity, including name, SSN, date of birth, mother's maiden name, or biometric records. SPI is often used interchangeably with PII.

m. **VA Sensitive Information (VASI)**. As defined by 38 U.S.C. § 5727, VASI is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information

whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information and records about individuals requiring protection under applicable confidentially provisions. PHI, PII and SPI are generally VASI.

n. **Violation**. Any incident where SPI was acquired, used, or disclosed in a manner that violates an information security or privacy policy, but may or may not be a breach, depending on the exclusions and risk analysis.

APPENDIX A - STANDARD RISK ASSESSMENT MATRICES.

a. **Introduction.** The following standard risk assessment matrices describe incident scenarios, determine whether a breach has occurred and in the event the incident includes PHI, determines whether the incident should be reported to HHS under the HIPAA Breach Notification Rule. If the facts of the incident fall outside of the standard risk assessment, a detailed risk assessment is required to determine if a breach has occurred.

b. **Mismailing.** The mismailing category includes all tangible material (e.g., envelope, container, package) sent through a mail carrier (e.g., United States Postal Service (USPS) or other commercial carrier) including prescriptions and other correspondence containing VA SPI that may have been sent to the incorrect address, damaged in transit, lost, mislabeled, or otherwise compromised while in transit to the proper recipient. **NOTE**: a third party includes trusted entities, but not VA personnel.

(1) As part of the standard risk assessment, prior to reviewing the matrix for tangible mail events, the following are exceptions and are not considered breaches:

(a) SPI viewed by another HIPAA CE.

(b) SPI viewed by other Federal agency, where the recipient returned the envelope or package to VA with all contents intact, or the recipient destroyed the SPI and certified such destruction in writing.

(c) SPI exposed to, but not acquired by, USPS or other mail carrier staff only during the performance of their official duties wherethe mailing was delivered to the appropriate recipient with all contents intact.

Table 1: Matrix 1 - Breach Determination for Tangible Mail Event

Tangible Mail Event: VA Tangible Material Containing SPI	Breach	Breach of PHI (HIPAA Reporting)
1. Sent to an incorrect address and returned to VA sealed and unopened	No [Excluded]	No
2. Sent to an incorrect address and SPI exposed to a third party (i.e., an individual or entity that is not a VA employee, contractor, BA, or other agent)	Yes	Yes
3. Sent incorrectly to a Federal agency or a HIPAA CE (e.g., non-VA health care provider or hospital)	No	No
4. Sent to an incorrect address, opened by third party (e.g., Veteran A received Veteran B's SPI), whether returned to VA or not	Yes	Yes
5. Exposed to a VA workforce member other than the intended recipient due to damaged container	No [Excluded]	No
6. Exposed to a third party due to damaged container	Complete detailed risk assessment tool	Complete detailed risk assessment tool
7. Sent to a third party where container is lost or damaged in transit	Complete detailed risk assessment tool	Complete detailed risk assessment tool
8. Sent to a VA employee, contractor, BA, or other agent where container is lost or damaged in transit	Yes	Yes
9. Sent to the correct address with SPI about an individual other than the intended recipient (e.g., a letter to Veteran B in envelope addressed to Veteran A)	Yes	Yes
10. Sent outside VA with more PII than is necessary for mailing (e.g., social security number (SSN), date of birth (DOB), PHI including clinic name) displayed on the label or outside of the container	Yes	Yes
11. Sent to a local or state agency or any other person or entity without proper authority	Complete detailed risk assessment tool	Complete detailed risk assessment tool

c. **Mishandling.** The mishandling category includes incidents in which SPI, regardless of format (i.e., electronic, paper, verbal) could have been exposed through improper handling.

(1) Readable SPI is data that is either able to be read or deciphered by a person, or capable of being processed or interpreted by a computer or other electronic device without the use of proprietary software or hardware.

(2) It is the policy of VA to ensure appropriate reasonable administrative, technical and physical safeguards are established to ensure the security and confidentiality of SPI (e.g., locking or logging off computers when unattended, locking SPI in file cabinets or desks, avoid speaking about SPI in public hallways and elevators, confirming email addresses and facsimile (fax) numbers prior to sending).

(3) Incidents in which SPI is found unexposed (e.g., in an unopened envelope or box, or in a location where access in violation of any of the applicable confidentiality provisions is unlikely) are excluded from the category of mishandled information.

(4) Incidents in which SPI could have been exposed (e.g., emailed or faxed to the wrong individual; documents which are 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) are considered mishandled information.

(5) As part of the standard risk assessment, prior to reviewing the matrix for mishandled events, the following exception should be applied.

(6) SPI viewed by another HIPAA CE or other Federal agency, where the recipient returned the SPI or appropriately destroyed the SPI.

Table 2 Matrix 2 - Breach Determination for Mishandling Event

Mishandling Events: VA SPI	Breach	Breach of PHI (HIPAA Reporting)
1. Readable SPI exposed only to VA personnel (e.g., employees, contractors, volunteers, students, etc.) where personnel do not nefariously use or disclose SPI	No [Excluded]	No
2. Readable SPI not exposed	No	No
3. Readable SPI exposed to a Veteran (e.g., paperwork of a Veteran handed to another Veteran) and the Veteran leaves the facility with the SPI	Yes	Yes
4. Readable SPI exposed to a Veteran or their Caregiver within the facility and immediately handed back to VA personnel	No [Excluded]	No
5. Readable SPI correctly provided to a Veteran and Veteran leaves SPI unsecured at facility	No [Not VA]	No
6. Readable SPI exposed to anyone else through any means other than email	Yes	Yes
7. Readable SPI lost and has not been found, exposure undeterminable	Yes	Yes
8. Readable SPI incorrectly faxed to wrong location within VA where personnel do not nefariously use or disclose SPI	No [Excluded]	No
9. Readable SPI incorrectly faxed to wrong location outside of VA (e.g., to public fax (e.g., business, individual), another HIPAA CE, another Federal agency)	Complete detailed risk assessment tool	Complete detailed risk assessment tool
10. SPI exposed on any social media platforms (e.g., Facebook, Twitter, Instagram)	Complete detailed risk assessment tool	Complete detailed risk assessment tool
11. Readable SPI exposed to anyone else through any means other than email	Complete detailed risk assessment tool	Complete detailed risk assessment tool

d. **Email.** The email category includes messages containing VA SPI distributed by electronic means from one computer user to one or more recipients.

(1) Email containing VA SPI must be encrypted with an encryption application certified by the National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS) 140-3 compliant.

(2) Email sent or received by a VA source containing SPI not encrypted with a FIPS 140-3 compliant encryption application is treated in this handbook as unencrypted email.

(3)) VA's Adjudication Procedures Manual, M21-1, Part XIV.4.B.1. specifies required safeguards for sending FTI within an email or as an attachment to any recipient.

(4) As part of the standard risk assessment, prior to reviewing the matrix for email events, the following exceptions should be applied:

(a) SPI disclosed (acquired and was or may have been viewed) by another HIPAA CE, Federal agency, or other entity with whom VA has a formal agreement (i.e., Data Use Agreement), where the recipient was the intended party and had legal authority to receive the SPI.

(b) SPI disclosed (acquired and was or may have been viewed) by VA personnel, where the recipient was the intended party, had legal authority to receive the SPI and certifies no other party had access to the personal email account and the email has been deleted.

Table 3 Matrix 3 – Breach Determination for Compromised Email Events

Compromised Email	Breach	Breach of PHI (HIPAA Reporting)
1. Encrypted email containing SPI sent inside or outside VA to wrong party	No [Excluded]	No
2. Unencrypted email containing SPI sent to unintended VA personnel at their VA email address where personnel do not nefariously use or disclose SPI	No [Excluded]	No
3. Unencrypted email containing SPI sent to the intended VA personnel at their VA email address	No [Excluded]	No
4. Unencrypted email containing SPI sent to intended Veteran, patient, or his/her personal representative outside VA Network	No [Right of Access]	No
5. Unencrypted email containing SPI sent to anyone other than a VA workforce member or intended Veteran, patient, or his/her personal representative outside VA	Complete detailed risk assessment tool	Complete detailed risk assessment tool
6. Emails sent to personal email address of VA personnel or trusted entity	Complete detailed risk assessment tool	Complete detailed risk assessment tool

e. **Equipment.** The equipment category includes unaccounted for, missing or stolen equipment that may be used to store, transmit, create, access, duplicate or copy, disclose, or use SPI, whether it is encrypted or unencrypted.

(1) It is the policy of VA to ensure VA facilities, contractors and BAs will immediately report upon discovery any 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.

(2) All missing equipment is reportable to the US-CERT.

(3) Unaccounted for equipment is IT equipment the facility lists on its inventory, not assigned to specific personnel or location and cannot be located but where there is no indication it was stolen.

(4) Stolen equipment is equipment VA has determined was stolen based on the available evidence (e.g., a laptop is missing from an employee's locked car and there is evidence someone broke into the car; a laptop stolen from a treatment unit after cutting the tether to the storage cart; or a hard drive is removed from a workstation).

(a) There should be affirmative evidence that would lead a reasonable person to conclude someone intentionally took the equipment or the container for the equipment (e.g., someone steals an employee's car containing a laptop and the laptop is not in the car when it is recovered).

i Missing equipment is equipment assigned to specific personnel or location and the equipment is lost or misplaced (e.g., an employee puts a laptop on top of their car and drives off).

ii As part of the standard risk assessment, prior to reviewing the matrix for equipment events, the following exception should be applied:

(b) Encrypted equipment or encrypted data.

(c) Equipment containing a Limited Data Set (LDS) as defined by the HIPAA Privacy Rule and the risk to the SPI being re-identified is low.

Table 4 Matrix 4 - Breach Determination for Equipment Events

Equipment – Unaccounted for, Stolen, or Missing	Breach	Breach of PHI (HIPAA Reporting)
1. Unaccounted for, stolen, or missing equipment not containing SPI	No	No
2. Unaccounted for, stolen, or missing equipment containing encrypted SPI or encrypted PHI	No [Excluded]	No
3. Unaccounted for, stolen, or missing equipment containing unencrypted SPI	Yes	Yes

f. **Unauthorized Access.** The unauthorized access to SPI category includes any access to SPI in violation of any of the applicable confidentiality provisions or security standards.

(1) Such unauthorized may include:

(a) Access to SPI by an unauthorized user (i.e., has not met the security standards to access the data, such as no background investigation if required); or

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

(2) As part of the standard risk assessment, prior to reviewing the matrix for unauthorized access or access for unauthorized purposes, the following exceptions should be applied:

(a) SPI belonging to Veteran A was acquired and was or may have been viewed by Veteran B through Veteran B's VA issued account (i.e., Blue Button, MyHealtheVet, or other program), however the SPI does not include unique identifiers (i.e., name, SSN) of Veteran A, where VA removed Veteran A's SPI from Veteran B's account or system and VA received confirmation from Veteran B that the information was not downloaded or otherwise saved.

(b) SPI was acquired and was or may have been viewed by another HIPAA CE, Federal agency, or other entity with whom VA has a formal agreement (i.e., Data Use Agreement), where the recipient confirms no SPI was stored or otherwise retained on IT systems.

Table 5 Matrix 5 - Breach Determination for Unauthorized Access/Access for Unauthorized Purpose Events

Unauthorized Access/Access for Unauthorized Purpose Events	Breach	Breach of PHI (HIPAA Reporting)
1. SPI accessed by VA personnel or trusted entity without authority or permission and investigation reveals an intent to access in violation of policy for malicious purposes, to cause actual or reputational harm, or discord (e.g., intentional access for purposes of obtaining information from VA systems for use in further nefarious, either criminal or non-criminal, activities).	Yes	Yes
2. SPI accessed by VA personnel or trusted entity without authority or permission and investigation reveals access in violation of policy but without malicious intent or to cause harm (e.g., intentional access for purposes of obtaining information from VA systems due to curiosity, or other activities that do not have nefarious purposes).	Complete detailed risk assessment tool	Complete detailed risk assessment tool
3. SPI accessed by VA personnel unintentionally or accidentally (e.g., in error)	No [Excluded]	No
4. SPI of another Veteran accessed electronically by a Veteran through their VA-issued account (e.g., My HealtheVet, eBenefits) due to a technical issue	Complete detailed risk assessment tool	Complete detailed risk assessment tool
5. SPI accessed electronically by any third party	Complete detailed risk assessment tool	Complete detailed risk assessment tool
6. SPI possibly exposed, but VA cannot determine the likelihood of unauthorized access or misuse of the SPI	Complete detailed risk assessment tool	Complete detailed risk assessment tool

g. **Improper Disposal.** The improper disposal category includes those situations in which storage media containing SPI cannot be accounted for at any time between release by a VA office or trusted entity and the ultimate destruction of the storage media or rendering of the SPI on the storage media permanently inaccessible (e.g., paper records containing SPI in a dumpster located behind a Community Based Outpatient Clinic (CBOC), including CBOCs on leased property, or a hard drive containing SPI on excessed VA IT equipment).

(1) Readable SPI is data that is either able to be read or deciphered by a person, or capable of being processed or interpreted by a computer or other electronic device without the use of proprietary software or hardware.

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

(3) As part of the standard risk assessment, prior to reviewing the matrix for improper disposal, the following exception should be applied:

(a) SPI was recovered by a HIPAA CE, Federal agency, or other entity with whom VA has a formal agreement (i.e., Data Use Agreement, or law enforcement), where the SPI was or may have been viewed and there is no indication any SPI removed was or accessed from the storage media.

Table 6 Matrix 6 - Breach Determination for Unauthorized Disposal Events

Unauthorized Disposal Events	Breach	Breach of PHI (HIPAA Reporting)
1. Encrypted SPI on storage media improperly disposed (i.e., in violation of policy)	No [Excluded]	No
2. Readable SPI recovered and accessible only by VA personnel or trusted entity personnel and there is negligible risk of harm	No [Excluded]	No
3. Readable SPI, such as paper, left unattended on VA property but sealed and secured in a manner that no SPI was actually acquired, accessed, or disclosed	No	No
4. Storage media or paper with readable SPI accessible by any third party	Complete detailed risk assessment tool	Complete detailed risk assessment tool

APPENDIX B – BREACH NOTIFICATION.

a. **Introduction.** Each incident determined to be a breach is fact-specific and as such, the decision of whether to notify individuals will depend on the circumstances of the breach. The DBRS will exercise care to evaluate the benefit of providing notice to individuals or the public as notification may not always be helpful to the individuals. The DBRS or the DBCT, when deciding whether to notify individuals potentially affected by a breach consider the assessed risk of harm. Once the decision to notify individuals is made, the DBRS considers the source, timeliness, contents and method of the notification, as well as any special considerations.

(1) When an incident is determined to be a breach, there are specific data elements, whether alone or combined with other data elements, requiring notification or credit monitoring services.

(2) Pursuant to 38 C.F.R. § 75.114, VA may, as a matter of discretion, provide an accelerated response to a breach by offering notification or credit monitoring services without an IRA.

(a) The decision to provide an accelerated response following a particular breach does not indicate that VA determined an "immediate, substantial risk of identity theft" or even a "reasonable risk" exists for the potential misuse of SPI involved in the incident.

(b) The following matrix outlines what specific data elements (whether alone or combined) require breach notification or credit monitoring services.

Table 7 Matrix 7 – Breach Notification or Credit Monitoring for Specific Data Elements

Data Elements Involved	Notification Only Warranted	Credit Monitoring Warranted
1. Full name only	No	No
2. Full name with other SPI	Yes, for PHI	No
3. Full name and DOB	No	Yes
4. Full name and home address	Yes	No
5. Full name and email address	No	No
6. Full SSN	No	Yes
7. Full name and partial SSN	Yes	No
8. Full name and PHI, including account numbers or disability codes	Yes	No
9. Partial SSN only	No	No
10. Partial SSN with other SPI	Yes, for PHI	No
11. Partial name with other SPI	Yes, for PHI	No
12. Other PII	Determined by DBRS	Determined by DBRS

b. **Breach Notification Letters.** When the DBRS determines an incident to be a breach requiring notification, the DBRS will instruct POs to promptly provide written notification of the breach by first-class mail to the individual affected (or next of kin if the individual is deceased) in accordance with 38 C.F.R. §§ 75.114 – 117. Notification templates are drafted, maintained and distributed to the field by the DBRS. The DBRS may, at their discretion, require an additional or different notification method depending on the number of individuals affected, available contact information, or the urgency with which individuals need to receive the notification.

(1) Notification letter types are determined in part by the data elements described in Matrix 7 Breach Notification or Credit Monitoring for Specific Data Elements, as well as the source (i.e., administration) responsible for the breach.

(2) Notification to the affected individuals must be made within 60 calendar days from the date the incident occurred, unless delayed upon lawful request as outlined in Section D of this appendix.

(3) Notification templates are provided to POs for each breach occurrence using concise plain language and shall include the following:

(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 SPI involved in the breach (e.g., full name, SSN, DOB, home address, account number and disability code);

(c) A statement of whether the information was encrypted or protected by other means, when it is determined disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information system;

(d) Guidance to potentially affected individuals on how they can mitigate their own risk of harm, countermeasures the agency is taking and services, if any the agency is providing affected individuals;

(e) Steps taken to investigate the breach, mitigate losses and protect against a future breach; and

(f) Whom potentially affected individuals should contact at the agency for more information, including a telephone number, email address and postal address.

(4) A “yes” answer in the “notification warranted” column or “credit monitoring warranted” column means the responsible VA entity must notify the affected individuals of the breach or provide credit monitoring services as directed by the DBRS.

(a) In the event the record subject is a person under the age of full legal responsibility, the DBRS will provide specific notification and enrollment instructions for minor credit monitoring services.

(5) A “yes” answer in the “notification warranted” column, where the record subject is deceased, requires a next of kin letter sent to the next of kin of record in accordance with 45 C.F.R. § 164.404.

(a) An offer of credit monitoring services will not be sent to individuals who are next of kin of a deceased Veteran unless the data of the next of kin was involved in a breach, or the deceased individual’s SPI involved in the breach could be used to harm the next of kin.

(6) When a breach involves PHI, the notification letter must meet the requirements of the HIPAA Breach Notification Rule. Appendix C outlines the HIPAA breach notification process.

(7) In the event breach notification letter(s) are returned as undeliverable, the responsible PO shall maintain the returned letter(s) in the PSETS administrative file. POs shall also track all returned notifications using a

spreadsheet or other means and make it available to the DBRS, administrations, or program offices upon request.

c. **Substitute Notice.** When there is not sufficient contact information to provide notification to an individual affected by a breach, or if the need to provide an immediate or preliminary notification in the wake of a high-profile breach is determined by the DBRS or DBCT, VA may provide a substitute notification in accordance with 38 C.F.R. § 75.117. A substitute notice may also serve as a supplemental notification for any breach, as determined by DBRS or DBCT, to keep potentially affected individuals informed. Substitute notices for breaches occurring within VHA, involving PHI shall be handled in accordance with 45 C.F.R. § 164.404 as directed by the DBRS or DBCT.

(1) Substitute notifications for fewer than 10 individuals may be provided by an alternative form of written notice, telephone, or other means as directed by DBRS.

(2) Substitute notifications for 10 or more individuals may consist of a conspicuous posting of the notification on the home page of VA's website or notification to a major print and broadcast media, including major media in areas where the potentially affected individuals reside, for a period of not less than 90 calendar days, as directed by DRBS.

(a) Substitute notices involving 10 or more individuals require the PO to coordinate with the local PAO to prepare a summary write-up of the breach using templates and examples provided by the DBRS. Once drafted, the PO shall submit summary write-ups to DBRS for approval prior to releasing to the VA Webmaster or media.

(b) Substitute notifications prepared for media releases must contain identical descriptions of the breach as in notification letters.

(c) Substitute notifications made to media shall include a toll-free phone number (and an email address if appropriate) individuals can use to learn whether their personal information was affected by the breach.

(d) In the event there is an ongoing investigation, VA may establish an ongoing communication method for interested individuals to automatically receive updates.

(e) Depending on the affected individuals, substitute notices may be provided in more than one language and will be consistent with Section 508 of the Rehabilitation Act of 1973, as amended.

(3) In the event a substitute notice is provided, the PO shall update the PSETS to indicate the method by which the substitute notice was provided and any actions taken.

(4) The PO must maintain a copy of the substitute notice in the PSETS administrative file and provide a copy to regional counsel.

d. **Law Enforcement Delay.** In accordance with 38 C.F.R. § 75.117, notifications may be delayed at the discretion of the DBRS or the DBCT upon lawful requests from other Federal agencies. The Attorney General, the head of an element of the Intelligence Community, the Secretary of the Department of homeland Security (DHS), or OIG may delay notifying individuals potentially affected by a breach if the breach notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions. Notification delays for breaches occurring within VHA, involving PHI shall be handled in accordance with 45 C.F.R. § 164.404 as directed by the DBRS or DBCT.

(1) A lawful request is one made in writing by the entity or VA component responsible for the investigation or data recovery efforts that may be adversely affected by providing notification.

(2) Any delay should not exacerbate risk or harm to any affected individual(s).

APPENDIX C – HIPAA BREACH NOTIFICATION.

a. **Introduction.** The incident and breach management processes described in this handbook apply to all breaches, with additional requirements applying to breaches occurring within VHA involving PHI maintained by VHA and VA components that are Business Associates (BAs) of VHA. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires covered entities (CEs) and their BAs to provide specific notification following breaches of unsecured PHI. Responses to breaches under the Rule are coordinated by the DBRS and the DBCT. A breach is treated as discovered on the first day the breach is known, or through the exercise of reasonable diligence, would have been known to the CE or BA.

b. **Breaches Under 500.** In addition to providing breach notification to individuals, HHS must be notified of any breaches occurring within VHA, involving the PHI of 499 or fewer individuals, with an annual notice or on a rolling basis, but no later than 60 calendar days after the end of each calendar year. The DBRS manages notification to HHS on a rolling basis. Once all requirements are met, including the PO uploading a redacted copy of the letter provided to individuals and the PO requesting closure of the PSETS event, the DBRS shall notify HHS.

c. **Breaches 500+.** HHS must be notified of any breaches occurring within VHA, involving the PHI of 500 or more individuals, concurrently with the individual notice as outlined in Appendix B of this handbook. The DBRS manages notification to HHS.

   (1) For a breach of PHI involving 500 or more residents of a state or jurisdiction, VHA and its BAs shall, following discovery of the breach, notify prominent media outlets serving the state or jurisdiction as outlined in Appendix B, Substitute Notice.

   (2) Once all requirements are met, including the PO uploading a redacted copy of the letter provided to individuals, the PO uploading the substitute notices posted conspicuously or to the media and the PO requesting closure of the PSETS event, the DBRS shall notify HHS.

   (3) Notification shall be made within 60 days of the date the breach was discovered, but no later than when the individuals are notified, whichever is sooner.

d. **Breaches with Business Associates.** If a breach of unsecured PHI occurs at or by a BA, the BA shall notify VHA following discovery of the breach within the timeframe indicated in the Business Associate Agreement and no later than 60 days from the discovery of the breach. The BA shall provide VHA with the identification of each individual affected by the breach, as well as any other available information as required for notification to affected individuals. Once all requirements are met, the DBRS shall notify HHS.