

2010 Data Protection Seminar

TMA Privacy Office



Breach Response



HEALTH AFFAIRS



TRICARE
Management Activity

Breach Response

Purpose

Provide a thorough understanding of the requirements of TRICARE Management Activity (TMA) personnel when assessing and responding to a breach



HEALTH AFFAIRS



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 Response Administrative Instruction (formerly known as the Breach Notification Standard Operating Procedure)



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

Source: DoD 5400.11-R, "DoD Privacy Program", May 14, 2007



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

Source: DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 23, 2004



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



Breach Response

Examples of Breaches

- Examples of breaches include:
 - Unauthorized use of another user's account
 - Unauthorized use of system privileges and data extraction
 - Unauthorized release of DoD sensitive information (SI), and execution of malicious code that destroys DoD SI
- If there is uncertainty as to whether an incident constitutes a breach, send an e-mail to the TMA Privacy Office at:
PrivacyOfficerMail@tma.osd.mil



HEALTH AFFAIRS



Breach Response

Reporting

When a loss, theft, or compromise of information occurs, the breach must be reported, as stated below:

TMA Components

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



HEALTH AFFAIRS



Breach Response

Reporting (continued)

- The Breach Report Form includes, but is not limited to:
 - Date of breach
 - Breach discovery date
 - Total number of individuals affected
 - Type(s) of PII/PHI involved
- The document can be downloaded at:
<http://www.tricare.mil/tma/privacy/downloads/Breach-Rpt.doc>



Breach Response

Risk Assessment

- Once a breach has been reported, 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
 - 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 the determination is made 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 notice should include the following elements:
 - A brief description of what happened, including the date of the breach
 - To the extent possible, a description of the types of personal information involved in the breach
 - A statement regarding whether the information was protected if it is determined this information would be beneficial and not compromise the security of the system
 - What steps individuals should take to protect themselves from potential harm
 - What the agency is doing to investigate the breach, mitigate losses, and to protect against further breaches
 - Who affected individuals should contact for more information, including a phone number, e-mail address, and postal address



TMA Incident Response Team and Breach Notification Administrative Instruction



HEALTH AFFAIRS



Breach Response

SOP Versus Administrative Instruction

The TMA Standard Operating Procedure (SOP) for Breach Response has been revised and re-formatted as an Administrative Instruction (AI)



HEALTH AFFAIRS



Breach Response

TMA Breach Notification AI

- Three main sections of the Breach AI include:
 - 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>



Breach Response

TMA Breach Notification AI (continued)

- The TMA Incident Response Team (IRT) and Breach Notification AI governs coordination of the breach response effort within TMA. Specifically, that effort consists of the following seven steps:
 - Incident Identification
 - Incident Reporting
 - Containment
 - Mitigation of Harmful Effects
 - Eradication
 - Recovery
 - Follow-up



HEALTH AFFAIRS



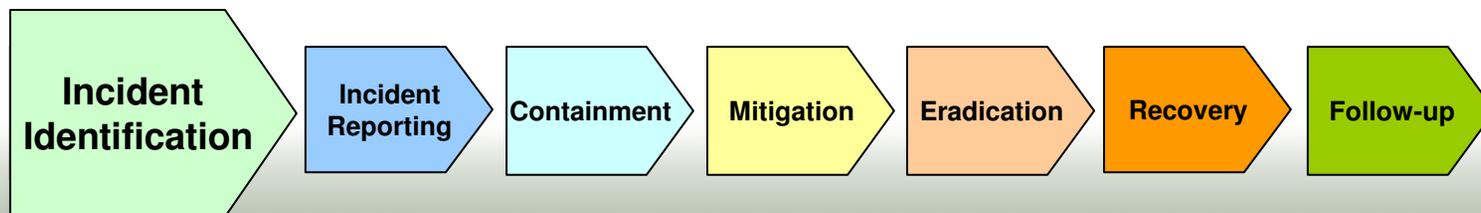
Breach Response

TMA Breach Notification AI (continued)

- Step 1: Incident Identification
 - Involves the examination of all available information in order 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 (OGC) representative
 - Create an incident identification log



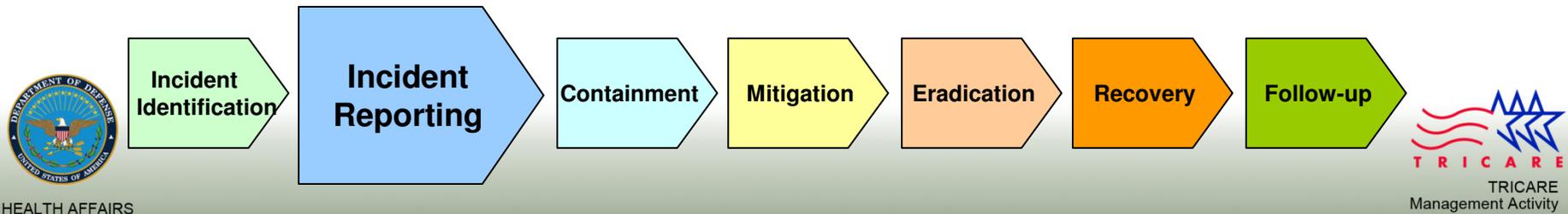
HEALTH AFFAIRS



Breach Response

TMA Breach Notification AI (continued)

- Step 2: Incident Reporting
 - TMA workforce members must report a potential or confirmed breach
 - TMA personnel must notify the TMA Privacy Officer and US-CERT within one hour
 - Incidents involving a malicious breach of PHI or PII must be reported to TMA Program Integrity
 - The TMA Privacy Officer and/or the Chief Information Officer will notify the Deputy Director, TMA and senior leadership

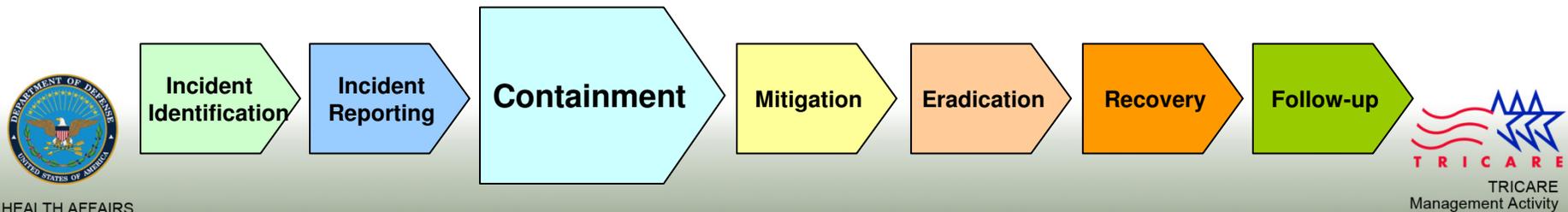


Breach Response

TMA Breach Notification AI (continued)

- Step 3: Containment

- Involves short-term actions that are immediately implemented in order to limit the scope and magnitude of an incident
- Containment activities include, 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

TMA Breach Notification AI (continued)

- Step 4: Mitigation of Harmful Effects
 - The information/system owner shall mitigate the harmful effects of all incidents by taking the following actions:
 - 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



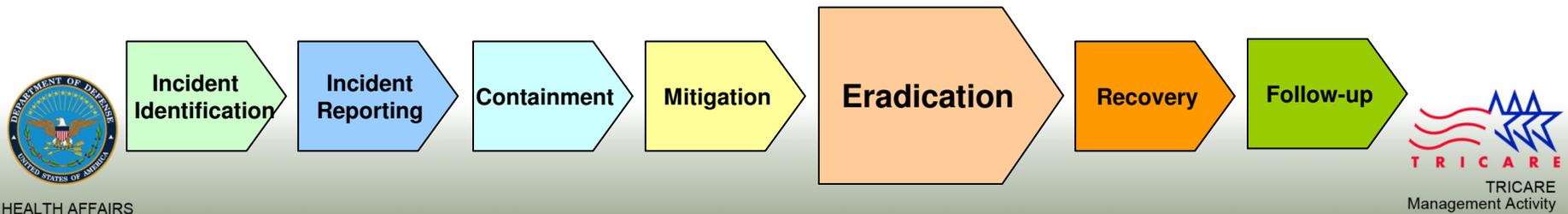
HEALTH AFFAIRS



Breach Response

TMA Breach Notification AI (continued)

- Step 5: Eradication
 - Entails removing the cause of an incident and mitigating vulnerabilities pertaining to the incident. 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

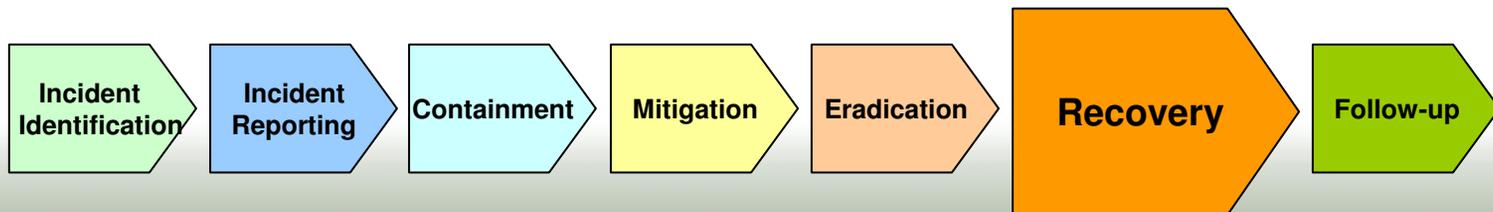
TMA Breach Notification AI (continued)

- Step 6: Recovery

- Recovery is the restoration of 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



Breach Response

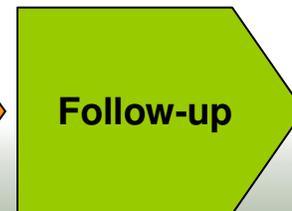
TMA Breach Notification AI (continued)

- Step 7: Follow-up

- Follow-up is a critical step in the incident response process and assists with the response to, and prevention of, future incidents
 - 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



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 Response Administrative Instruction (formerly known as the Breach Notification Standard Operating Procedure)



HEALTH AFFAIRS



Breach Response

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 24, 2003
- DoD 5400.11-R, “Department of Defense Privacy Program”, May 14, 2007
- OSD Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”, June 5, 2009



HEALTH AFFAIRS



Breach Response

Resources (continued)

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

