TMA Privacy Office Information Paper

SPECIFICATIONS: SECURITY INCIDENT PROCEDURES

HIPAA Security ♦ September 2012

I. Supporting Regulations for this Information Paper

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (45 C.F.R. § 164.308(a)(6)) establishes the requirements for security incidents.

B. The Department of Defense (DoD) Health Information Security Regulation (DoD 8580.02-R, C2.7.) implements the aforementioned section of the HHS HIPAA Security Rule within the Military Health System.

C. The TRICARE Management Activity (TMA) Memorandum, "Incident Response Team and Breach Notification Policy Memorandum," November 5, 2009 provides guidance on TMA security incident and breach procedures.

D. TRICARE Management Activity (TMA) "Guidelines for Reporting Lost, Stolen, or Compromised Personally Identifiable and/or Protected Health Information," May 12, 2011 provides guidance on TMA security incident procedures.

E. Military Health System (MHS) Information Assurance (IA) Implementation Guide, "Incident Reporting and Response Program," February 22, 2012 provides the MHS implementation guidance for incident reporting.

F. Department of Defense (DoD) 5400.11-R, "Department of Defense Privacy Program," May 14, 2007 establishes the definition of a 'breach'.

G. Office of Management and Budget (OMB) Memorandum (M) 07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," May 22, 2007 provides guidance on breach notification.

II. Guidance For Standards and Implementation Specifications

A. The first part of the Security Incident Procedures standard within the Security Rule ("the Rule") (45 C.F.R. § 164.308(a)(6)(i) and DoD 8580.02-R, C2.7.1) requires covered

entities to "implement policies and procedures to address security incidents," including developing the associated procedures for handling security incidents and breaches involving electronic Protected Health Information (ePHI). PHI is individually identifiable health information maintained by a covered entity and can include such identifiers as names, addresses, telephone numbers, medical records, social security numbers, and other information that could be used to identify an individual. ePHI is PHI that is transmitted or maintained in electronic form.

B. A security incident, as defined by the Rule, is "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system."
   1. Some examples of security incidents include policy violations, denial of service attacks, malicious software, intrusions, unauthorized disclosures, or cases in which an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.

   2. It should be noted that ensuring PHI is encrypted at all times, while in transit (e.g. email) and at rest (e.g. hard drive encryption on your laptop), is the only acceptable security control that prevents a loss of PHI from needing to be reported as a breach.

C. The second part of the Security Incident Procedures standard within the Security Rule ("the Rule") (45 C.F.R. § 164.308(a)(6)(ii) and DoD 8580.02-R, C2.7.2) outlines a covered entities responsibilities as they pertain to the "response and reporting" of security incidents. The requirements include ensuring processes and procedures are in place for each of the following areas:

   1. Identification and response to suspected or known security incidents;
   2. Mitigation, to the extent practicable, of harmful effects of security incidents that are known or suspected; and
   3. Documentation of the incidents and their outcomes

D. Offices should ensure they establish, and are aware of, the appropriate response procedures for all levels of incidents.

   1. For example, in the case of TMA, the TMA HIPAA Security Officer works collaboratively with the Office of the Chief Information Officer/Information Assurance (OCIO/IA), and members of TMA leadership to develop and ensure the applicable TMA policies and procedures are in place (see Supporting Regulations and References for further information).

   2. The developed procedures demonstrate how TMA identifies and responds to suspected or known security incidents; mitigates, to the extent practicable, the harmful effect(s) of security incidents; and documents the incidents and their outcomes.

E. It is important to note the difference between a "security incident" and a "breach." See definitions.

F. Per DoD 5400.11-R (reference F), all security incidents must be reported, and security incidents involving either personally identifiable information (PII) or protected health information (PHI) must be reported to the United States Computer Emergency Readiness Team (https://forms.us-cert.gov/report/) and the TMA Privacy and Civil Liberties Office (PrivacyOfficerMail@tma.osd.mil or (703) 681-7500) within 1 hour of becoming aware of the situation/event (see Figure 1 for a reporting decision tree and Appendix A for the TMA Breach Reporting form).

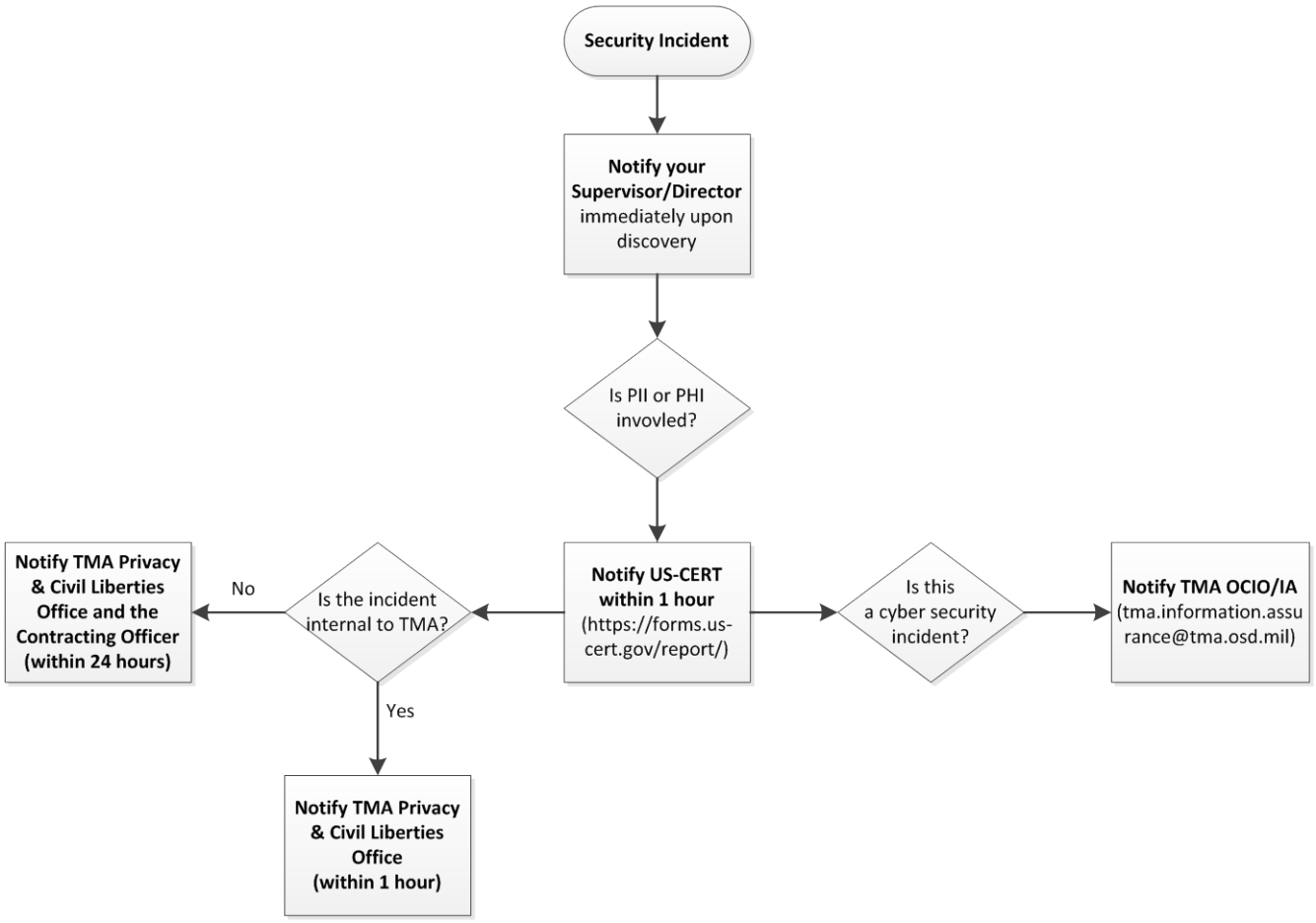
G. Typically, users are not in a position to determine if a breach has occurred or not. (See the definitions section for the difference between a "security incident" and a "breach.") That determination is made after a proper investigation that involves the TMA Privacy Office.

1. The TMA Privacy Office will work with the OCIO/IA, Office of General Counsel, the TMA Incident Response Team (IRT), and other relevant departments and agencies to determine if the incident qualifies as a breach under the provisions of the Health and Human Services (HHS) Breach Rule and will subsequently report the incident directly to the Secretary, HHS, as appropriate.

2. In instances where reporting to HHS is required, the TMA Privacy Office, Director, will report the incident to HHS and provide courtesy notification to the TMA Component.

Figure 1

Security Incident Reporting Procedures
For TMA Incidents involving PII/PHI



III. Definitions Associated with Standards and Implementation Specifications

A. Breach: The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information in which persons other than authorized users gain access or potential access to such information for other than authorized purposes in which one or more individuals will be adversely affected (Department of Defense (DoD) 5400.11-R, "DoD Privacy Program," May 14, 2007 and further enforced by the Health Information Technology for Economic and Clinical Health (HITECH) Act, February 17, 2009). Examples of breaches include but are not limited to unauthorized use of another user's account, unauthorized use of system privileges, extraction, or unauthorized release of DoD sensitive information (SI), and execution of malicious code that destroys DoD SI.

B. Covered Entity: A health plan or a healthcare provider who transmits any health information in electronic form in connection with a transaction (see DoD 6025.18-R, paragraph DL1.1.35.) covered by this Regulation, e.g. ACS X12N 837 healthcare claims, ASC X12N 270/271 eligibility inquiries and responses, and the electronic forms of other transactions identified at DoD 6025.18-R, DL1.1.35. In the case of a health plan administered by the Department of Defense, the covered entity is the DoD Component (or subcomponent) that functions as the administrator of the health plan. (See DoD 6025.18-R, paragraph DL1.1.17. for additional information on health plan administrators.) To the extent this Regulation prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. Under subparagraph DoD 6025.18-R, C3.2.2., all covered entities of the Military Health System (MHS) (including both health plans and healthcare providers) are designated as a single covered entity. Not all healthcare providers affiliated with the Armed Forces are covered entities; among those who are not are providers associated with Military Entrance Processing Stations (MEPS) and Reserve components practicing outside the authority of military treatment facilities (MTFs) who do not engage in electronic transactions covered by the Regulation.

C. Documentation: Written security plans, rules, procedures, and instructions concerning all components of an entity's security program, and written records of any action, activity, or assessment required by HIPAA and DoD 8580.02-R, C1.6.4.5.

D. Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

E. Military Health System (MHS): All DoD health plans and all DoD healthcare 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 TRICARE Management Activity (TMA), the Army, the Navy, or the Air Force.

F. Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by a covered entity in its role as an employer.

Appendix A:

MEMORANDUM FOR DoD BREACH REPORTING:
Can be found online at: http://www.tricare.mil/tma/privacy/breach.aspx

SUBJECT: Lost, Stolen, or Compromised Personally Identifiable Information

1a. Date of Breach: **1b. Breach Discovery Date:**

2a. US-CERT Number: **2b Date Reported to US-CERT:**

3. Is this the initial report to the TMA Privacy and Civil Liberties Office? ☐ **Yes** ☐ **No**

3a. If no, what were the dates of the previous reports?

(Note: Report updates should be made in red text.)

4. DoD Component/Organization involved:

Component Name	
Organization	
POC Title/Organization	
Telephone	
Email	

5. Business Associate involved (if applicable):

Business Associate Name	
Address	
POC Title/Organization	

Telephone	
Email	

6. Person to contact for further information regarding this report.

Name	
Address	
Title/Organization	
Telephone	
Email	

7. Total number of individuals affected by the breach: Unknown ☐

7a. Breakout number by category:

Government Civilians		**Government Contractors**	
Military (Reserve)		**Military (Dependent)**	
Military (Active)		**Military (Retired)**	
Other/Unknown (please specify)			

7b. If the total number of affected individuals is greater than 500, do those affected reside in the same state or jurisdiction? ☐ **Yes** ☐ **No** ☐ **N/A If no, please explain.**

8. Did this incident involving one of the following:

(Double click each box to select those that apply):

☐ Paper Records	☐ Info-Sharing

☐ Equipment	☐ Record Disposal
☐ E-mail	☐ Other (specify)

8a. If the breach involved equipment, what and how many pieces of equipment were involved in the incident? ☐N/A **(Double click each box to select those that apply):**

Type of Equipment	How Many	Type of Equipment	How Many
☐CPU		☐External Hard drive	
☐Laptop		☐IPOD	
☐Blackberry		☐Cell Phone	
☐Data Stick		☐Network Intrusion	
☐Flash drive		☐ Other (specify)	

8b. How was the equipment protected? (Double click each box to select all that apply):

Personally Owned	☐	**Password Protected**	☐
Encryption Software installed	☐	**PKI/CAC Enabled**	☐
Contractor Owned	☐	**Not protected**	☐
Government Owned	☐	Other (specify)	☐

8c. If the breach involved e-mail complete the following:

(Double click each box to select those that apply):

Select all that apply	Yes	No
E-mail was encrypted	☐	☐

E-mail sent outside of DoD (e.g., to public, other Federal agency)	☐	☐
non-Federal agency	☐	☐
Other (specify)	☐	☐

8d. Type of Personally Identifiable Information involved in the incident (Double click each box to select all that apply): If PHI is involved, please specify the elements in item #9 (description).

Type of PII	**Select all that apply**	**Type of PII**	**Select all that apply**
Social Security Numbers (SSN)	☐	DOB	☐
Names	☐	PHI (health information)	☐
Personal home addresses	☐	Financial information containing PII	☐
Personal phone numbers	☐	Passwords	☐
Personal e-mail address	☐	Other (specify)	☐

9. Description of breach. (150 words or fewer; bulleted format is acceptable)

10. Describe actions taken in response to the breach. (150 words or fewer; bulleted format is acceptable)

11. Potential impact of the breach based on risk assessment (refer to the Risk Assessment Model in Appendix A of DA&M Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", June 5, 2009)**:**

a) LOW: The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

b) MODERATE: The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

c) HIGH: The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

12. Date Individual Notice Provided (if applicable)?

12a. Substitute Notice Required (y/n)? If yes, please explain the method used in providing this notice.

12b. Date Media Notice Provided (if applicable)?

13. Person submitting this report if different than #4 and #5.

Name	
Address	
Title/Organization	
Telephone	
Email	