HEALTH AFFAIRS

TRICARE
Management
Activity

American Health Information Management Association
Joint Veterans Affairs HIM and Military Services Special Interest Session

Presenters:

Office of General Counsel
TRICARE Management Activity

Privacy Officer
Veterans Health Administration

October 2006

One in five Americans had personal information lost or stolen this year.

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

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

TRICARE Management Activity

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

573,000 state employee records **stolen**

Georgia Technology Authority

1 million personal records **stolen**

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

One in five Americans had personal information lost or stolen this year.

196,000 cus
security nu
birthdates a

Fi
INV

573,000 st
emplo
records **sto**

Marriott

00,000 customer
es, social security
mbers and credit
card data **lost**

ntifiable
omised

rican
Cross

1 million personal
records **stolen**

Since January 1, 2006 more than
63.7 million Americans

– 21% of the population –

have had their personal information
lost or stolen.

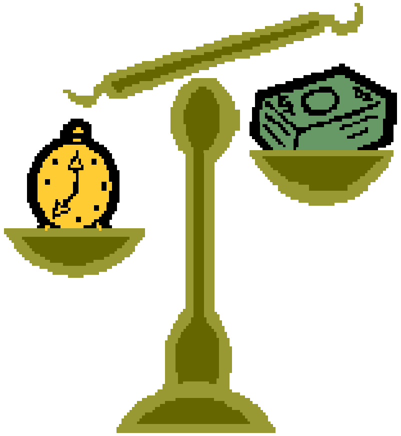
United States
Department of Veterans Affairs

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

It can take years to build citizen and consumer trust, and only one data incident to destroy it.

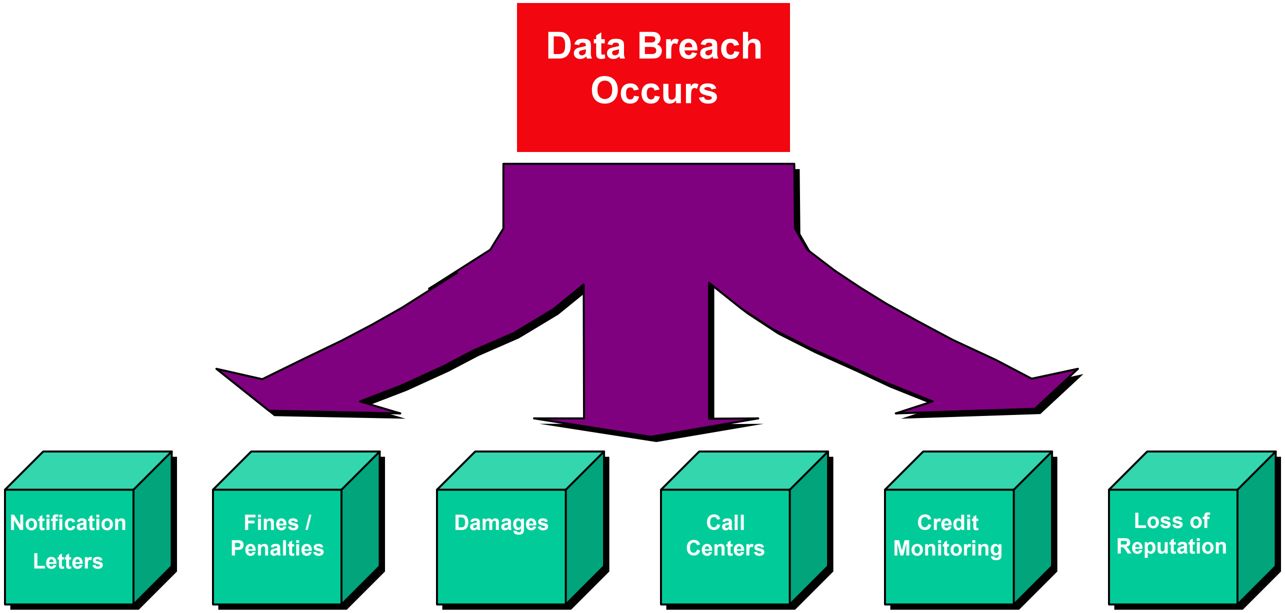
When a breach occurs, the costs are overwhelming.

- Loss of current and future customers
- Tarnished reputation
- Lawsuit
- Possible fines and penalties
- Administrative costs (letters, postage, call centers, credit monitoring)
- Labor to do administration for the above actions and more



The cost in trust probably will exceed the high cost of implementing remediation.

If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.


Data Breach Occurs

Notification Letters

Fines / Penalties

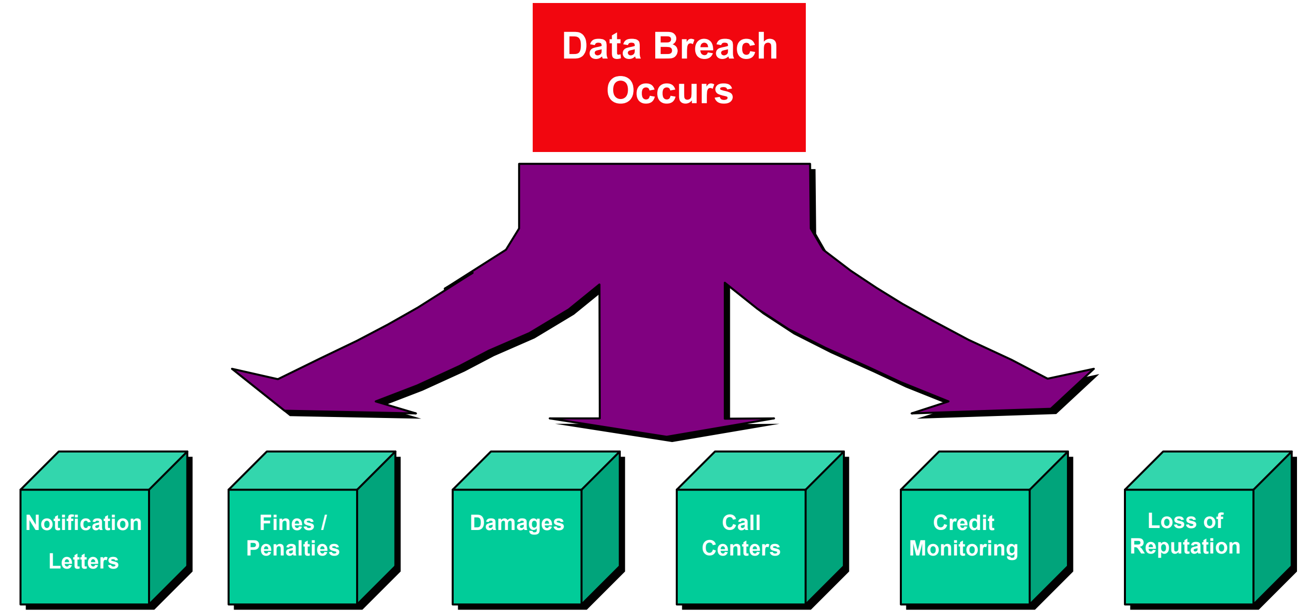
Damages

Call Centers

Credit Monitoring

Loss of Reputation

If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.



Data Breach Occurs

Notification Letters

Fines / Penalties

Damages

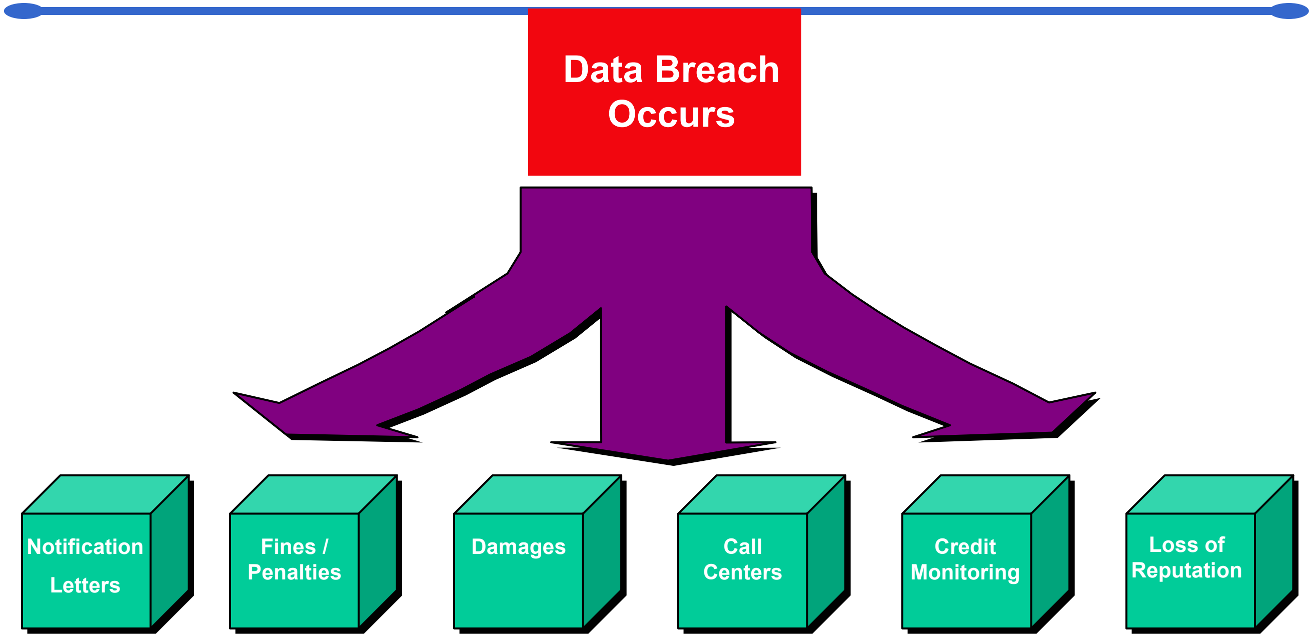
Call Centers

Credit Monitoring

Loss of Reputation

$1.50-2.00/
letter

If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.



Data Breach Occurs

Notification Letters

Fines / Penalties

Damages

Call Centers

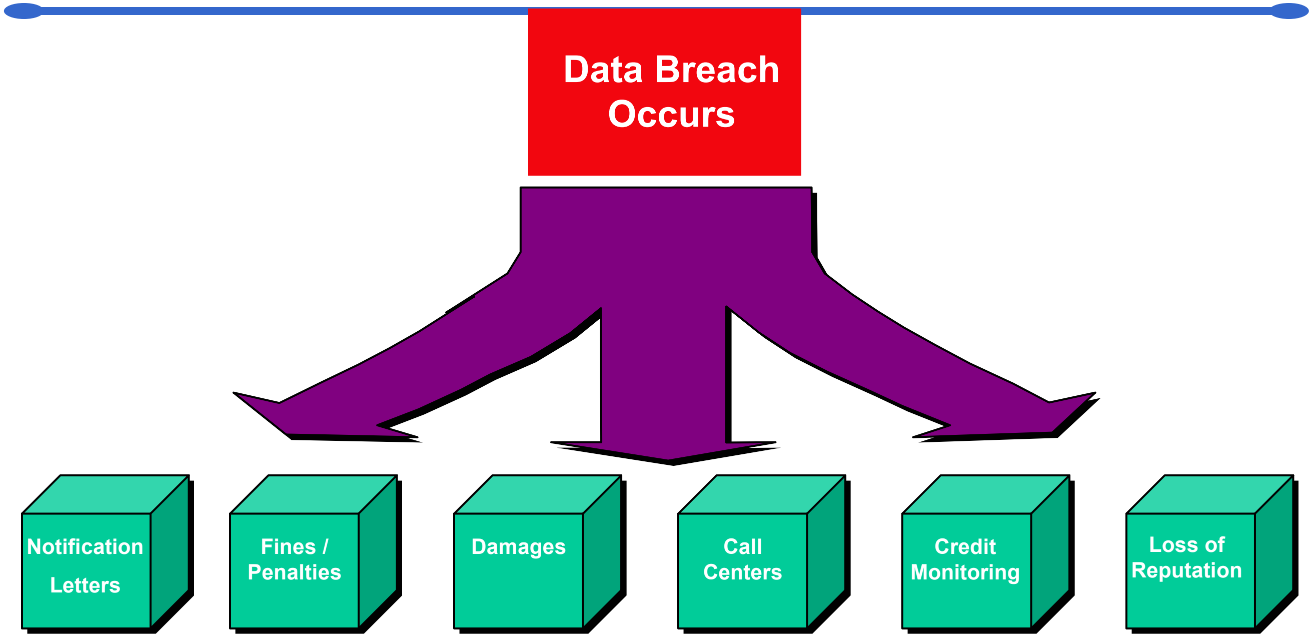
Credit Monitoring

Loss of Reputation

$1.50-2.00/ letter

$1000-250,000/ penalty

If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.



Data Breach Occurs

Notification Letters

Fines / Penalties

Damages

Call Centers

Credit Monitoring

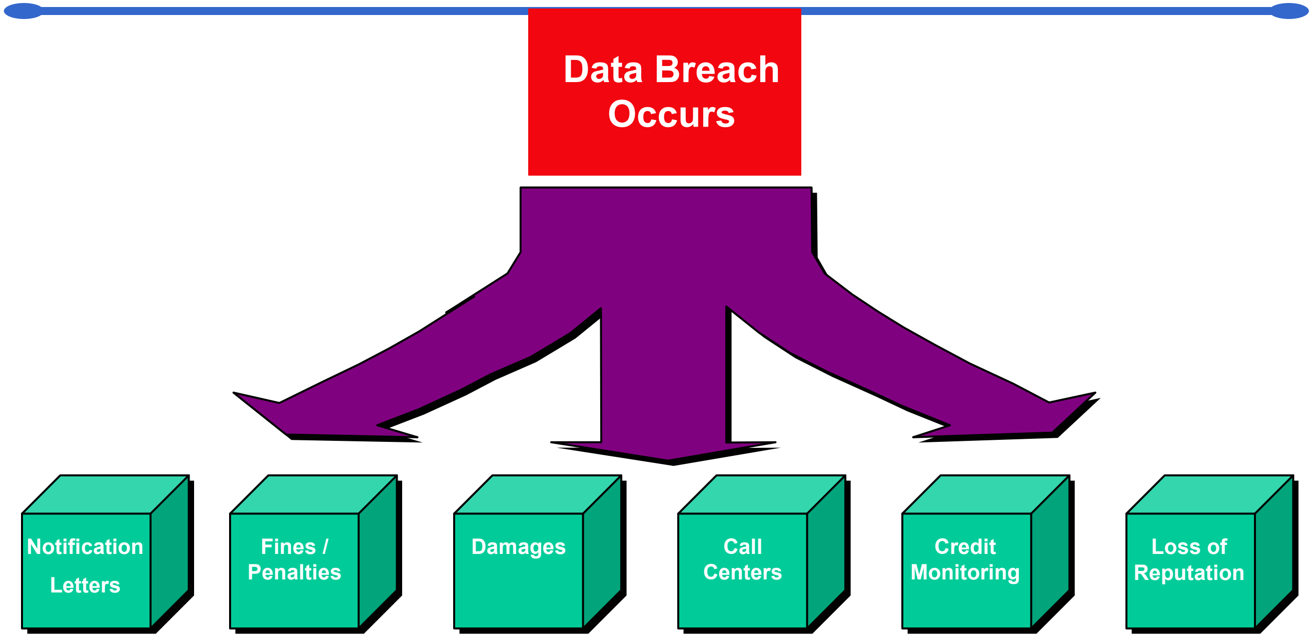
Loss of Reputation

$1.50-2.00/ letter

$1000-250,000/ penalty

$1,000/ person

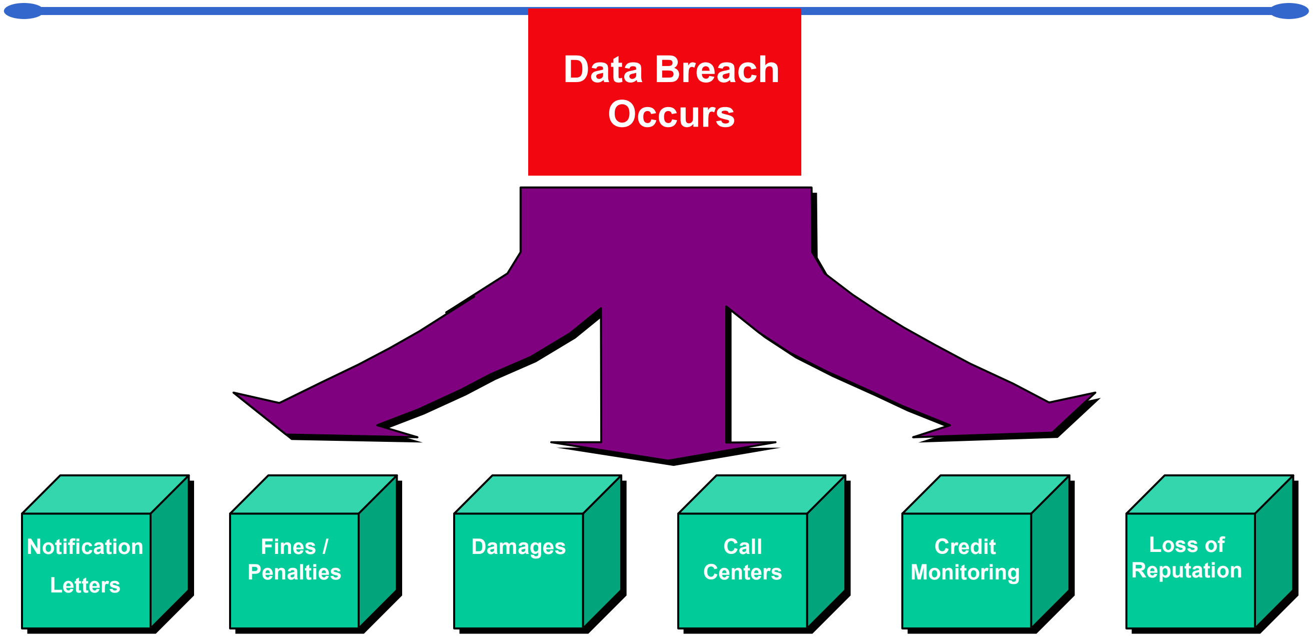
If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.



Data Breach Occurs

Notification Letters	Fines / Penalties	Damages	Call Centers	Credit Monitoring	Loss of Reputation
$1.50-2.00/ letter	$1000-250,000/ penalty	$1,000/ person	$10.00-31.00/ call		

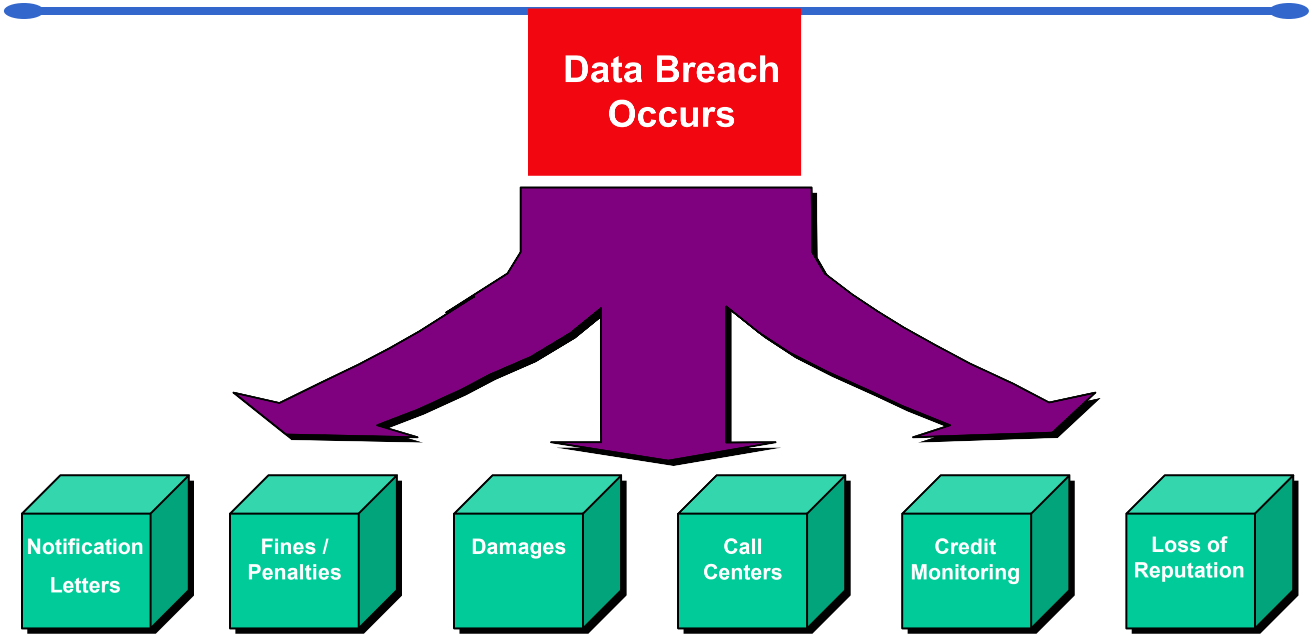
If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.



Data Breach Occurs

Notification Letters	$1.50-2.00/ letter
Fines / Penalties	$1000- 250,000/ penalty
Damages	$1,000/ person
Call Centers	$10.00- 31.00/ call
Credit Monitoring	$60/ person
Loss of Reputation	

If a data breach does occur, costs will be incurred through a variety of incident response activities and remediation efforts.



Data Breach Occurs

Notification Letters	$1.50-2.00/ letter
Fines / Penalties	$1000-250,000/ penalty
Damages	$1,000/ person
Call Centers	$10.00-31.00/ call
Credit Monitoring	$60/ person
Loss of Reputation	PRICELESS!

We are all vulnerable. Are you ready?

The issue is not *whether* you will experience a data breach but rather *how* you will respond when the inevitable occurs.

OMB has issued memoranda on safeguarding personally identifiable information (PII) .

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

- System Review (NIST Checklist)

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

Department of Defense (DoD) has issued a response to OMB M-06-16 and OMB M-06-19.

DoD Guidance on Protecting Personally Identifiable Information (PII)

- Evaluate all PII for impact of loss or unauthorized disclosure and protect accordingly.
- Assign a High or Moderate PII Impact Category to all PII electronic records
- Report loss or suspected loss of PII
  - Within one hour to US-CERT
  - Within 24 hours to DoD Component Privacy Office/POC
  - Within 48 hours to DoD Privacy Office

- For PII electronic records categorized as High Impact:
  - DAA approval required for storage, processing or downloading on mobile computing devices or removable electronic media
  - Restricted to workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive (i.e., "protected workplaces")
  - If accessed remotely
    - DoD approved PKI certificate on approved hardware token
    - Screen Lock with 15 minutes or less inactivity period constraint
    - Conform to IA Control ECRC-1, Resource Control
  - If removed from "protected workplaces"
    - Sign in and out
    - Encrypt

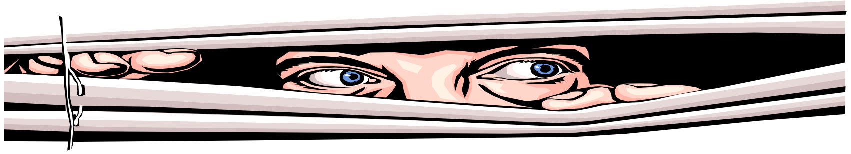
We must take a proactive stance to prevent data breaches.

- Investigate potentially risky business practices
  - Teleworking arrangements
  - Portable storage devices
  - Unencrypted data transmission
  - System access privileges
- Examples of TMA practices for protection and prevention of data breaches
  - TMA Incident Response Plan analysis
  - Chartering of TMA Health Information Privacy and Security Compliance Committee (HIPSCC) Data Protection Policy Working Group (DPPWG)

Risky Business

Teleworking arrangements require agreements

Risks	DoD Mitigation Strategies	Control from NIST SP 800-53
• Remote access to systems. • Removal of data from organization's physical and technical confines. • Lack of appropriate user awareness of technical security safeguards.	• Restrict teleworkers to government owned equipment. • Make supervisors an integral part of the approval process. • Promote teleworking as the exception not the norm. Tie authorization to specific tasks and timeframes. • Maintain accurate logs of personnel authorized to telework. • Conduct annual review of policies and procedures.	• Require virtual private network use (VPN) (AC 20) • Review policies and procedures for correctly restricting equipment use to government-owned equipment (AC 20) • Review policies and procedures for remote access control, monitoring and authorization (AC 17)



Risky Business

Portable storage devices require encryption

Risks	DoD Mitigation Strategies	Control from NIST SP 800-53
• Portable media devices more susceptible to theft or loss. • Removal of data from organization's physical and technical confines. • Ability to transport very large volumes of data.	• Require the use of government owned equipment. • Allow only encrypted data to be downloaded to portable storage devices.	• Review policies and procedures that correctly restrict use to government-owned equipment (AC 20) • Implement access controls for portable and mobile devices in accord with organization policy and procedures (AC 19)

Originally uploaded by John Fader 17:59, 4 December 2004

Risky Business

Data transmission requires encryption

Risks	DoD Mitigation Strategies
• Data can be intercepted by unauthorized persons.	• Mandate the encryption of all data transmissions.
Controls from SP 800-35	
• Ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (SC-8) • Prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (SC-9)	

E-mailing patient data "in the clear" (i.e. not encrypted) poses hazards to integrity and confidentiality. If you use TRICARE-Online (TOL) to communicate individually identifiable patient information, encrypt e-mails following TOL policies. For other e-mail methods, use available encryption options or avoid e-mailing individually identifiable health information.

My HIPAA Security Official is:

www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity

Risky Business

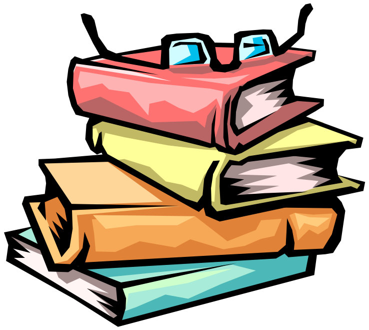
System access privileges must be audited

Risks	DoD Mitigation Strategies	Control from NIST SP 800-53
• Employee access privileges not revoked when appropriate. • Access levels do not align with responsibilities. • Leaves open access for hacker to use.	• Periodically review all employee access privileges. • Require managerial sign off on all systems access requests, including authorization for specific access level. • Monitor and audit data being accessed by personnel. • Tie removing personnel’s access to systems to another mandatory stage of the out processing procedure.	• Investigate any indications of inappropriate or unusual activity (AU-6) • Review access control policy and procedures and updated them periodically (AC 1) (AC 3) (AC 5) (AC 6) (AC 13) (AC 17) (AC 18) (AC 19) AC 20) • Employ automated mechanisms (AC-1) • Automatically terminate temporary accounts (AC-1) • Automatically disable inactive accounts (AC-1) • Employ automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited (AC-1)

Before a Breach Occurs: Incident Response Plan

DoD Approach to Incident Response

- Implemented in the event of a suspected or actual unauthorized data disclosure or security breach
- Clearly defined roles and responsibilities
- Centralized approach to incident response and reporting
- Institutionalized mitigation plan development and tracking through to resolution
- Includes templates for reports, notification letters, web pages and other communications



During an Incident: Incident Response Plan

Incident Response Team (IRT)

- Multidisciplinary
- Follows incident from designation of Incident Response Manager to mitigation to dissemination of lessons learned
- Coordinates external and internal communications
- Team actions and reporting timelines based on incident severity classification and Mission Assurance Category

During an Incident: Incident Response Plan

Recognizing That An Incident Has Occurred

	Indicators of Potential Incidents
1	A system alarm or similar indication from an intrusion detection tool.
2	Suspicious entries in system or network accounting.
3	Unsuccessful login attempts.
4	Unexplained new user accounts
16	Presence of, regardless of means, on a system that is not properly classified for such data, i.e. Secret information on a Sensitive Information system.
17	Unexplained modification or deletion of data.
18	Denial of service or inability of one or more users to login to an account.

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

The Incident Response Plan contains a list of eighteen situations that may indicate an incident has occurred.

During an Incident: Incident Response Plan

Determining Incident Severity

- Severity: the impact (effect) the incident has on the operational status of the organization, the risk to patient care, and/or the potential for negative public relations consequences.
- Incident severity levels are classified on a scale of 1 through 5, with 1 being the most severe and 5 the least severe.
- Severity levels are mapped to “Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, 25 March 2003, CH 3, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND).”

During an Incident: Incident Response Plan

Incident Severity Classifications

Severity Level	Description	Example	CJCSM 6510.1 Severity
5	Small numbers of system probes or scans detected on external systems.	Network administrator detects intermittent pinging activity to router from known source.	n/a
	Isolated lapses in physical security.	Broken lock has not been fixed on door. No information missing.	n/a
1	Successful root level intrusion, Denial of Service, Reconnaissance and Malicious Logic with significant impact on operations.	Successful login to router by unauthorized personnel (internal or external Network Administrator.	Severe
	Widespread lapses in physical, environmental or personnel security, Significant risk to TMA operations or negative public relations impact.	Papers and files on desk are stolen from desk in office with broken door lock that has not been fixed for extended period of time. Papers contain sensitive information.	Severe

The MHS Health Information Privacy and Security Compliance Committee (HIPSCC)

- Mission: To oversee the status of health information security and privacy compliance across the MHS
- Responsibilities:
  - To advise on positions and challenges relative to privacy and security issues
  - To support efforts to ensure the privacy and security of health information held by TMA and its business associates

Veterans Health Administration (VHA)
Data Security and Storage

- Requiring facilities to refrain from storing individually identifiable information on desktops unless absolutely necessary. Whenever possible use secure network drives.

VHA
Data Security and Storage

- Placing servers and other devices in a locked secure area
- Physically locking up laptops when on site
- Restricting access to private and secure areas
- Enforcing policies on electronic data security

VHA
Portable Storage Devices

- Requiring facilities to refrain from storing individually identifiable information on laptops unless absolutely necessary, then ENCRYPT.
- VA Directive 6504 addresses encryption requirements, secure storage of portable devices and approvals for employees to remove data from facilities.

VHA

Portable Storage Devices

- **Laptop Encryption Effort through September 15, 2006 Includes:**
  - Government Furnished Laptops
  - Windows Based Laptops
  - Research Laptops
  - Remote desktops that are utilized similar to a remote laptop
- **Follow-on phases will address:**
  - Personally Owned and Contractor Owned Devices
  - Macintosh and Linux OS
  - Mobile Media - USB, CD's
  - Encrypted Laptops Using Encryption Software Other Than GuardianEdge
  - Desktops
  - OIG Laptops/Remote Devices that are currently using PGP Encryption

VHA
Employees Taking Data Outside VA

- Request and obtain supervisor and ISO approval for such transport, transmission, access, use, processing or storage;
- Take appropriate measures to protect information, network access, passwords and equipment;
- Promptly report misuse of access or compromise or loss of VA information assets;

Employees Taking Data Outside VA

- Refrain from using automatic password saving features;
- Use extreme caution when accessing VA information in open areas or areas where non-authorized persons may see VA information such as airport lounges and hotel lobbies; and
- Protect VA equipment and information from loss or theft at all times, especially when traveling.

VHA
Teleworking

- Risks
  - Remote access to systems.
  - Removal of data from organization’s physical and technical confines.
  - Lack of appropriate user awareness of technical security safeguards.
  - Lack of appropriate physical security controls outside VA facilities.

VHA

Mitigation Strategies For Teleworking

- Physically secure equipment at all times – if equipment is out of your control it must be locked up using security controls outlined in VA Directive 6504.
- Ensure equipment is up to date on virus protections and firewall software.
- Restrict remote employees to government owned equipment.
- Enforce PC health checks for all remote connections to VA networks.

VHA

Mitigation Strategies for Teleworking

- Involve the Information Security Officer and the Supervisor in the approval process.
- Promote remote access as the exception not the norm.
- Conduct annual review of policies, procedures, and telework agreements.

VHA
Incident Response

- Implemented in the event of a suspected or actual unauthorized data disclosure or security breach
- Centralized approach to incident response and reporting
- Department-wide incident response policy and reporting computer system
- Interim templates for reports and notification letters provided

VHA Incident Response

Initiation and Notification

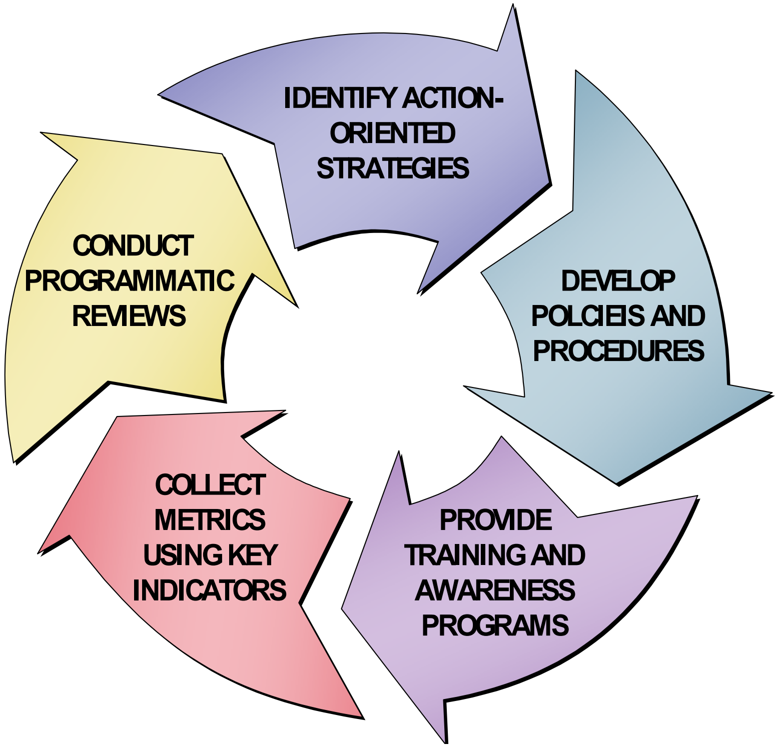
- All VA employees should notify the facility Information Security Officer (ISO) and Privacy Officer of any suspected privacy and/or security breach involving PHI as soon as the incident occurs.
- This allows for timely reporting to VA.

VHA Incident Response

Official Reporting

- The ISO will report incident to the VA-Security Operations Center (SOC) via email mail group using the Incident Report Template.
- The Privacy Officer will enter all information known about the breach into the Privacy Violation Tracking System (PVTS). The new PVTS system of linked to the VA-SOC.
- The VA-SOC will report to the US-CERT to meet the OMB mandatory one hour reporting requirement.

Privacy protection is an on-going process


IDENTIFY ACTION-ORIENTED STRATEGIES
DEVELOP POLCIEIS AND PROCEDURES
PROVIDE TRAINING AND AWARENESS PROGRAMS
COLLECT METRICS USING KEY INDICATORS
CONDUCT PROGRAMMATIC REVIEWS

QUESTIONS?

Samuel P. Jenkins, Privacy Officer

TRICARE Management Activity
Department of Defense
Sam.Jenkins@tma.osd.mil

Stephania Putt, Privacy Officer

Veterans Health Administration
Department of Veterans Affairs
Stephania.Putt@va.gov

http://www.tricare.osd.mil/TMAPrivacy/default.cfm