

JUNE 7-8, 2011

TMA Privacy Weekly

TMA Privacy and Civil Liberties Office
2011 DATA PROTECTION SEMINAR



Breach Response



Breach Response Purpose

The purpose of this presentation is to provide a thorough understanding of the requirements of TRICARE Management Activity (TMA) personnel when assessing and responding to a breach.



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response Objectives

- Upon completion of this presentation, you should be able to:
 - Describe the key components of breach reporting, notification, and mitigation
 - Define your role in identifying and responding to breaches
 - Identify the three components of the TMA Breach Notification Administrative Instruction (AI) (formerly known as the Breach Notification Standard Operating Procedure (SOP))



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response Definitions

- **Personally Identifiable Information (PII):** Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

Definitions (continued)

- **Protected Health Information (PHI):** Individually identifiable information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to:
 - The past, present, or future physical or mental health, or condition of an individual
 - Provision of health care to an individual
 - Payment for the provision of health care to an individual
- If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered PHI



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

Definitions (continued)

- **Breach:** Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

General Examples of Breaches

- Examples of breaches include:
 - Unauthorized use of another user's account
 - Unauthorized use of system privileges and data extraction
 - An unencrypted e-mail containing PII/PHI that is sent outside of the network or sent into the network and forwarded
 - The theft or loss of a laptop containing PII/PHI
 - Inadvertent posting of PII/PHI in training slides or on the Internet
 - Unauthorized access to PHI



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

Real Breach Scenarios

- A facility discovered Public Shared Folders (with PII/PHI) within a messaging system were created without appropriate access controls and permissions
- A beneficiary discovered an in-room computer used for charting at bedside was left unlocked and unattended. The computer monitor contained a list of patients (with PII) seen in the emergency room for that day
- After stopping in a facility parking lot to talk to a colleague, an employee mistakenly left his government-owned laptop in the parking lot and drove away. The laptop was unencrypted; PHI was contained in unprotected files. The laptop was later found by an employee of the same facility who did not access the PHI and returned it as quickly as possible



HEALTH AFFAIRS



TRICARE®

TRICARE
Management Activity

Breach Response Reporting

When a breach occurs within a TMA component, the breach must be reported to:

- Leadership: Immediately
- United States Computer Emergency Readiness Team (US-CERT): Within 1 hour (<https://forms.us-cert.gov/report/>)
- TMA Privacy and Civil Liberties Office (Privacy Office): Within 1 hour (by e-mail to PrivacyOfficerMail@tma.osd.mil)
- Defense Privacy and Civil Liberties Office: Within 48 hours (the Privacy Office is responsible for this step following receipt of the TMA Breach Report Form)

Note: Notify issuing banks if government issued credit cards are involved; law enforcement, if necessary; and all affected individuals within 10 working days of breach and identity discovery, if necessary



Breach Response

Reporting (continued)

- When reporting a breach, a TMA Breach Report Form must be used and can be downloaded at:
<http://www.tricare.mil/tma/privacy/breach.aspx>
- The form contains several descriptive fields, such as:
 - Date of breach
 - Breach discovery date
 - Date reported to US-CERT and US-CERT #
 - Total number of individual(s) affected by the breach
 - Type(s) of data elements involved

Note:

The form is updated regularly.

Check the Privacy Office Web site for the most current version.



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

Risk Assessment

- Once a breach is discovered, a risk assessment must be conducted to determine the likelihood of harm, based on the following five factors:
 - Nature of the data elements breached
 - Number of affected individuals
 - The number of affected individuals is a determining factor in how notifications are made, not whether they are made
 - Likelihood the information is accessible and usable
 - Likelihood the breach may lead to harm
 - Ability of the agency to mitigate the risk of harm



Breach Response

Individual Notification

- If it is determined that notification to affected individuals is required, written notification must occur within 10 days after the breach is discovered and the identities of the individuals ascertained
- The following elements must be included:
 - A description of the specific data involved
 - Facts and circumstances surrounding the breach
 - Protective actions TMA is taking or other actions the individual can take to mitigate against future harm
 - Any mitigation support services that have been implemented (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, etc.)
- A sample notification letter is available in the TMA Incident Response Team (IRT) and Breach Notification AI:

<http://www.tricare.mil/tma/privacy/RegulatoryRequirementsandGuidance.aspx>



HEALTH AFFAIRS



TRICARE
Management Activity

TMA Incident Response Team and Breach Notification Administrative Instruction



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

Standard Operating Procedure vs AI

The TMA SOP for Breach Notification was revised and re-formatted as an AI.



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

TMA Breach Notification AI

- Three main sections of the Breach Notification AI
 - Roles and Responsibilities: Outlines the expectations of each program office in the process of handling an incident
 - Procedures: Details specific actions and a progression of events that occur after a breach has been identified
 - Appendices: Provides various resources for assessing, reporting, and mitigating a breach
- The full document can be accessed at the following link:
<http://www.tricare.mil/tma/privacy/downloads/TMA-BreachResponseAdministrativeInstruction.pdf>



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

TMA Breach Steps

- When responding to a breach, the following seven steps should be observed:
 - Incident Identification
 - Incident Reporting
 - Containment
 - Mitigation of Harmful Effects
 - Eradication
 - Recovery
 - Follow-up



HEALTH AFFAIRS

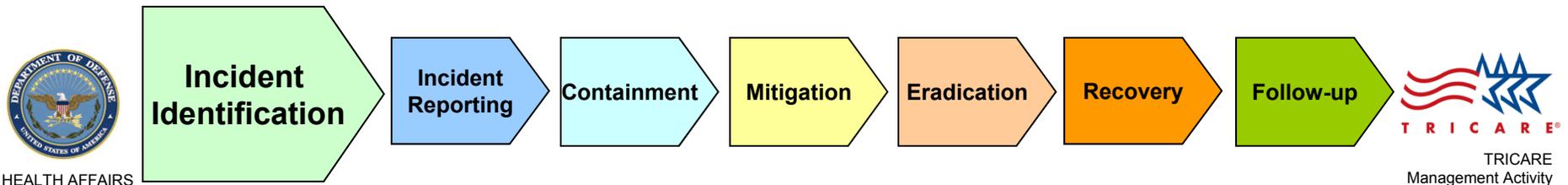


TRICARE
Management Activity

Breach Response

Step 1: Incident Identification

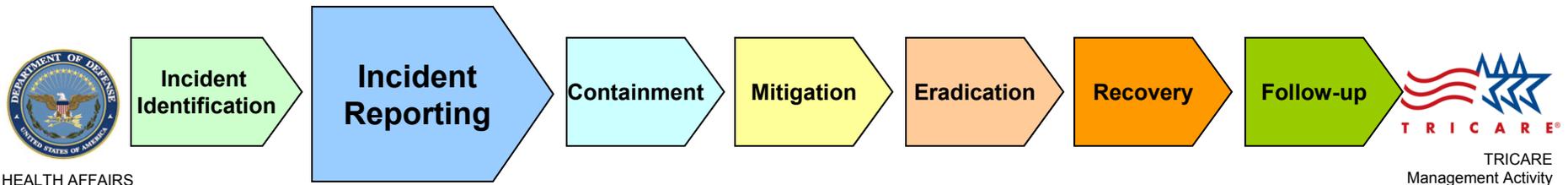
- Examine all available information to determine if an event/incident has occurred
 - Action steps:
 - Analyze all available information
 - Confirm and classify the severity of the incident
 - Determine the appropriate plan of action
 - Acknowledge legal issues addressed by the Office of General Counsel representative
 - Create an incident identification log



Breach Response

Step 2: Incident Reporting

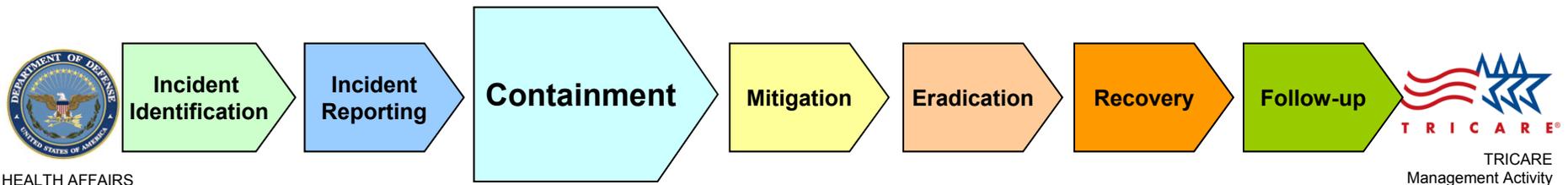
- TMA workforce members must report a breach (see slide 8)
- TMA personnel must notify the US-CERT and Privacy Office within one hour
- Incidents involving a malicious breach of PII/PHI must be reported to TMA Program Integrity
- The Director, TMA Privacy and Civil Liberties Office and/or the Chief Information Officer will notify the Deputy Director, TMA and senior leadership



Breach Response

Step 3: Containment

- The short-term actions that are immediately implemented in order to limit the scope and magnitude of an incident
- Includes, at a minimum, the following action steps:
 - Determine a course of action concerning the operational status of the compromised system and identify critical information affected by the incident
 - Follow existing local and higher authority guidance regarding any additional incident containment requirements



Breach Response

Step 4: Mitigating Harmful Effects

- The information/system owner shall mitigate the harmful effects of all incidents by:
 - Securing the information and taking the affected system off-line as soon as possible
 - Applying appropriate administrative and physical safeguards/blocking all exploited ports
 - Notifying other information/system owners of the attempted breach
 - Assessing the need for providing free credit monitoring and identity fraud expense coverage for affected individuals



HEALTH AFFAIRS

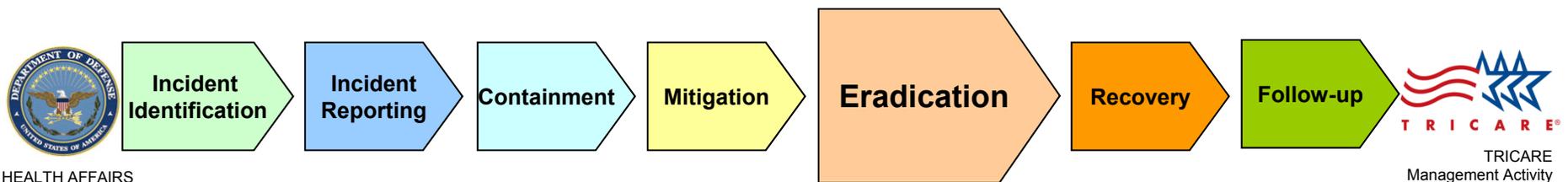


TRICARE
Management Activity

Breach Response

Step 5: Eradication

- Remove the cause of an incident and mitigate vulnerabilities pertaining to it
 - All eradication activities are to be documented by the IRT and the information/system owner
 - Specifically, document eradication activities in the incident identification log



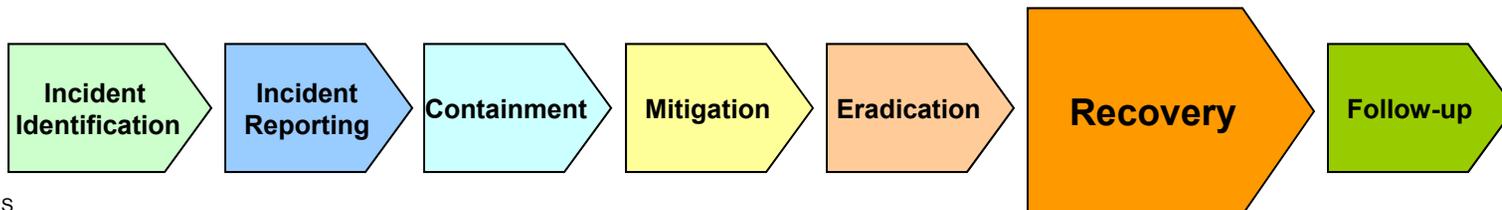
Breach Response

Step 6: Recovery

- Restore business operations to the normal condition
 - Verify that restoration actions were successful and that the business operation has returned to its normal condition
 - Execute the necessary changes to the system and document recovery actions in the incident identification log
 - Notify users of system availability and security upgrades that were implemented due to the incident



HEALTH AFFAIRS



TRICARE
Management Activity

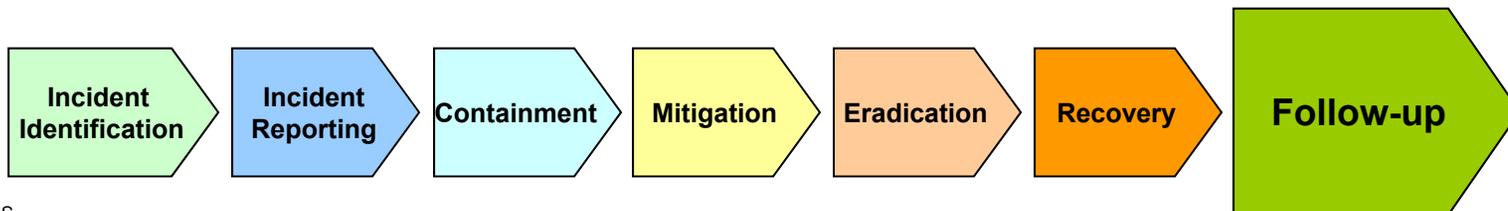
Breach Response

Step 7: Follow-Up

- Follow-up is critical
- It assists with the response to, and prevention of, future incidents
- Activities include:
 - Develop a lessons learned list, and share with TMA personnel and with other DoD organizations, as applicable
 - Amend operating procedures and policies, as appropriate
 - Provide subsequent workforce training and awareness lessons, as necessary



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response Summary

- You should now be able to:
 - Describe the key components of breach reporting, notification, and mitigation
 - Define your role in identifying and responding to breaches
 - Identify the three components of the TMA Breach Notification AI



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response Resources

- DoD 5400.11-R, “Department of Defense Privacy Program”, May 14, 2007
- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 24, 2003
- DoDI 8500.2, “Information Assurance (IA) Implementation”, February 6, 2003
- DoD 8580.02-R, “DoD Health Information Security Regulation”, July 12, 2007
- OSD Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”, June 5, 2009



Breach Response

Resources (continued)

- TMA Incident Response Team and Breach Notification Administrative Instruction, November 5, 2009, <http://www.tricare.mil/tma/privacy/downloads/TMA-BreachResponseAdministrativeInstruction.pdf>
- Breach Response section of the Privacy Office Web site: <http://www.tricare.mil/tma/privacy/breach.aspx>
- E-mail PrivacyOfficerMail@tma.osd.mil for subject matter questions
- To subscribe to the Privacy Office E-News, go to: <http://www.tricare.mil/tma/privacy/maillinglist.aspx>



HEALTH AFFAIRS



TRICARE
Management Activity