

# HIPAA Incident Response Plan

2007 ERMC IA and HIPAA  
Security Symposium  
TMA Privacy Office



HEALTH AFFAIRS



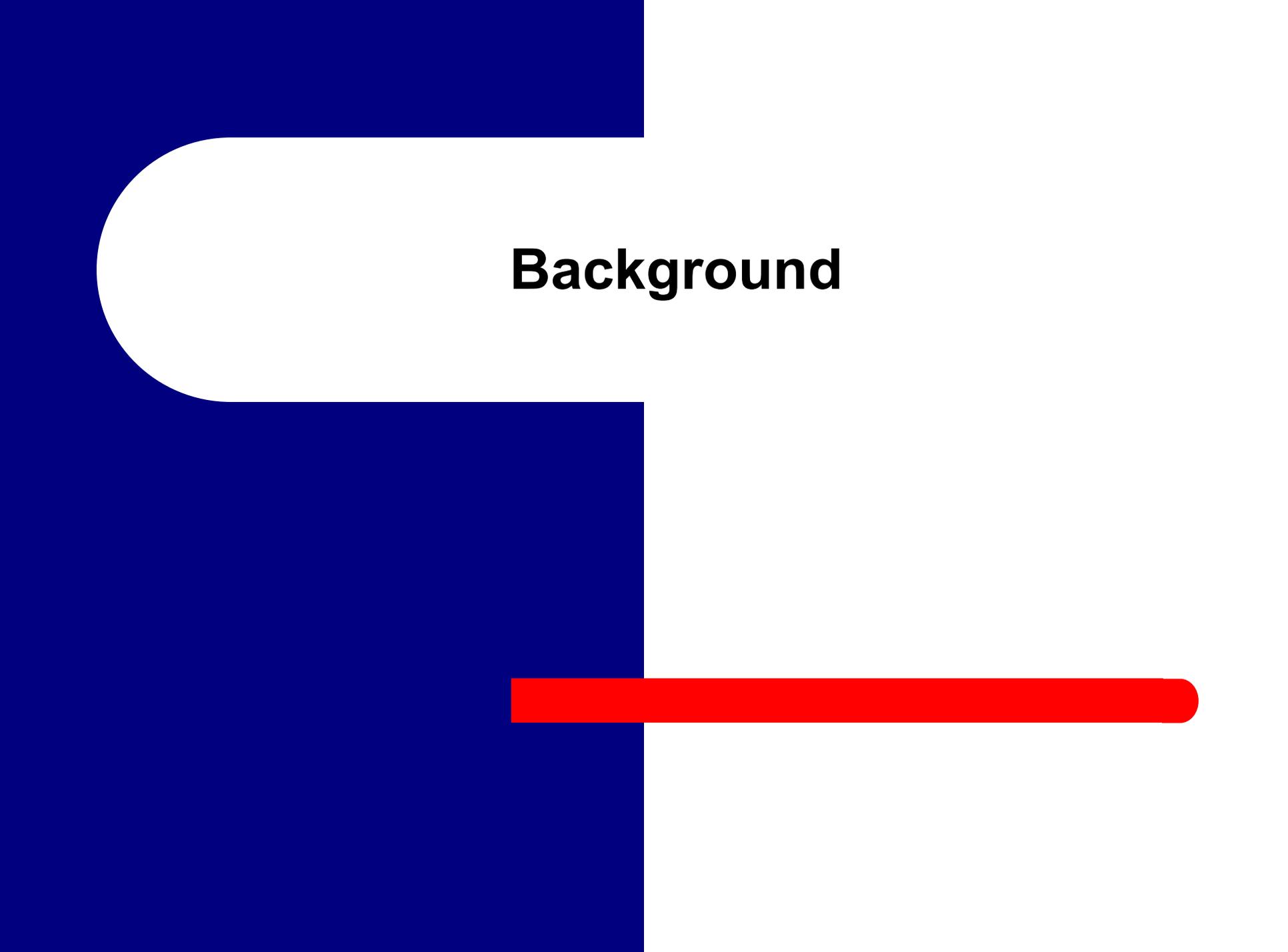
TRICARE Management Activity

# Agenda

- Background Information
- HIPAA Incident Response Plan
- Case Study

# Training Objectives

- Upon completion of this course, you should be able to:
  - Demonstrate how HIPAA Privacy and Security requirements have affected and added to DoD requirements for Incident Response
  - Identify recent Federal mandates that affect our Incident Reporting requirements
  - Describe the roles and responsibilities of the individuals and the departments affected by and responding to incidents
  - Recognize the seven basic steps of a comprehensive Incident Response Plan



**Background**

## Background Information

# Does Your IRP Need Updated?

- DoD policies and requirements relating to incident response and reporting have changed in recent years
- Your IRP might not specifically address the reporting process or procedures that are unique to a HIPAA incident
- The environment is not static

# Background Information

## It's all over the news



TRICARE  
Management  
Activity

**14,000** beneficiaries'  
identifiable  
information  
**compromised**



**200,000** customer names, social  
security numbers and credit card  
data **lost**

**196,000** customer social security  
numbers, names, birthdates and  
addresses **lost**



**American  
Red Cross**

**1 million** personal  
records **stolen**

**573,000** state  
employee records  
**stolen**



**26.5 million** veteran and  
active duty military  
records **lost**

\*Source: Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>

Background Information

## Does your IRP cover everything it should?

### **Common misconception:**

Data breaches affect only individuals  
that store their information online

Background Information

## Does your IRP cover everything it should?

### Reality:

Data breaches can affect all forms of information

- paper records
- emails
- phone messages
- reservation data

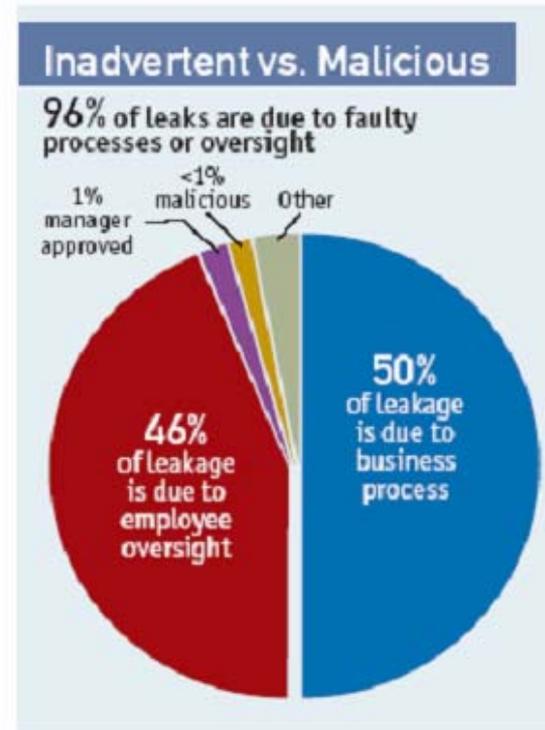
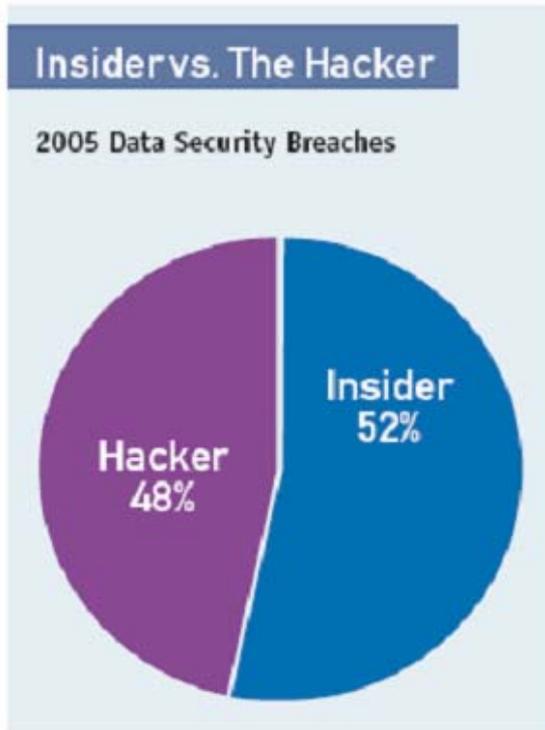
## Background Information

# What Are the Harmful Effects

- To the MTF
  - Interruption of Business
  - Substantial costs for investigation, recovery, legal fees and/or fines, mitigation
  - Bad publicity
- To the Individual
  - ID Theft
  - Medical Identity Theft
  - Substantial outlay of time and money to repair damage to credit rating and medical and financial records

# Background Information

## The Shifting Threat



\*Source: Electronic Privacy Information Center, <http://www.epic.org>

## Background Information

# The Government Response

### OMB M-06-15

- Restates Privacy Act Requirements
- Conduct Policy and Process Review
- Weaknesses identified must be included in agency Plan of Action and Milestones (POA&M)
- Remind Employees of Responsibilities for Safeguarding PII, the rules for acquiring and using such information, and the penalties for violating these rules

### OMB M-06-16

- Requires agencies to perform a technology assessment to ensure appropriate safeguards are in place, including:
  - Encryption standards
  - Allow remote access only with two-factor authentication
  - Use a “time-out” function for remote access and mobile devices;
  - Log all computer-readable data extracts and time parameters

### OMB M-06-19

- Revises current reporting requirements to require agencies to report **all** (electronic and physical form) incidents involving personally identifiable information to US-CERT **within one hour** of discovery (both suspected and confirmed breaches)
- Privacy and Security Funding Reminder

## Background Information

# The Government Response

### OMB Memo: Recommendations for Identity Theft Related Data Breach Notification

Presents the recommendations of the Identity Theft Task Force which include detailed considerations for planning and responding to data breaches that could result in identity theft.

- Recommendations for agencies:
  - Establish a core management group that can be convened to respond in the event of a breach
  - The group should conduct a risk analysis to determine whether the incident poses problems related to identity theft
  - If the agency determines there is a risk of identity theft, they should tailor its response to the nature and scope of the risk presented. The memorandum provides a menu of steps for an agency to consider, so that it may pursue such a risk-based, tailored response.

## Background Information

# The DoD Response

- OSD 12282-05, July 15, 2005, Notifying Individuals When Personal Information is Lost, Stolen, or Compromised
- ASD(NII) Memorandum, Use of Commercial Wireless Local-Area Network Devices, Systems, and Technologies in the DoD Global Information Grid, June 2, 2006
- DoD CIO Memorandum, August 18, 2006, DoD Guidance on Protecting Personally Identifiable Information (PII)
- DoD CIO Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, July 3, 2007

## Background Information

# Requirement

- DoD 8500.2-I, VIIR-1. Incident Response Planning
  - An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedures for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually

## Background Information

# Requirement

- DoD 8580.02-R, C2.7. SECURITY INCIDENT PROCEDURES
  - Implement policies and procedures to address security incidents. Security incidents as defined for the purposes of this Regulation, include, but are not limited to, policy violations by users, denial of service attacks, intrusions, unauthorized disclosures, theft and/or loss of information
  - Establish response procedures for all levels of incidents that demonstrate how the organization will:
    - Identify and respond to suspected or known security incidents
    - Report all suspected or known security incidents to the appropriate authorities in accordance with [references]
    - Mitigate, to the extent practicable, harmful effects of security incidents
    - Document security incidents and their outcomes

## Background Information

# Requirement

- DoD 6025.18-R, C14.6.  
STANDARD: MITIGATION
  - A covered entity shall mitigate, when practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this Chapter by the covered entity or its business associate



## Background Information Requirement

- DoD 5400.11-R, C1.5.
  - To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise
  - The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained



## Background Information

# Requirement

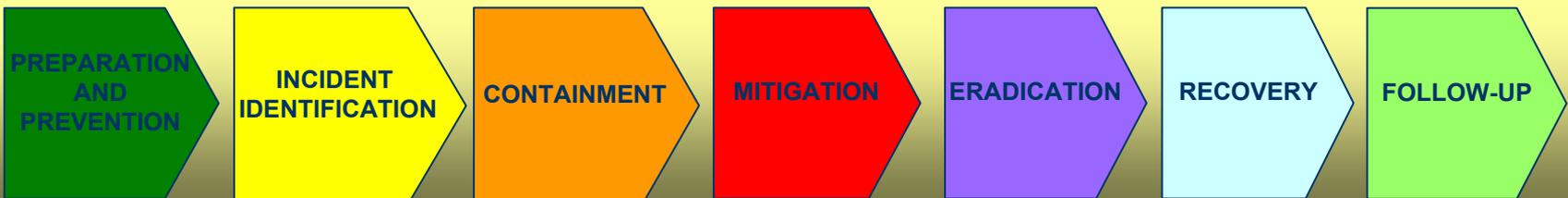
- DoD 5400.11-R, C10.6.1.
  - When a loss, theft, or compromise of information occurs the breach shall be reported to:
  - The United States Computer Emergency Readiness Team (US CERT) within one hour of discovering that a breach of personally identifiable information has occurred
  - The Senior Component Official for Privacy within 24 hours of discovering that a breach of personally identifiable information has occurred

# Incident Response Plan



## Incident Response Plan Procedures

- Local incident response plans should include, at a minimum:
  - Preparation and Prevention
  - Incident Identification
  - Containment
  - Mitigation
  - Eradication
  - Recovery
  - Follow-up



## Incident Response Plan

# Preparation and Prevention (1 of 3)

- Proper preparation will help organizations:
  - Respond effectively when any incident occurs
  - Prevent future incidents



## Incident Response Plan

# Preparation and Prevention (2 of 3)

- Preparation and prevention activities include, at a minimum, the following:
  - A written incident response plan that addresses all categories of incidents
  - Making you local incident response plan available to key organizational staff so that they know how to respond if an incident occurs
  - A communication plan/strategy that will be used to report incidents to appropriate officials

## Incident Response Plan

# Preparation and Prevention (3 of 3)

- Preparation and prevention activities include, at a minimum, the following (Cont.):
  - Train organizational staff on how to properly identify, respond, and report incidents
  - Maintain up-to-date security patches and security tools, such as malicious code detection and eradication applications
  - Follow other existing local and higher authority guidance regarding additional security incident preparation and prevention requirements

## Incident Response Plan

# Incident Identification (1 of 5)

- Incident identification involves the analysis of all available information in order to determine if an incident has occurred

PREPARATION  
AND  
PREVENTION

INCIDENT  
IDENTIFICATION

CONTAINMENT

MITIGATION

ERADICATION

RECOVERY

FOLLOW-UP

## Incident Response Plan

# Incident Identification (2 of 5)

- Some situations that may indicate that an incident has occurred include:
  - Unsuccessful login attempts
  - Missing equipment/media (lost or stolen)
  - A privacy complaint that implicates an information system or network as the source of an unauthorized disclosure
  - Data sitting in hallways or dumpsters

## Incident Response Plan

# Incident Identification (3 of 5)

- Incident identification activities include, at a minimum, the following:
  - Analyze all available information regarding any unexplained event to determine if an incident has occurred which involves or has the potential to involve PHI
  - Obtain a full back-up of the system in which suspicious events have been observed after a security incident involving ePHI has been identified

## Incident Response Plan

# Incident Identification (4 of 5)

- Incident identification activities include, at a minimum, the following (Cont.):
  - Classify the severity of the incident using US Computer Emergency Response Team (US CERT) guidance when the incident requires reporting to US CERT
  - Create an incident identification log (electronic or written) to document and record all actions that are taken once an incident has been identified, and document the purpose for reclassification

## Incident Response Plan

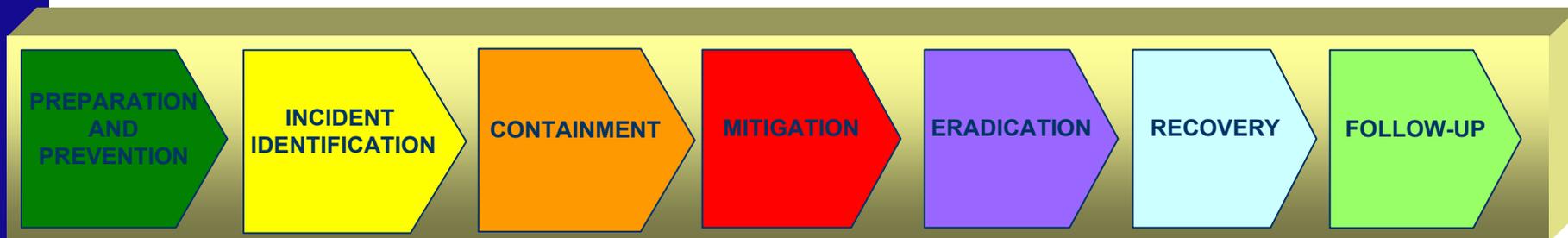
# Incident Identification (5 of 5)

- Incident identification activities include, at a minimum, the following (Cont.):
  - Activate the local IRT including:
    - Systems Administrator
    - Network Manager
    - IAM
    - IAO
    - HIPAA Security and Privacy Officer
    - Other key organizational staff
  - Follow existing local and higher authority guidance regarding any additional security incident identification requirements

## Incident Response Plan

# Incident Containment (1 of 3)

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



## Incident Response Plan

# Incident Containment (2 of 3)

- Containment activities include, at a minimum, the following:
  - Determine a course of action concerning the operational status of the compromised system
  - Determine a course of action regarding the critical information and/or computing services affected by the incident
  - Validate whether the ePHI should be left on information systems or if possible, whether it should be copied to alternative media and the system taken off-line

## Incident Response Plan

# Incident Containment (3 of 3)

- Containment activities include, at a minimum, the following (Cont.):
  - Document containment actions in the incident identification log
  - Provide periodic situational updates to the local IRT and all other appropriate officials (internal and external) according to local and higher authority guidance
  - Follow existing local and higher authority guidance regarding any additional security incident containment requirements

## Incident Response Plan

# Mitigation of Harmful Effects (1 of 4)

- Develop a methodology for communicating with victims, investigators, senior leadership (both within the MHS and external), Congress, the media (both paper and television), law enforcement agencies, and other governmental parties
  - The methodology may range from sending letters to victims to using the Web site as the primary tool for providing up-to-date information

PREPARATION  
AND  
PREVENTION

INCIDENT  
IDENTIFICATION

CONTAINMENT

MITIGATION

ERADICATION

RECOVERY

FOLLOW-UP

## Incident Response Plan

**Mitigation of Harmful Effects** (2 of 4)

- Stakeholder and Notification Methodology Table

STAKEHOLDER ENTITY	METHODOLOGY
Victims whose individually identifiable health information has been accessed inappropriately	<ul style="list-style-type: none"> <li>a. Information letter via U.S. mail</li> <li>b. Incident-specific Web site</li> <li>c. 1-800 number for questions and answers</li> </ul>
<p>Senior Leadership – examples include:</p> <p>DoD Senior Leadership (as determined by Service/MHS Senior Leaders)</p> <p>Army, Navy, Air Force Medical Departments</p>	<ul style="list-style-type: none"> <li>a. Phone (initial contact)</li> <li>b. E-mail message</li> </ul>
General Counsel/Judge Advocate General	<ul style="list-style-type: none"> <li>a. Initial contact by phone, followed by</li> <li>b. E-mail</li> </ul>
Computer Incident Response Team (CIRT)	<ul style="list-style-type: none"> <li>a. Initial contact by phone, followed by</li> <li>b. E-mail</li> <li>c. Meetings</li> </ul>

## Incident Response Plan

# Mitigation of Harmful Effects (3 of 4)

- Mitigation activities include, at a minimum, the following:
  - Notifying all affected individuals
    - For victims that have had PHI/PII disclosed or if a victim is a senior level person, one should consider notification as expeditiously as possible (phone)
    - Initial contact with the victim should provide them with a brief synopsis of the impact of the incident, and what steps they should take to mitigate personal risk

## Incident Response Plan

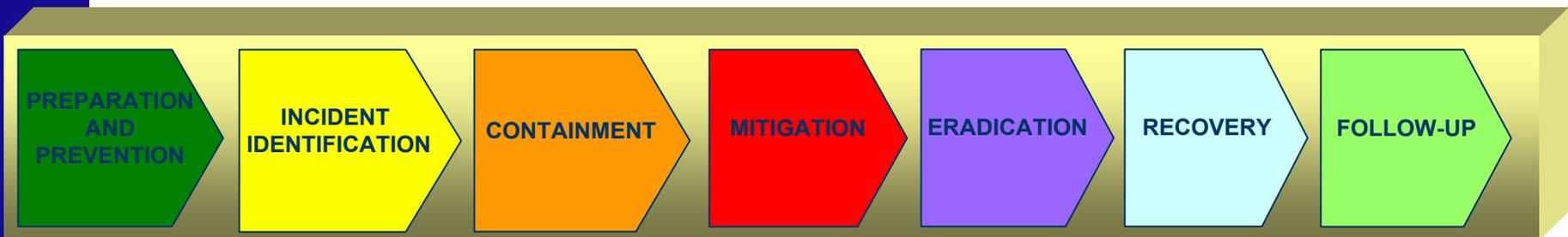
# Mitigation of Harmful Effects (4 of 4)

- Mitigation activities include, at a minimum, the following (Cont.):
  - Establish a toll-free number for call-in purposes
  - Establish a Web site (Intranet-based) for beneficiary communication
  - Establish a centrally managed e-mail address for victims
  - Assign a representative to speak to the public

## Incident Response Plan

# Eradication (1 of 2)

- Eradication entails removing the cause of an incident and mitigating vulnerabilities pertaining to the incident



## Incident Response Plan

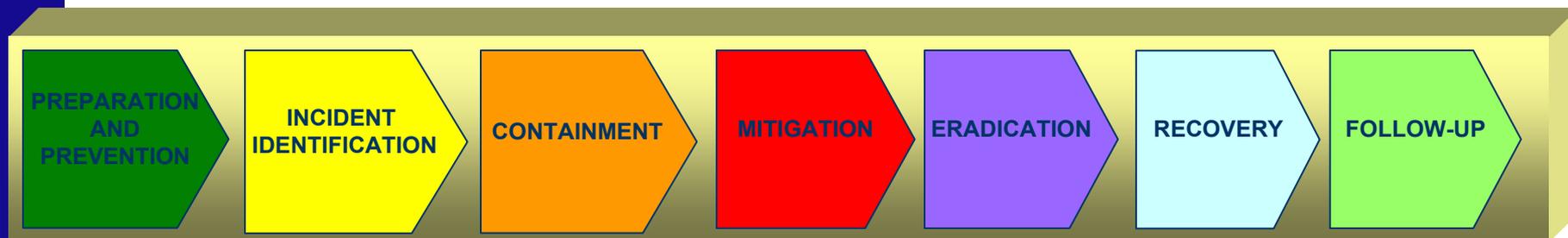
# Eradication (2 of 2)

- Eradication activities include, at a minimum, the following:
  - Document eradication response actions in the incident identification log
  - Follow existing local and higher authority guidance regarding additional incident eradication requirements

## Incident Response Plan

# Recovery (1 of 2)

- Recovery is the process of restoring to normal the status that existed prior to the occurrence of the incident



## Incident Response Plan

# Recovery (2 of 2)

- Recovery activities include, at minimum, the following:
  - Verify that any restoration actions were successful and that the operational status has been returned to its normal condition
  - Document recovery response actions in the incident identification log
  - Follow existing local and higher authority guidance regarding any additional incident recovery requirements

## Incident Response Plan

# Follow-Up (1 of 3)

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

PREPARATION  
AND  
PREVENTION

INCIDENT  
IDENTIFICATION

CONTAINMENT

MITIGATION

ERADICATION

RECOVERY

FOLLOW-UP

## Incident Response Plan

# Follow-Up (2 of 3)

- Follow-up activities should include, at a minimum, the following:
  - Conduct a lessons learned meeting with appropriate personnel to review all the actions taken in response to the security incident
  - Develop a methodology to document the lessons learned from the HIPAA incident and to measure the effectiveness of response procedures
  - Provide the lessons learned to all appropriate individuals within the organization

## Incident Response Plan

# Follow-Up (3 of 3)

- Follow-up activities should include, at a minimum, the following (Cont.):
  - Generate recommendations that can assist with the response to, and prevention of, future incidents based on the lessons learned
  - Make improvements/modifications to incident response procedures, and test as necessary
  - Follow existing local and higher authority guidance regarding any additional incident follow-up requirements

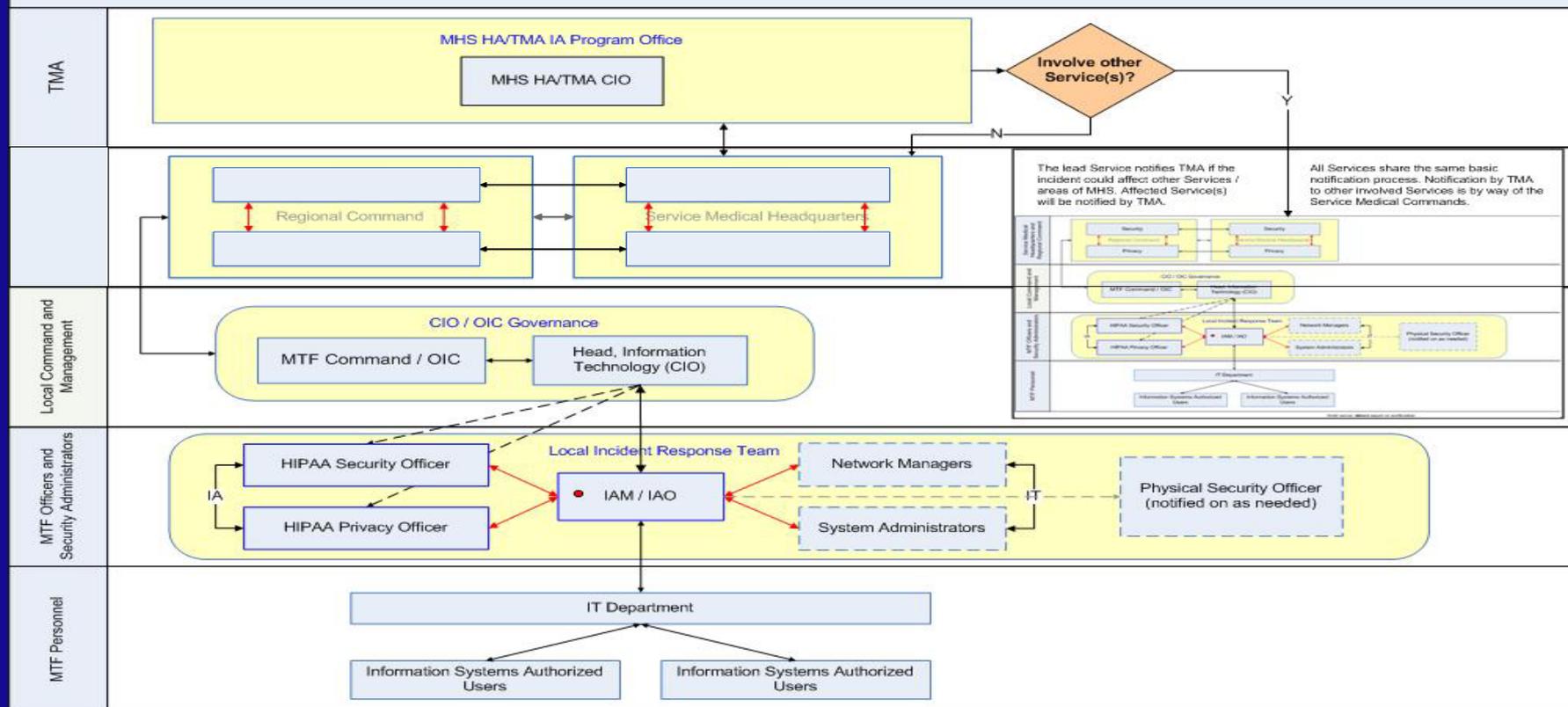
## Other elements – roles and responsibilities

- Be specific
- IRT members
- Include who is responsible for:
  - Each activity associated with the steps
  - Coordinating the response
  - Making notifications both internally and externally
  - Communicating with the public
  - Allocating funding
- Regularly updated contact lists

# Incident Response Plan

## Suggested role diagram

### MHS HIPAA Security Incident Notification Process



● The Information Assurance Manager / Officer represents the central point of contact to (1) receive and determine the nature and initial severity of a reported incident, (2) notify the local response team members, and (3) inform the CIO.

- Solid arrow: direct report or notification
- - - Dashed arrow: indicates possible notification, based on analysis of incident.
- Red arrow: indicates critical notification based on analysis of impact and severity
- Grouping: presumes local procedures for maintaining communication and awareness

## Incident Response Plan

# Other elements - reporting

- Incident reporting pertains to timely dissemination of information when an incident occurs
- The organizational incident response plan should include a communication strategy and methodology for notifying and updating concerned individuals at all levels of the organization when an incident occurs

## Incident Response Plan

# Other elements - reporting

- Reporting activities include, at a minimum, the following:
  - Develop a process and procedures for reporting security incidents and communicating situational updates, as necessary
  - Identify a point of contact at each level of the organization to serve as the lead in reporting security incidents to the appropriate officials
  - Report incidents involving the loss or suspected loss of personally identifiable information to the US CERT within one hour

## Incident Response Plan

# Other elements - reporting

- Reporting activities include, at a minimum, the following (Cont.):
  - Report the loss or suspected loss of PII to the DoD Component Privacy Office within 24 hours and the DoD Privacy Office within 48 hours or as established by the Defense Senior Privacy Official
  - Follow existing local and higher authority guidance regarding additional incident reporting requirements

## Incident Response Plan Summary

- You should now be able to:
  - Identify some of the key responsibilities and duties of the organizational staff that may be involved in managing and reporting HIPAA security incidents
  - Identify the types of security incidents that qualify as reportable incidents and, based upon the severity of the event, require notification of officials within TMA
  - Outline the structure and process for reporting HIPAA security incidents

# Case Study



## Case Study

# Scenario

- Routine network monitoring by Department of Defense (DoD) led to the discovery of an intrusion on a TRICARE Management Activity (TMA) computer. In April 2006, TMA's investigation of the intrusion determined that several databases containing sensitive information of almost 14,000 individuals were affected.

## Case Study Scenario

- No medical records were involved in this incident. Some of the databases contained information such as:
  - Names
  - Social Security Numbers
  - Drug Enforcement Administration numbers
  - Credit card information
  - Address – home, personal E-mail
  - Personal phone numbers
  - Protected Health Information (example: computer-related accommodation request, an E-mail about a medical condition)

## Case Study

# Timeline

- Feb 19 – Network Breach reported to the TMA CIO by JTF/GNO
- Feb 21 - IP address linked to an internal TMA server. Network Operations begins validating that incident was a breach
- Feb 21 – Incident confirmed as a data breach
  - Initial investigation revealed that suspect hacked into server and initiated rogue software application to gain privilege and extract data.
  - 150 databases and 1 excel spreadsheet affected

## Case Study

# Timeline

- Feb 23 – DISA contacted to begin forensic analysis
- Mar 10 – Database owners, directorates and POCs identified and notified
- Mar 30 – Notified Congress via white paper sent to House Armed Services Committee and Senate Armed Services Committee

## Case Study

# Response

- Affected server removed from network and analyzed by DISA
- Conducted notification activities
  - DoD and TMA leadership
  - Defense Criminal Investigative Service
  - Office of General Council
  - DoD Privacy Office
  - TMA Privacy Office

## Case Study

# Response

- Analyzed data to determine if incident involved sensitive data
- Notified the affected individuals of data breach and potential identity theft issues
- Conducted an analysis of policies and processes
- Reviewed the roles and responsibilities of the enterprise
- Provided additional training to our workforce
- Implemented specific administrative, physical and technical controls

# Case Study

**What went wrong?**

## **Case Study**



**Was the government response  
adequate?**

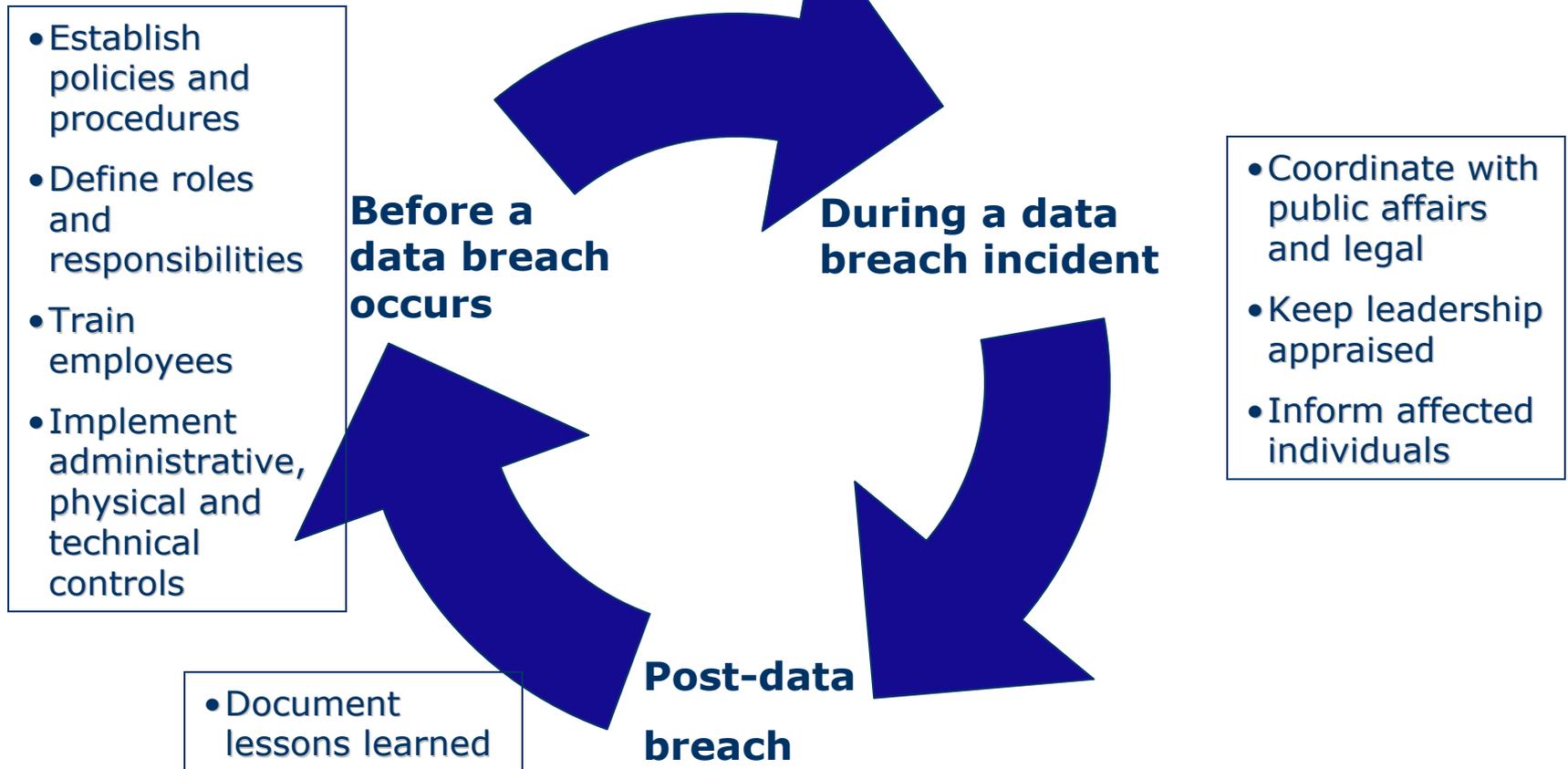
## **Case Study**



**How can we prevent this type of incident from re-occurring?**

## Case Study

# Prevention Activities



## Case Study

# Prevention Activities

- Examine roles and responsibilities
- Examine business agreements
- Review your facility's information flow
- Conduct periodic risk assessments
- Identify where information resides
- Train your employees on global policies *and* local procedures
- Test and Update Your Incident Response Plan

## Case Study

# Key Takeaways

- Data breach incidents can happen anywhere, anytime
- Be proactive in developing strategies to prevent data breaches
- Realize that the best strategy won't prevent every data breach
- Keep abreast of legislation and regulations
- Stay engaged
- Create and communicate your Lessons Learned

## Incident Response Plan Summary

- You should now be able to:
  - Identify some of the key responsibilities and duties of the organizational staff that may be involved in managing and reporting HIPAA security incidents
  - Identify the types of security incidents that qualify as reportable incidents and, based upon the severity of the event, require notification of officials within TMA
  - Outline the structure and process for reporting HIPAA security incidents

Presentation Title

## Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- DoD 8580.02-R, DoD Health Information Security Regulation
- <http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm>
- <http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm> to subscribe to the TMA Privacy Office E-News
- [phimtsupport@tma.osd.mil](mailto:phimtsupport@tma.osd.mil) or [help@mhs-helpdesk.com](mailto:help@mhs-helpdesk.com) for tool related questions
- [Privacymail@tma.osd.mil](mailto:Privacymail@tma.osd.mil) for subject matter questions
- Service HIPAA Representatives

**Thank You!**



HEALTH AFFAIRS



TRICARE Management Activity