



Defense Health Agency **ADMINISTRATIVE INSTRUCTION**

NUMBER 071
September 15, 2015

A&MD

SUBJECT: Incident Response Team (IRT) and Breach Response Requirements

References: See Enclosure 1

1. **PURPOSE.** This Defense Health Agency Administrative Instruction (DHA-AI), based on the authority of References (a) and (b), and in accordance with the guidance of References (c) through (m):

a. Reissues DHA-AI No. 71 to update responsibilities and establish the processes and procedures for individuals and supervisors responsible for assessing and responding to a confirmed or suspected breach that occurs within the DHA.

b. Incorporates and cancels Reference (m).

2. **APPLICABILITY.** This AI applies to:

a. All DHA personnel, to include: assigned or attached Service members, federal civilians, contractors (when required by the terms of the applicable contract), and other personnel assigned temporary, or permanent duties at DHA to include regional and field activities (remote locations).

b. All DHA workforce members requiring access to Personally Identifiable Information (PII) and/or Protected Health Information (PHI).

c. All DHA workforce members with access to the DHA network.

3. **POLICY.** It is DHA policy, pursuant to DoD policy, and in accordance with References (d) through (k), that:

a. Breach response processes and procedures are established to identify, mitigate, and contain the potential damage from the loss/compromise of PII and PHI data to institute a standard process and procedure for reporting and responding to breaches.

b. An IRT convenes to respond to all suspected or confirmed breaches that, in the discretion of the IRT Co-Chairs, are of such a significant nature as to require the coordination of the IRT.

c. All DHA workforce members report a breach upon discovery of a suspected or confirmed breach as detailed below. A breach will be treated as discovered as of the first day on which it is known or suspected, regardless of the source of the breach.

(1) Upon discovery of a breach, DHA workforce members should:

(a) Inform their supervisor immediately.

(b) Report to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour if the incident involves a confirmed cyber security incident at <https://www.us-cert.gov/forms/report> (Reference (k)).

(c) Report to the DHA Privacy and Civil Liberties Branch (DHA Privacy Office) within 1 hour by sending an e-mail to dha.ncr.pcl.mbx.dha-privacy-officer@mail.mil.

(d) If e-mail reporting is not possible, notify the DHA Privacy Office via telephone at (703) 681-7500; however, written notification must be made within 24 hours.

(2) The DHA Privacy Office will make the determination regarding whether a breach is reportable to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) under the Health Information Technology for Economic and Clinical Health (HITECH) Act and its amendments to the Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Rules.

(3) DHA Supervisors will ensure all DHA workforce members who access PII/PHI are aware of this process and the procedures for responding to suspected or confirmed breaches.

4. RESPONSIBILITIES. See Enclosure 2

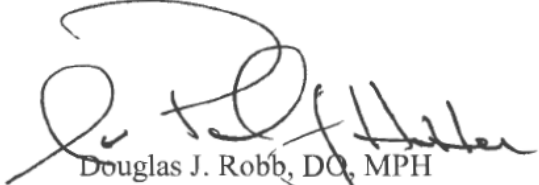
5. PROCEDURES. See Enclosure 3

6. RELEASABILITY. **Not cleared for public release.** This AI is available to DHA employees and contractor support personnel with Common Access Card authorization on the DHA Intranet.

7. EFFECTIVE DATE. This AI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with DHA Procedural Instruction 5025.01 (Reference (c)).



Douglas J. Robb, DO, MPH
Lieutenant General, USAF, MC, CFS
Director

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

Appendices

- Appendix 1: DHA Reporting/Notification Guidelines Table
- Appendix 2: DHA Breach Response Checklist
- Appendix 3: Guidelines for Reporting Breaches
- Appendix 4: DHA Breach Risk Analysis Template
- Appendix 5: Plan of Action and Milestone Template
- Appendix 6: After Action Report Template
- Appendix 7: Communication Templates
- Appendix 8: Sample Notification Letter Template
- Appendix 9: Congressional Information Paper/Letter Template
- Appendix 10: Sample Substitute Notice Template
- Appendix 11: Sample Media Announcement Template

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....6

 DIRECTOR, DHA.....6

 IRT CO-CHAIRS.....6

 CHIEF, DHA PRIVACY OFFICE.....8

 GENERAL COUNSEL/LEGAL ADVISOR.....9

 OFFICE OF THE DIRECTOR, DHA.....9

 MILITARY HEALTH SYSTEM COMMUNICATIONS DIVISION.....9

 A&MD.....10

 BUSINESS SUPPORT DIRECTORATE REPRESENTATIVE.....10

 RELEVANT PROGRAM OFFICE/DHA DIRECTORATE.....10

 HIT DIRECTORATE REPRESENTATIVE.....11

 ADDITIONAL IRT PARTICIPANTS.....12

ENCLOSURE 3: PROCEDURES.....14

 BREACH IDENTIFICATION.....14

 BREACH REPORTING FOR MHS BREACHES.....14

 CONTAINMENT.....15

 MITIGATION OF HARMFUL EFFECTS.....15

 ERADICATION.....16

 RECOVERY.....16

 FOLLOW-UP.....17

APPENDICES

 APPENDIX 1: DHA REPORTING/NOTIFICATION GUIDELINES TABLE.....18

 APPENDIX 2: DHA BREACH RESPONSE CHECKLIST.....19

 APPENDIX 3: GUIDELINES FOR REPORTING BREACHES.....22

 APPENDIX 4: DHA BREACH RISK ANALYSIS TEMPLATE.....23

 APPENDIX 5: PLAN OF ACTION & MILESTONE TEMPLATE.....24

 APPENDIX 6: AFTER ACTION REPORT TEMPLATE.....25

 APPENDIX 7: COMMUNICATION TEMPLATES.....26

 APPENDIX 8: SAMPLE NOTIFICATION LETTER TEMPLATE.....27

 APPENDIX 9: CONGRESSIONAL INFORMATION PAPER/LETTER TEMPLATE.....28

 APPENDIX 10: SAMPLE SUBSTITUTE NOTICE TEMPLATE.....29

 APPENDIX 11: SAMPLE MEDIA ANNOUNCEMENT TEMPLATE.....30

GLOSSARY.....31

 PART I: ABBREVIATIONS AND ACRONYMS.....31

 PART II: DEFINITIONS.....32

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5136.01, “Assistant Secretary of Defense for Health Affairs (ASD(HA)),” September 30, 2013
- (b) DoD Directive 5136.13, “Defense Health Agency (DHA),” September 30, 2013
- (c) DHA Procedural Instruction 5025.01, “Publication System,” August 21, 2015
- (d) DoD 6025.18-R, “Department of Defense Health Information Privacy Regulation,” January 24, 2003, (or its successor)
- (e) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007, (or its successor)
- (f) DoD Directive 5400.11-R, “Department of Defense Privacy Program,” October 29, 2014
- (g) DoD Directive 8580.02-R, “Department of Defense Health Information Security Regulation,” July 12, 2007 (or its successor)
- (h) Office of the Secretary of Defense Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII),” dated June 5, 2009
- (i) Title XIII, Subtitle D of Public Law 111-5 (also known as “Health Information Technology for Economic and Clinical Health (HITECH) Act”)
- (j) Title 45, Code of Federal Regulations, Part 160, “General Administrative Requirements,” January 10, 2014¹
- (k) Office of the Secretary of Defense Memorandum, “Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations,” August 2, 2012, (or its successor issuance)
- (l) DoD Memorandum, “New FY 2015 Annual Federal Information Security Management Act (FISMA) Breach Response and Notification Reporting Requirement,” February 20, 2015
- (m) DHA-AI No. 71, “Defense Health Agency Incident Response Team and Breach Response Requirements,” June 6, 2014 (*herby cancelled*)

¹ Incorporating modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Enforcement and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, January 25, 2013, as corrected by Technical Corrections to the HIPAA Privacy, Security and Enforcement Rules, 78 Fed. Reg. 34264, June 7, 2013 (also known as the “Omnibus Final Rule”)

ENCLOSURE 2

RESPONSIBILITIES

In cases where the following offices/individuals are unable to fulfill their duties with regard to the IRT, such offices/individuals will appoint an alternate to act with the authority to fulfill the requirements and responsibilities set forth by this AI.

1. DIRECTOR, DHA. The Director, DHA, will be responsible for the implementation of this AI to safeguard the privacy and security of PII/PHI entrusted to the DHA and to ensure reasonable and appropriate safeguards are maintained for all such PII/PHI created, maintained, received, or transmitted through electronic or non-electronic media.

2. IRT CO-CHAIRS. The IRT Co-Chairs will consist of the DHA Chief of Staff (CoS) and the Chief, DHA Privacy Office.

a. Required IRT participants are:

- (1) DHA Privacy Office;
- (2) Office of General Counsel;
- (3) Office of the Director, DHA (Front Office);
- (4) DHA Communications Division
- (5) Administration and Management Division (A&MD);
- (6) Business Support Directorate;
- (7) Relevant Program Office; and
- (8) Health Information Technology (HIT) Directorate, for electronic breaches.

b. Additional participants may be directed by the IRT Co-Chairs, such as the Human Resources Division, depending on the coordination reasonably required to respond considering the nature of the breach.

c. Serve as the central points of contact (POCs) for the IRT, and ensure participants receive all information in a timely manner.

d. Convene a meeting with the IRT and ad hoc participants, as required, within 1 business day of learning of a significant suspected or confirmed breach.

e. Report details of the breach, along with the relevant Program Office, to the IRT, including:

- (1) How and when the breach occurred;
- (2) Dates and times when the breach was discovered;
- (3) All internal and external offices that have been notified;
- (4) Current status of business operation and security of the system; and
- (5) Briefing of any other known, relevant details to the IRT.

f. Designate Action Officers (AOs) (may also be information owner or assigned POC where the breach occurred) to create and provide to the Co-Chairs:

- (1) Summary of breach;
- (2) Meeting minutes;
- (3) Updates for Senior Leadership;
- (4) Subject matter support and documentation (e.g., briefings);
- (5) Reports to external agencies, as necessary (e.g., HHS);
- (6) Establish a mitigation strategy or Plan of Action and Milestones (POA&M); and
- (7) Maintain all appropriate documentation relating to the breach, and share with the DHA Privacy Office, upon request.

g. Using DHA Privacy Office guidance, determine the associated risk of harm based on a thorough analysis of the breach and recommendations of the IRT.

h. Ensure compliance with reporting requirements, and act as the conduit of information between the information owner and the IRT.

i. Assign mitigation tasks to the IRT participants, as appropriate, and ensure completion of all assigned tasks in a timely manner.

j. Coordinate with the Business Support Directorate and other necessary Directorates and staff in estimating the costs of the breach including, but not limited to: notifying potentially affected individuals who experience issues with their credit, offering credit monitoring, providing restoration services for affected individuals, the establishment of a call center, mailings, etc.

k. Determine the appropriate representative to sign the breach notification letter and package.

l. Make recommendation to leadership for the establishment of a Breach Response Call Center, if deemed necessary.

m. Maintain documentation that the general requirements of notification to affected individuals are satisfied.

n. Maintain responsibility for the preparation of the After Action Report for Senior Leadership using the standard DHA template (Appendix 6).

o. Assist in the determination of briefings and responses to the Armed Services and Defense Appropriations Committees, as required.

p. Coordinate debrief/lessons learned for Senior Leadership.

3. CHIEF, DHA PRIVACY OFFICE. The Chief, DHA Privacy Office, will:

a. Serve as the central office POC for receiving notification of all suspected or confirmed breaches, and further report all breaches, including those at the Purchased Care Support Contractor level, to the DoD Defense Privacy and Civil Liberties Division within 48 hours.

b. Determine when an IRT is required, and notify the DHA CoS and Chief of A&MD.

c. Analyze and present, based on subject matter expertise, the risk that the PII or PHI has been compromised due to the nature of the breach.

d. Provide guidance and oversight of the breach to the AO to ensure compliance with all requirements including: reporting, individual notification, internal and external communications, and necessary mitigation steps.

e. Maintain comprehensive files on each suspected or confirmed breach detailing actions taken, to include executive summaries, e-mail communication, letters, breach response status reports, and meeting minutes for documentation, historical, and lessons learned purposes.

f. Make required breach determinations, and ensure compliance with the applicable provisions of the HIPAA Rules (including Reference (i), Parts 160 and 164, applicable to DHA as a covered entity). Actions include but are not limited to:

(1) Individual notifications;

(2) Reporting to the Secretary of HHS;

(3) Reporting to the DoD Defense Privacy and Civil Liberties Division;

(4) Notifying media, as appropriate; and

(5) Cooperating with any investigations led by HHS/OCR.

g. Lead coordination and preparation efforts for all responses to Congressional inquiries concerning a breach.

h. Conduct annual incident response training for potential IRT participants and DHA personnel workforce.

i. Track and identify organizational trends and provide training and guidance as appropriate.

j. Make final determination on when a secondary general or substitute breach notice is an appropriate response to the breach.

k. Ensure appropriate Contracting Officer's Representative (COR) and Contracting Officer (CO) are informed of the breach and involved in all relevant communications.

4. GENERAL COUNSEL/LEGAL ADVISOR. The General Counsel or servicing Legal Advisor will:

a. Provide legal advice and counsel and coordinate with the DHA Privacy Office (and as appropriate the DHA Directorate(s)) on the probability of compromise assessment and analysis, individual notification determination, and recommended mitigation actions.

b. Provide legal advice and counsel to the DHA Privacy Office, DHA Communications Division, and other appropriate offices on the development of the strategic communications plan and other communication products.

c. Provide legal advice and counsel on any other breach response legal issues.

5. OFFICE OF THE DIRECTOR, DHA. The Office of the Director, DHA (Front Office) will inform and update all Senior Leaders of Health Affairs (HA) and Office of the Secretary of Defense offices, as needed.

6. MILITARY HEALTH SYSTEM (MHS) COMMUNICATIONS DIVISION REPRESENTATIVE. The MHS Communications Division Representative will:

a. Act as the DHA spokesperson for all Public Affairs notifications, including media queries, and coordinate review and approval with the General Counsel/servicing Legal Advisor and the DHA Privacy Office.

b. Establish communication with the Military Services Medical Departments, if needed, as

well as external agencies.

c. Collaborate with the DHA Privacy Office to draft a Breach Response Strategic Communication Plan for all target audiences including media, beneficiaries, and others for implementation by DHA.

d. Serve as lead in drafting all breach-related communication products for stakeholders and coordinate review and approval with the DHA Privacy Office for privacy and HIPAA compliance purposes.

e. Provide guidance to TRICARE Service Center representatives, contract partners, and other stakeholders to respond to beneficiary inquiries.

f. Ensure information is posted on relevant Web sites.

g. Be prepared to respond to all beneficiary inquiries related to the breach.

h. Collaborate with the DHA Privacy Office on drafting and posting Frequently Asked Questions (FAQs) relating to the breach.

7. A&MD. The appropriate offices within A&MD will:

a. Secure the physical location of the breach upon request. The Security Officers at the DHA satellite offices, as directed, will secure the physical location of the breach, and notify and provide status reports of all breach-related activities to the DHA Security Manager.

b. Ensure appropriate mitigation actions are taken by Personnel Security, if necessary.

c. Ensure appropriate mitigation actions are taken by Physical Security, if necessary.

d. Ensure appropriate mitigation actions are taken by Information Security, if necessary.

8. BUSINESS SUPPORT DIRECTORATE REPRESENTATIVE. The Business Support Directorate Representative will:

a. Assess the financial implications of the breach.

b. Determine costs associated with impact, risk, and mitigation for the breach, and propose an allocation of required resources and funding to the appropriate approval authority.

9. RELEVANT PROGRAM OFFICE/DHA DIRECTORATE. The Relevant Program Office or DHA Directorate where the breach occurred will:

- a. Isolate the system to preclude any further breach activity in collaboration with the appropriate partners, such as security.
- b. Provide assistance on identifying how and why the incident occurred.
- c. Identify with the appropriate Directorates, such as the HIT Directorate, the compromised data including the identification of specific fields (name, rank, address, phone number, etc.).
- d. Provide subject matter expertise and support to the IRT in order to accurately determine the scope, probability of compromise of the PII/PHI, and sensitivity level of the breach.
- e. Ensure processes and procedures are in place for containing and monitoring the suspected or confirmed breach.
- f. Ensure mitigation tasks are executed as directed by the IRT Co-Chairs.
- g. Ensure processes and procedures, including cyber security, are followed.
- h. Notify users of system availability, when appropriate.
- i. Ensure proper reporting has taken place.
- j. Coordinate with the DHA Privacy Office prior to contacting the Defense Manpower Data Center to obtain names and addresses for the impacted population.
- k. Maintain any/all documentation regarding the suspected or confirmed breach from discovery to close until advised to be destroyed by the DHA Privacy Office or Legal Counsel.
- l. Provide necessary support and actions as required.

10. HIT DIRECTORATE REPRESENTATIVE. The HIT Directorate Representative will:

- a. Ensure compliance with cyber security reporting and notification as necessary.
- b. Secure/isolate affected equipment to prevent further breach activity.
- c. Consult with the appropriate offices to determine possible criminal activity and whether law enforcement notification is warranted from the suspected or confirmed breach.
- d. Coordinate collection of IT-related information, such as access logs, inventory of systems, and individual accounts.
- e. Conduct forensic investigations where IT expertise is needed.
- f. Receive reports of possible vulnerabilities within systems, and share expertise about

possible vulnerabilities within systems.

g. Implement mitigation strategies, and oversee mitigation actions regarding any suspected vulnerabilities in centrally managed systems.

h. Report to the IRT Co-Chairs any mitigation actions taken in response to a breach, including when the breach has been declared closed.

i. Recommend potential system actions that are warranted to prevent breaches.

11. ADDITIONAL IRT PARTICIPANTS. The participants of the IRT will vary depending on the nature of the breach. The following additional participants may be required by the IRT Co-Chairs:

a. Program Integrity Office Representative. The Program Integrity Office Representative will:

(1) Be notified if a breach is suspected or confirmed to be a malicious breach, or involve fraud concerning PII and/or PHI.

(2) Serve as DHA's liaison with law enforcement. Law enforcement notification should not be delayed.

b. Program Integration Representative. The Program Integration Representative will:

(1) Coordinate, review, and submit notification to the congressional defense committee.

(2) Serve as the DHA breach response representative for congressional offices.

c. Procurement Division Representative. The Procurement Division Representative will:

(1) Coordinate with the Program Offices, in consultation with the DHA Privacy Office and General Counsel/Legal Advisor, as necessary, to enable Program Offices to comply with requirements to ensure DHA's purchased care, dental, and other contractors have appropriate provisions in any agreements or contracts for reporting and responding to suspected or confirmed breaches occurring within their purview.

(2) Coordinate required acquisition actions, which may include credit monitoring and call center support.

(3) Evaluate contract language.

- (4) Determine potential contract violation.
- (5) Be available to assist in obtaining contracting information for credit monitoring services.

ENCLOSURE 3

PROCEDURES

The following are key steps necessary to execute a comprehensive and effective breach response program. Depending on the nature of the breach, these activities may be done sequentially, in parallel, and in addition; steps may be repeated. The DHA Privacy Office has the expertise to assist with carrying out any of the below steps.

1. BREACH IDENTIFICATION. Recognizing that an event has occurred and initiating next steps.
 - a. Gather all available information, and make required assessments.
 - b. Confirm and classify the scope, risk, and severity of the breach.
 - c. Determine an appropriate plan of action.
 - d. Coordinate legal issues with the Office of the General Counsel or servicing Legal Advisor.
 - e. Document and record all actions taken upon discovery of a suspected or confirmed breach.

2. BREACH REPORTING FOR MHS BREACHES. Reporting the breach to the established chain of command in a timely manner.
 - a. For internal reporting, DHA workforce members must immediately report a suspected or confirmed breach to their supervisor. The following must then take place:
 - (1) Notify the appropriate Branch Directorate.
 - (2) Notify US-CERT (of only confirmed cyber security related breaches).
 - (3) Notify the DHA Privacy Office (via e-mail, or telephone if necessary).
 - (4) Report all potentially malicious breaches to DHA Program Integrity and DoD Defense Criminal Investigative Service (DCIS), if necessary.
 - (5) The Chief, DHA Privacy Office, will notify the DHA CoS and the Chief of A&MD, when necessary.
 - (6) The DHA CoS will notify the Director, DHA, other Senior Leadership, MHS Communications Division, and Program Integration as deemed necessary.

b. For Service-level breaches, the DHA Privacy Office will review and monitor all individual notifications of breaches involving PII/PHI and will coordinate with the respective Service POCs, as needed.

(1) For breaches determined to meet the requirements of a breach reportable to HHS/OCR, the DHA Privacy Office will initiate reporting and associated individual notification requirements, working closely with the Service POC.

(2) The Director, DHA, or designee will inform the Assistant Secretary of Defense for Health Affairs (ASD(HA)) as deemed necessary.

c. Additional internal and external reporting is coordinated by the IRT Co-Chairs with the DoD Components, if needed, to ensure:

(1) All reporting, including reports to Congress, DoD leadership, ASD(HA), Under Secretary of Defense for Personnel and Readiness, Service medical departments, media/press, and Congress are completed appropriately.

(2) Individual notification occurs within the required time period.

d. If criminal activity is suspected, appropriate law enforcement organizations, such as the DCIS, and/or counterintelligence must be contacted.

e. In the event of a breach where a contractor is accountable, the AO must maintain chronological tracking documentation and, as needed with the appropriate COR and CO, provide the necessary information to the IRT.

3. CONTAINMENT. Limiting the impact of the breach.

a. For electronic breaches, determine a course of action concerning the operational status of the compromised system, and identify the critical information and/or computing services affected by the breach.

b. For non-electronic breaches, identify the best strategy to minimize the impact of the breach.

c. Follow existing guidance regarding containment requirements. For example, determine if the compromised information should be left on the current system or if the system should be taken offline and the information transferred to alternative media.

d. Provide regular or situational updates to the DHA Privacy Office (and upon request by the IRT Co-Chairs).

4. MITIGATION OF HARMFUL EFFECTS. Communicating with potentially affected individuals, investigators, and other involved entities.

a. The Information/System Owner will mitigate the harmful effects of all breaches (both electronic and paper) by implementing or creating a mitigation strategy and, as necessary, a POA&M, which includes:

- (1) Immediately securing the affected information as much as practicable.
- (2) Applying appropriate administrative, physical, and technical safeguards.
- (3) Notifying the Information/System Owners and the appropriate Program Office of the breach.

b. Contractors operating under a business associate agreement (BAA) will, at their own expense, take action to mitigate, to the extent practicable, any harmful effect known to the contractor as a result of a violation of the requirements of the BAA clause such as deletion of e-mail communications and files as appropriate. Additionally, the contractor will keep the DHA Privacy Office apprised of all actions taken in response to a suspected or confirmed breach. Contractors should be reminded of their responsibilities and requirements to comply with Reference (i).

c. Action Steps for IRT:

- (1) If a breach of PII/PHI held by a contractor has occurred, notification of affected individuals will be made by the contractor's senior executive upon DHA Privacy Office review and approval of the notification letter.
- (2) Notify/update senior leadership of the breach.
- (3) Draft appropriate reports for DHA Senior Leadership, as appropriate.
- (4) Determine whether individual notification is required and, if so, determine the appropriate means of such notification.

5. ERADICATION. Removing the cause of the breach and alleviating vulnerabilities.

a. The AO must make every effort to remove the cause of the breach to prevent and mitigate any vulnerability.

b. Examples of such actions include: wiping a hard drive clean or deleting any computer viruses.

6. RECOVERY. Restoration of business operations to normal status.

a. Follow existing and published guidance regarding recovery requirements.

- b. Document recovery response actions.
 - c. Execute the necessary changes to business practices and/or network/system.
 - d. Conduct forensic analysis of the servers or business processes, as appropriate.
 - e. Fully restore system and data.
 - f. Notify users of system availability and updates, as appropriate.
7. FOLLOW-UP. Taking necessary actions to prevent future occurrences.
- a. Ensure all tasks in the mitigation strategy or POA&M are completed.
 - b. Create a debrief for Senior Leadership.
 - c. Develop a lessons learned document, including actions taken immediately following the breach and actions planned moving forward.
 - d. Amend and disseminate operating policies and procedures.
 - e. Share lessons learned with workforce.
 - f. Provide subsequent workforce training and awareness lessons.
 - g. Identify needed personnel actions such as sanctioning or counseling.

APPENDIX 1

DHA REPORTING/NOTIFICATION GUIDELINES TABLE

| Task | Timeline |
|---|---|
| <ul style="list-style-type: none"> • Notify your Supervisor/Director | - Immediately, upon discovery |
| <ul style="list-style-type: none"> • *Notify US-CERT | - Within 1 hour only if breach is confirmed as cyber-security related |
| <ul style="list-style-type: none"> • If breach is <u>internal to DHA</u>, report to DHA Privacy Office at dha.ncr.pcl.mbx.dha-privacy-officer@mail.mil | - Within 1 hour |
| <ul style="list-style-type: none"> • Notify the Agency Privacy Officer/Senior Representative for the Service/Senior Component for Privacy | - Within 24 hours |
| <ul style="list-style-type: none"> • Report MHS-related breaches, <u>external to DHA**</u> to the DHA Privacy Office at dha.ncr.pcl.mbx.dha-privacy-officer@mail.mil and CO. • Non MHS-related breaches should be reported to the appropriate chain of command or supervision | - Within 24 hours |
| <ul style="list-style-type: none"> • Notify Strategic Communications and Program Integration | - Within 24 hours |
| <ul style="list-style-type: none"> • Notify the DoD Defense Privacy and Civil Liberties Division and Component Head | - Within 48 hours - Completed by the DHA Privacy Office for breaches internal to DHA |
| <ul style="list-style-type: none"> • Notify all affected individuals, if required by the DHA Privacy Office | - Within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained |
| <ul style="list-style-type: none"> • Notify DCIS | - If criminal activity is a potential element of the breach |
| <ul style="list-style-type: none"> • Notify issuing banks | - If government issued credit cards are involved |

* US-CERT no longer requires reporting of breaches involving paper; notification is required of only confirmed cyber-security related incidents (notification of suspected cyber-security related incidents is voluntary)

** External MHS breaches include those that take place outside of a DHA covered entity, such as a military treatment facility under the Department of the Army or a Purchased Care Contractor.

APPENDIX 2

DHA BREACH RESPONSE CHECKLIST

Date and Time Breach Occurred: _____

Date and Time Breach Discovered: _____

Location of Breach: _____

Number of Potentially Affected Individuals:

Breach Requires Reporting to the Department of Health and Human Services (HHS): Yes / No

Date Supervisor Notified: _____

Date DHA Privacy Office Notified: _____

Breach point of contact (POC) (Name and Contact Information): _____

Notification

____ US-CERT (within 1 hour if breach is confirmed as cyber-security related)
○ Date Completed: _____

____ Branch Privacy Officer/Senior Privacy Representative (within 1 hour)
○ Date Completed: _____

____ DHA Leadership
○ Date Completed: _____

____ DoD Defense Privacy and Civil Liberties Division and Component Head (within 48 hours)
○ Date Completed: _____

____ DHA Program Integrity and DCIS if breach is suspected or confirmed to be malicious
○ Date Completed: _____
○ Name of Notified Individual(s): _____

____ Affected individuals within 10 working days of breach discovery and ascertainment of contact information, if necessary
○ Date Completed: _____

____ HHS Secretary, if necessary
○ Date Completed: _____

____ Prominent media outlets, if necessary
○ Date Completed: _____
○ Name of Notified Media: _____

Assigned Action Officer(s): Obtain the following information regarding the breach:

____ Type of data compromised including specific categories (i.e., Social Security Numbers, names, medical diagnoses, home addresses, etc.)

_____ Mitigation, containment, and eradication efforts taken in response to the breach

_____ Number and identification (i.e., active duty, retirees, reservists, dependents, civilians) of potentially affected individuals

Incident Response Team

_____ Convene meeting within 1 day of breach discovery and include all appropriate parties

_____ Coordinate with information owner and/or the Program Office’s designated POC who serves as a subject matter expert with regard to the program office’s operations to assist in obtaining relevant information pertaining to the breach

- The Privacy Office will determine the level of risk to the affected individuals and, if notification will be required, the DHA Privacy Office determines whether DHA, other DoD Component, or the contractor will notify the affected individual(s)

_____ Report investigation updates to the IRT Co-Chairs and DHA Privacy Office

_____ Determine a course of action for the operational status of the compromised system, physical space, or business practice

_____ Document and preserve all actions pertaining to the investigation of the breach, including containment and mitigation actions

_____ Assist in estimating costs associated with the breach, including mitigation actions such as notifying the affected individuals

_____ Document lessons learned and provide to DHA Privacy Office

_____ Develop a comprehensive final report (After Action Report – See Appendix 6)

Individual Notification

_____ Draft notification letter

- If required, the contractor will obtain DHA approval of letters

_____ Coordinate with Defense Manpower Data Center (DMDC) to obtain affected individual contact information

_____ Coordinate final approval process through DHA Privacy Office

_____ Deputy Director, DHA, determines who will sign the final letter

_____ Mail signed letters with all necessary enclosures and attachments

_____ Coordinate with DMDC in gathering information pertaining to individuals for whom letters were returned

_____ Assist in documenting those individuals without current contact information

_____ Establish a call center to provide responses to affected individuals who have additional questions/concerns

FOR DHA PRIVACY REFERENCE, AS NEEDED

| | |
|--------------------------|--|
| Breach Report Received | |
| Breach Reported to DPCLD | |
| Breach Reported to HHS | |
| Breach Reported to Media | |
| Breach Resolved | |

_____ Establish a website to include general information pertaining to the breach, FAQs, and guidance concerning identity theft, along with contact information for credit bureaus

_____ Ensure press releases are prepared and issued, if necessary

FOR DHA PRIVACY REFERENCE, AS NEEDED

| | |
|--------------------------|--|
| Breach Report Received | |
| Breach Reported to DPCLD | |
| Breach Reported to HHS | |
| Breach Reported to Media | |
| Breach Resolved | |

APPENDIX 3: GUIDELINES FOR REPORTING BREACHES



Guidelines for Reporting Breaches

Purpose:

Protecting the privacy and security of personally identifiable information (PII) and protected health information (PHI) is the responsibility of all DHA Directorates, Divisions, and Special Staff elements, to include the TRICARE Regional Offices, TRICARE Area Offices, and all other organizational entities within DHA. All of DHA must adhere to the reporting and notification requirements set forth in the DoDD 5400.11, "Department of Defense Privacy Program," October 29, 2014, Office of the Secretary of Defense Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2009; DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, or its successor issuance; and DoD 6025.18-R, "Department of Defense Health Information Privacy Regulation," January 24, 2003, or its successor issuance.

Definition:

DoDD 5400.11 defines "lost, stolen or compromised information," otherwise termed a breach, as follows:

"A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic."

The DHA Privacy Office will determine whether a breach meets the requirements of reporting to the Department of Health and Human Services (HHS).

Guidance:

This document outlines the DoD Reporting and Notification Requirements for breaches:

1. Notify your Supervisor/Director (immediately, upon discovery)
2. *Notify the United States Computer Emergency Readiness Team (within 1 hour only if the breach is confirmed as cyber-security related, e.g., not a paper breach)*
 - If breach is internal to DHA, report to the DHA Privacy Office within 1 hour.
3. Notify the Agency Privacy Officer/Senior Representative for the Service/Senior Component for Privacy (within 24 hours)
 - If breach is external to DHA, report to the DHA Privacy Office within 24 hours at dha.ncr.pcl.mbx.dha-privacy-officer@mail.mil or (703) 681-7500 and the Contracting Officer within 24 hours.
 - The DoD breach reporting form (DD Form 2959) is available on the DHA Privacy Office website at: <http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI>
4. Notify the DoD Defense Privacy and Civil Liberties Division and Component Head (within 48 hours) (completed by the DHA Privacy Office)
5. Notify all affected individuals within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, if required by the DHA Privacy Office
6. Notify law enforcement authorities, if necessary
7. Notify issuing banks if government issued credit cards are involved

If PHI is involved, please refer to DHA Privacy Office guidance for additional breach reporting and notification actions as required by the HHS Final Omnibus Rule and Title 45, CFR, Parts 160 and 164.

Breaches often occur when PII or PHI is mishandled. Examples of these types of breaches may include, but are not limited to:

- Misdirected fax documents that reach anyone other than the intended recipient
- Failing to properly secure documents when mailing or transporting
- Lost or stolen removable media devices (e.g., laptops, thumb drives, compact discs)
- Transmission of unsecured e-mails and unencrypted files
- Unauthorized access to computer systems
- Inappropriate disposal of documents
- Inadvertent posting on the internet

APPENDIX 4

DHA BREACH RISK ANALYSIS TEMPLATE

| Section 1. | | |
|--|-------------------|------------|
| Covered Entity Involved | Date of Discovery | Tracking # |
| Total Number of Potentially Impacted Individuals | | |

| Section 2. |
|---|
| <p>1) Is the information unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Department of Health and Human Services (refer to section 13402(h)(2) of HITECH Act)? Yes or No</p> <p><i>If Yes, then STOP here. No breach has occurred that requires notification. If No, then proceed to next question.</i></p> |
| <p>2) Is there evidence to indicate that the information was NOT viewed or accessed by an unintended/unauthorized party? Yes or No</p> <p><i>If Yes, then STOP here. No breach has occurred that requires notification. If No, then proceed to next question.</i></p> |

| Section 3. |
|--|
| <p>Do one of the following exceptions apply? Yes or No</p> <p><i>If Yes, select the appropriate exception below.</i></p> <ul style="list-style-type: none"> a. Good faith, unintentional acquisition, access, or use of PHI, within the scope of duty, by an employee/workforce member of a covered entity. b. Inadvertent disclosure to another person authorized to handle PHI within the covered entity. c. Recipient could not reasonably have retained the data. |

| Section 4. |
|-----------------------------------|
| <p>Final Determination</p> |

APPENDIX 5

PLAN OF ACTION AND MILESTONE TEMPLATE

Recommended when significant mitigation steps are warranted.

| Task for Mitigation | Priority | Milestone | Milestone Due Date | Status | Date of Completion | Point of Contact | Comments |
|---------------------|----------|-----------|--------------------|--------|--------------------|------------------|----------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

***The DHA Privacy Office will provide guidance on the breach response documentation and report frequency requirements**

Task for mitigation – Action to be taken to prevent the breach from reoccurring. Ex: Provide refresher training for employees.

Priority – Low, medium, or high - depending on the severity of the breach.

Milestone – Specific action steps that support the completion of the task for mitigation. Multiple milestones can support the completion of a single task.

Milestone due date – The date the individual milestone is scheduled to be completed

Status – Field to track the progress of the task. Ex: In progress or Completed

Date of Completion – The date the task or milestone has been completed

Point of contact – The name of the person responsible for ensuring the completion of the milestone or task

Comments – Provide additional information on the task or milestone

APPENDIX 6

AFTER ACTION REPORT TEMPLATE

Summary of the Incident:

Actions Taken:

What Went Well:

Areas for Improvement:

Recommendations:

| | | | |
|--------------------------|--|-------------------------|----------------|
| Breach Report Received | | | |
| Breach Reported to DPCLD | | | |
| Breach Reported to HHS | | | |
| Breach Reported to Media | | | |
| Breach Resolved | | | |
| | | Privacy Office Approval | Signature Date |

APPENDIX 7

COMMUNICATION TEMPLATES

The communication templates that follow (Appendices 8–11) are being provided as reference, sample materials. These templates are subject to change at any time dependent upon the specific circumstances surrounding the breach.

APPENDIX 8

SAMPLE NOTIFICATION LETTER TEMPLATE

[Use Appropriate Letterhead]

Date

Name

Address

City/State/Zip

Subject: Notification of Disclosure

Dear _____:

[Insert Organization] is [insert explanation of who the letter is coming from]. This letter is to notify you of the potential compromise of your Personally Identifiable Information and Protected Health Information as it is essential that individuals remain aware of any events that may affect their privacy.

The potential compromise occurred on [Insert Date], when [Insert Details Surrounding Breach]. The data elements involved include, [Insert Data Elements]. On [Insert Date of Discovery], we were notified, and we immediately conducted response efforts, including an investigation. To prevent any future similar occurrences, we [Insert Mitigation Actions].

[Insert details regarding risk of harm to patients and what steps affected individuals can take to protect themselves from identity theft].

We take this potential compromise very seriously. We value [Insert Population] and share the goal of safeguarding your information. On behalf of [Insert Organization Name], I apologize for any inconvenience and concern this issue may have caused you. We look forward to providing further health care management services to you. If you have further questions or concerns, please contact [Insert Contact Name, Number, and E-mail].

Sincerely,

[Insert Signature Block of Responsible,
Senior-Level Individual]

APPENDIX 9

CONGRESSIONAL INFORMATION PAPER/LETTER TEMPLATE

On, [Insert date], [Insert component/organization] discovered/reported a data breach involving Personally Identifiable Information and Protected Health Information that may impact approximately [Insert number of individuals affected] TRICARE beneficiaries. [Insert breach details].

Upon discovery on [Insert date], the [Insert component/organization] immediately began an investigation and [Insert mitigation actions]. Additionally, [Insert actions recommended to potentially impacted individuals to protect themselves from fraud or identity theft].

[Insert the overall impact of the breach, the breach's current status, and issues that remain to be resolved].

[Insert component/organization] takes the protection of privacy very seriously. [Insert what the component/organization is doing to mitigate harm to individuals and prevent future occurrences]. Maintaining the privacy and security of beneficiary information is one of the Defense Health Agency's greatest concerns. We are proud to serve our Nation's military heroes and their families and are committed to providing them the best possible health care.

If you have any questions or concerns, please direct them to [Insert contact information].

Frequently Asked Questions:

[Insert FAQs based on details relevant to the breach]

SAMPLE FAQs:

1. *How many individuals were affected?*
2. *What information was potentially compromised?*
3. *How did the breach occur?*
4. *What actions can potentially affected individuals take as a result of the breach?*

APPENDIX 10

SAMPLE SUBSTITUTE NOTICE TEMPLATE

On, [Insert date], [Insert component/organization] discovered that [Insert breach details including: when the breach occurred, the nature of the breach, and the Personally Identifiable Information and Protected Health Information data elements involved].

Upon discovery, the [Insert component/organization] immediately began an investigation and [Insert cause of the breach, if known]. To mitigate this incident and prevent future similar occurrences, [Insert mitigation and other relevant actions taken].

While there is no evidence to indicate that any personal information was used in a malicious manner [Omit if the aforementioned statement is known to be false], it is the Department of Defense's and [Insert component/organization] policy to notify individuals of any event that may affect their privacy. Each affected individual, for which a current address was located, was notified of the details surrounding this breach via letter. The letter also provided impacted beneficiaries with constructive assistance regarding actions available to further safeguard their personal information.

Concerned individuals should be guided by the actions recommended by the Federal Trade Commission (FTC) at: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>. The FTC site provides instructions for placing a free fraud alert on credit reports and also other valuable information regarding actions that can be taken now or in the future, should any problems develop. [Insert additional steps, if necessary].

We have taken additional measures to assist our beneficiaries who may be concerned if they were impacted by this breach. Affected individuals may contact [Insert name of contact individual, if applicable, phone number and e-mail address].

APPENDIX 11

SAMPLE MEDIA ANNOUNCEMENT TEMPLATE

On, [Insert date], [Insert component/organization] discovered that approximately [Insert number of individuals affected] patients' Personally Identifiable Information and Protected Health Information from [Insert location] was [Insert breach details].

Upon discovery on [Insert date], the [Insert component/organization] immediately began an investigation and [Insert mitigation actions]. Additionally, you [Insert steps individuals should take to protect themselves].

[Insert component/organization] takes the protection of privacy very seriously; we are [Insert what the component/organization is doing to mitigate harm to individuals and prevent future occurrences].

If you have any questions, please direct them to [Insert contact information].

Frequently Asked Questions (FAQs):

[Insert FAQs based on details relevant to the breach]

SAMPLE FAQs:

- 1. How many individuals were affected?*
- 2. What information was potentially compromised?*
- 3. How did the breach occur?*
- 4. What actions can potentially affected individuals take as a result of the breach?*

GLOSSARY

PART I: ABBREVIATIONS AND ACRONYMS

| | |
|---------|--|
| AI | Administrative Instruction |
| A&MD | Administration and Management Division |
| AO | Action Officer |
| ASD(HA) | Assistant Secretary of Defense for Health Affairs |
| BAA | business associate agreement |
| CFR | Code of Federal Regulations |
| CO | Contracting Officer |
| COR | Contracting Officer's Representative |
| CoS | Chief of Staff |
| DCIS | Defense Criminal Investigative Service |
| DHA | Defense Health Agency |
| DHA-AI | Defense Health Agency Administrative Instruction |
| DMDC | Defense Manpower Data Center |
| FAQs | Frequently Asked Questions |
| HA | Health Affairs |
| HHS | Department of Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act |
| HITECH | Health Information Technology for Economic and Clinical Health |
| IRT | Incident Response Team |
| IT | Information Technology |
| MHS | Military Health System |
| OCR | Office for Civil Rights |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| US-CERT | United States Computer Emergency Readiness Team |

PART II: DEFINITIONS

AO. A designated DHA workforce member(s) with subject matter expertise within the Directorate or Program where the breach occurred who serves as the lead breach response POC and helps implement response actions on behalf of the DHA Directorate/Program Office.

breach or DoD breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

covered entity. A health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

cyber security incident. A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices (National Institute of Standards and Technology Special Publication 800-61). In general, types of activity that are commonly recognized as being in violation of a typical security policy include, but are not limited to, attempts (either failed or successful) to gain unauthorized access to a system or its data, including PII-related incidents, unwanted disruption or denial of service, the unauthorized use of a system for processing or storing data and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

HHS breach. The acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. HHS's definition of a breach excludes:

- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

- A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (Please note an HHS breach is different from a DoD privacy breach).

Information/System Owner. The official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. In most cases, may also be the AO.

IRT. A multidisciplinary team to foster information sharing and facilitate coordinated responses to breaches.

MHS. DoD organized health care arrangement, which includes all DoD health plans and all DoD health care providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by DHA, the Army, the Navy, or the Air Force. Not all health care providers affiliated with the Armed Forces are covered entities; among those who are not providers associated with Military Entrance Processing Stations and Reserve Components practicing outside the authority of military treatment facilities who do not engage in electronic transactions.

PHI. Individually identifiable health information that relates to the individual's past, present, or future physical or mental health, the provision of health care, or the payment for health services, and that identifies the individual or it is reasonable to believe the information can be used to identify the individual. PHI excludes information contained in employment records held by a covered entity in its role as an employer. PHI is a subset of PII.

PII. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a Social Security Number; age; military rank; civilian grade; marital status; race; salary; home/office phone number; biometric; personnel; medical; and financial information; and any other information that is linked or linkable to a specified individual. This also includes information which can be used to distinguish or trace an individual's identity and any other personal information which is linked or linkable to a specified individual.

workforce member. Workforce members are DoD and other government employees, military Service members, contractor and subcontractor employees, and other agents whose conduct, in the performance of work for or on behalf of DHA, is under the direct control of DHA or a DHA contractor or subcontractor.