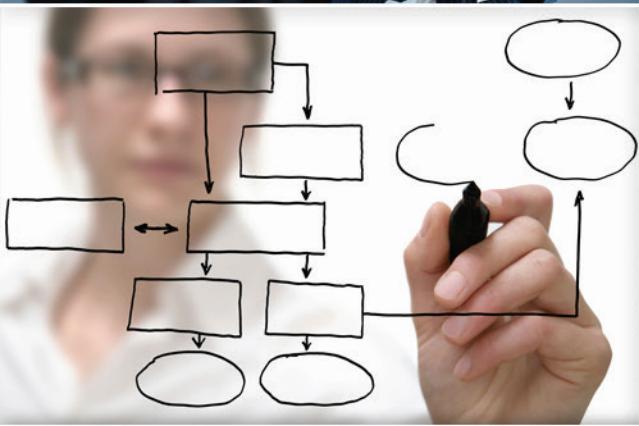


TMA PRIVACY AND CIVIL LIBERTIES OFFICE

2012 HEALTH INFORMATION PRIVACY & SECURITY TRAINING



Comprehensive Breach Response Efforts

THE POWER OF TEAM WORK

Committed to Protecting Beneficiary Data

Comprehensive Breach Response Efforts

Purpose

The purpose of this presentation is to provide a thorough understanding of the requirements of all Military Health System (MHS) workforce members, to include the organization's civilian employees, uniformed service members, and contractors requiring access to PII and PHI, when responding to a breach.



Comprehensive Breach Response Efforts

Objectives

- Upon completion of this presentation, you should be able to:
 - Explain the importance of your role as an MHS workforce member
 - Describe the key definitions and elements of an effective breach response program
 - Explain the purpose of the DoD Risk Assessment Table
 - Be familiar with MHS breach trends and take away essential best practices and training tips



Comprehensive Breach Response Efforts

Our Obligation

- DoD takes any potential compromise of patient information very seriously
- We are obligated to protect and safeguard the information we are entrusted with
- Maintaining the privacy and security of personally identifiable and protected health information (PII/PHI) is one of MHS's greatest concerns



Comprehensive Breach Response Efforts

Key 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



Comprehensive Breach Response Efforts

Key Definitions

- **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



Comprehensive Breach Response Efforts

Key Definitions

- **DoD 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 an other than authorized purpose, where one or more individuals will be adversely affected



Key Definitions

- “**HHS Breach**”: The unauthorized acquisition, access, use, or disclosure of PHI which compromises the privacy or security of the PHI
 - “Compromised” means that the breach poses significant risk of financial, reputational or other harm to the affected individual(s)
 - This definition of breach excludes certain unintentional uses or disclosures involving authorized personnel and situations where an unauthorized person would not have been able to retain the PHI



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



Breach Response 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



Comprehensive Breach Response Efforts

MHS Breach Reporting

- When a breach occurs within the MHS, it must be reported to:

- Leadership: Immediately
- United States Computer Emergency Readiness Team (US-CERT): within one hour
- TMA Privacy and Civil Liberties Office (TMA Privacy Office):
 - within one hour if the breach occurs at TMA
 - within 24 hours if the breach occurs at the Service-level
- Defense Privacy and Civil Liberties Office: within 48 hours of breach discovery (***TMA Privacy Office is responsible for this step for breaches occurring at TMA***)
- Department of Health and Human Services/Office for Civil Rights: (***TMA Privacy Office makes this determination for all of the MHS***)
 - without unreasonable delay and in no case later than 60 days of discovery if there are 500 or more individuals affected
 - report on an annual basis, but no later than 60 days after the end of the calendar year if there are fewer than 500 individuals affected

Note: Notifying 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



Comprehensive Breach Response Efforts

Breach Reporting

- When reporting a breach, you must include the following elements:
 - 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
 - Description of the breach
 - Mitigation steps taken
- For TMA, the required Breach Report Form can be downloaded at: <http://www.tricare.mil/tma/privacy/breach.aspx>



Comprehensive Breach Response Efforts

DoD Risk Assessment Table

- Once a breach is discovered, a risk assessment must be conducted to determine the likelihood of harm, based on the following 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



Comprehensive Breach Response Efforts

Individual Notification

- If it is determined that notification to the affected individual(s) 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 the MHS is taking and/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 DoD 5400.11-R and the TMA Administrative Instruction for Breach Notification



Comprehensive Breach Response Efforts

TMA Lessons Learned

- Over the past year, TMA has learned it is CRITICAL:
 - To assemble the Incident Response Team immediately following notification of a potentially high impact/volume breach
 - Chief of Staff, Privacy, General Counsel, Public Affairs, and the Action Officer (point of contact where breach occurred)
 - To know who the key stakeholders and players are
 - Congress, Leadership, General Counsel, Beneficiaries, Beneficiary Counseling and Assistance Coordinators, Contract Partners, Service Medical Departments, etc.
 - To have a strong strategic communications plan in place
 - Privacy working closely with TMA's Beneficiary Education & Support Division to develop internal documents for Public Affairs and Leadership, and also a timely web announcement with relevant Questions and Answers
 - To allow Privacy to take the lead in drafting/reviewing all correspondence for compliance purposes
 - Having templates readily available
 - Assigning a lead for version control



Comprehensive Breach Response Efforts
MHS Lessons Learned

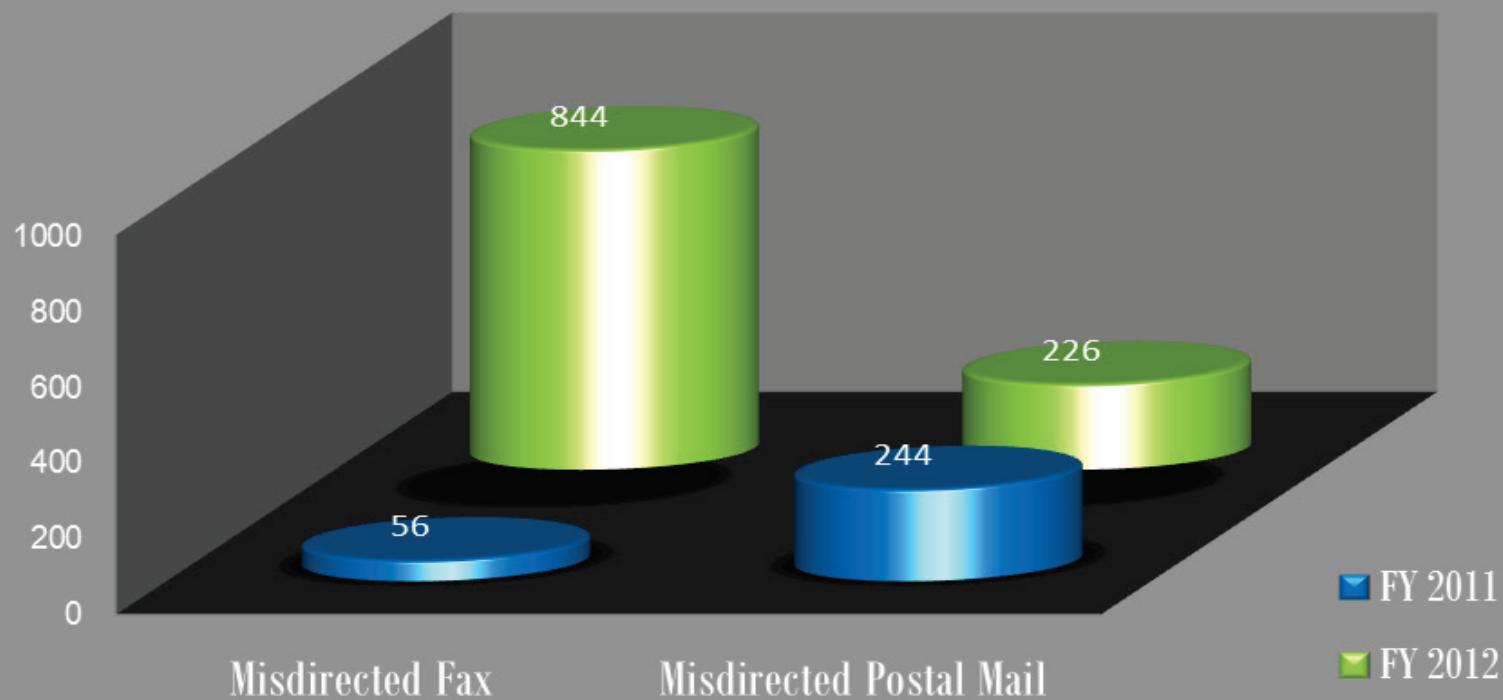
Open Forum to Share Breach Response Lessons Learned



Comprehensive Breach Response Efforts

MHS Breach Trends: FY 2011 – 2012

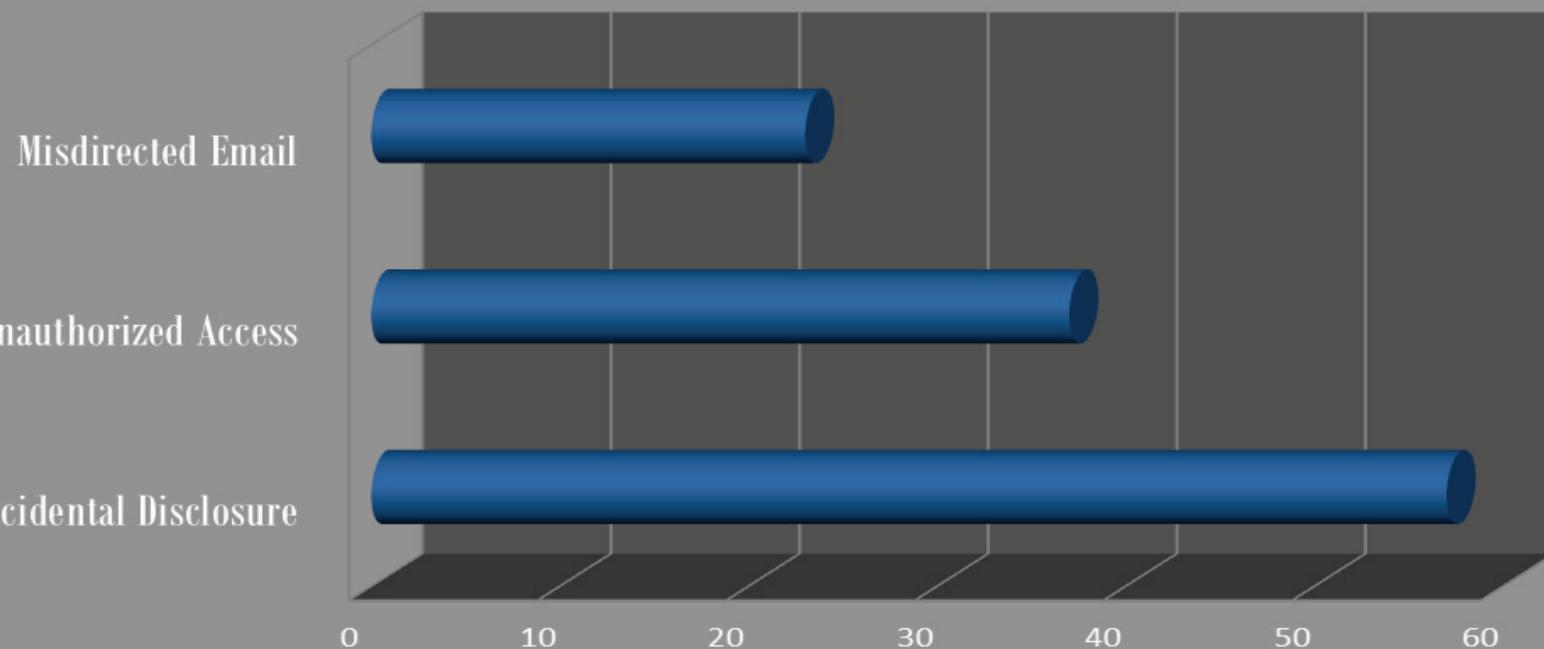
Most Common Breaches FY11 & 12 (Q1-Q3)



Comprehensive Breach Response Efforts

Service-level Breach Trends

Top 3 Service-Level Breaches FY2012 (Q1-Q3)



2012	Accidental Disclosure	Unauthorized Access	Misdirected Email
	57	37	23



Comprehensive Breach Response Efforts

Summary

- You should now be able to:
 - Explain the importance of your role as an MHS workforce member
 - Describe the key definitions and elements of an effective breach response program
 - Explain the purpose of the DoD Risk Assessment Table
 - Be familiar with MHS breach trends and take away essential best practices and training tips



Comprehensive Breach Response Efforts

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



Comprehensive Breach Response Efforts

Resources

- 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>
- Subscribe to the Privacy Office E-News at:
<http://www.tricare.mil/tma/privacy/mailinglist.aspx>

