THE THIRTEENTH NATIONAL HIPAA SUMMIT
The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance
September 24-29, 2006
Washington DC Renaissance Hotel
Washington, DC

Data Breach Prevention 101 and Lessons Learned

Mr. Sam Jenkins

TMA Privacy Office

Department of Defense

TRICARE
Management
Activity

Agenda

- Objectives and Background
- Where were we last year?
- What happened?
- How did we respond?
- Lessons Learned

Objectives and Background

MHS: Military Health System

TMA: TRICARE Management Activity

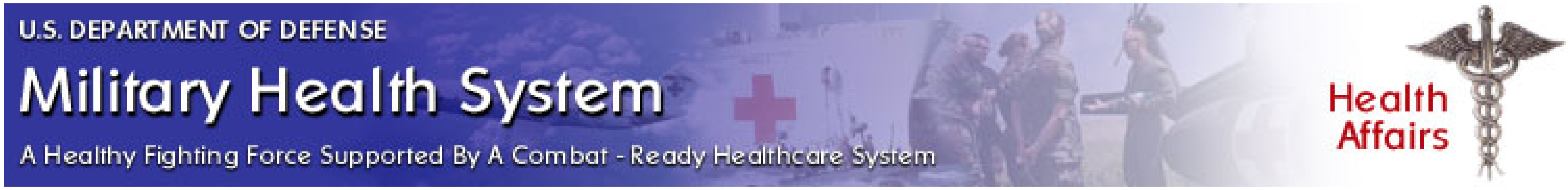
Objectives

The purpose of this presentation is to:

- Share the story about how the TRICARE Management Activity has responded to recent data breaches
- Quantify the cost estimates of recent data loss and data breaches both in the public and private sectors
- Describe government actions in response to the increase in data breaches
- Discuss the types of actions we took before, during and after a data breach

The MHS includes Provider, Payor, Government, and Life Sciences

U.S. DEPARTMENT OF DEFENSE
MILITARY HEALTH SYSTEM
TRICARE: Your Military Health Plan
TRICARE


U.S. DEPARTMENT OF DEFENSE
Military Health System
A Healthy Fighting Force Supported By A Combat - Ready Healthcare System
Health Affairs

Profile: MHS

TRICARE Facts and Figures

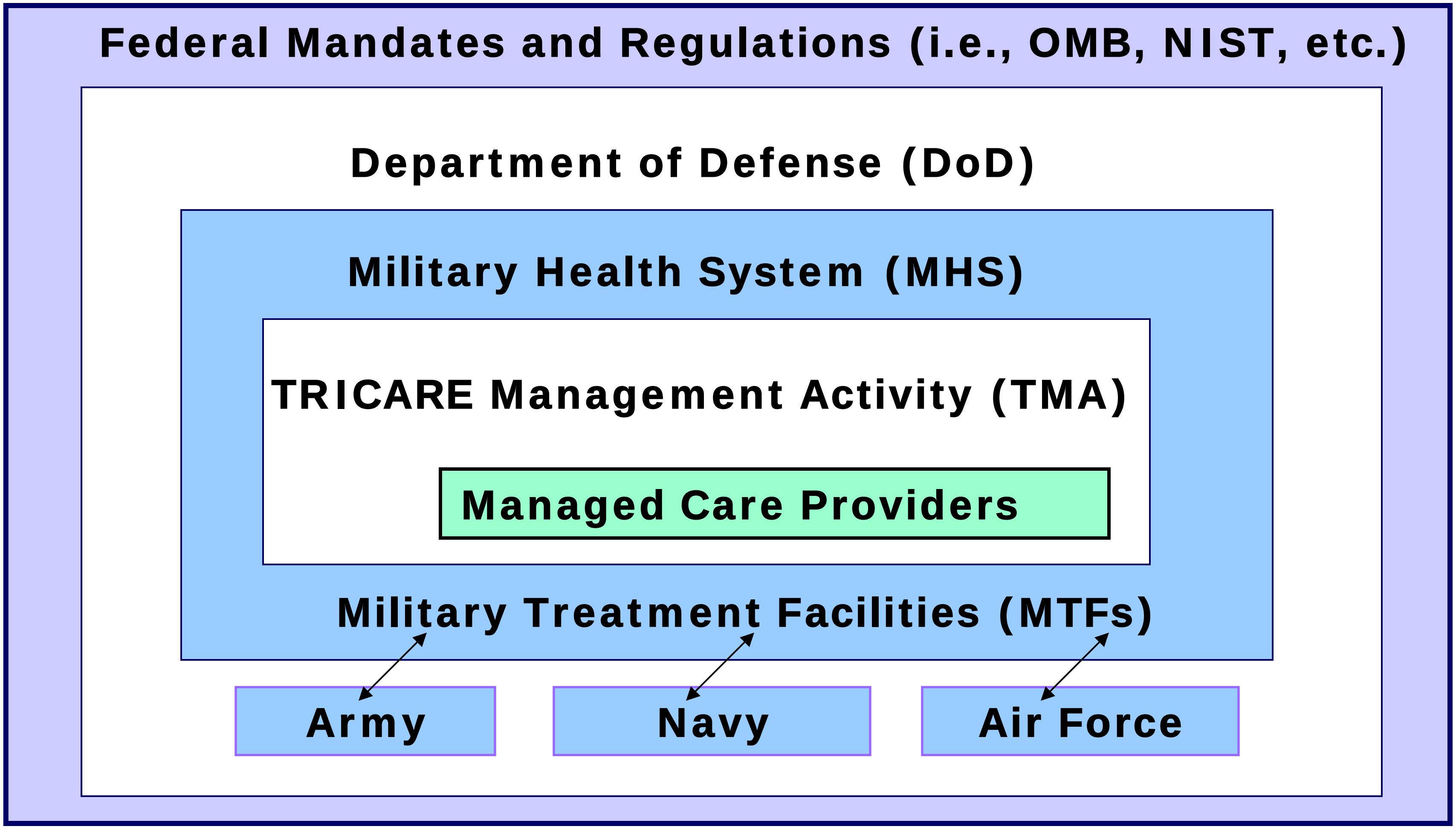
- **TRICARE Eligible Beneficiaries:** 9.2 million
- **TRICARE Prime Enrollees:** 5.0 million
- **MHS Direct Care Facilities:**
  - 70 Military Hospitals/Medical Centers
  - 411 Medical Clinics
  - 417 Dental Clinics
- **MHS Personnel:** 132,500
  - 44,100 Civilian
  - 88,400 Military
- **FY07 DoD Health Care Expenditures:** $37.1 billion
  - $26.4 billion Unified Medical Program
  - $10.7 billion Medicare Eligible Retiree Accrual Fund

A Week in the Life

- **Inpatient Admissions:** 18,300
  - 5,300 Direct Care
  - 13,000 Purchased Care
- **Outpatient Visits**: 1.8 million
  - 640,000 Direct Care
  - 1.17 million Purchased Care
- **Prescriptions:** 2.1 million (Includes retail, direct care and mail order)
- **Births:** 2,200
  - 1,000 Direct Care
  - 1,200 Purchased Care
- **Dental Procedures** (Direct care only): 104,000
- **Claims processed:** 3.12 million
- **Weekly Bill:** $711 million

Source: TRICARE Stakeholders Report 2006

Compliance environment is complex



Federal Mandates and Regulations (i.e., OMB, NIST, etc.)
Department of Defense (DoD)
Military Health System (MHS)
TRICARE Management Activity (TMA)
Managed Care Providers
Military Treatment Facilities (MTFs)
Army
Navy
Air Force

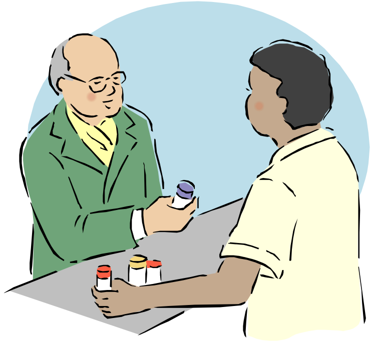
Our commitment is the driver

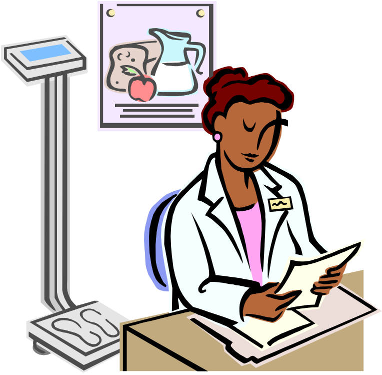
The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.

Where Were We Last Year?

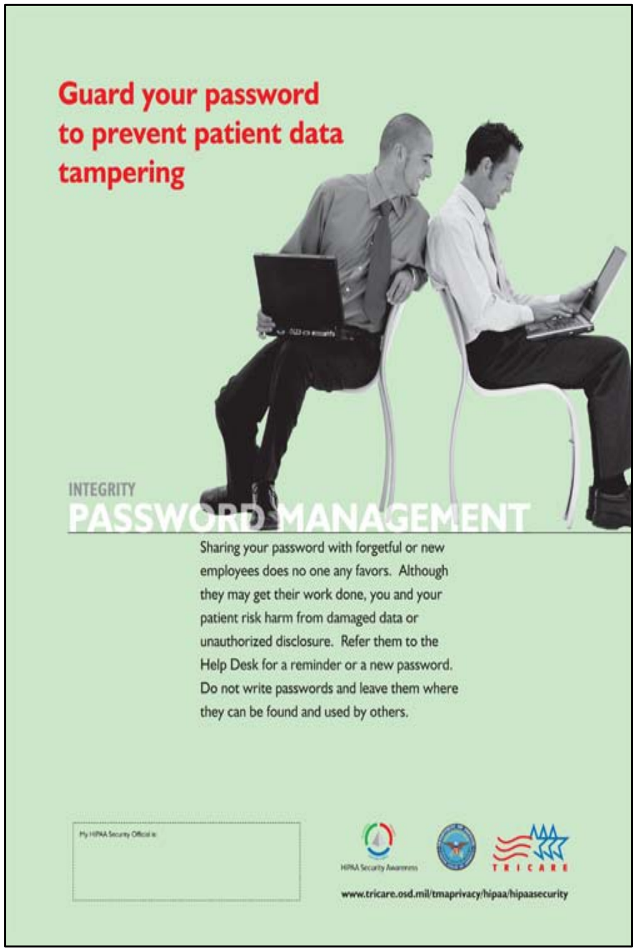
Good HIPAA security and privacy practices in place

- A lot of things going on in your day-to-day activities
  - Policies and procedures
  - Roles and responsibilities assigned
  - Access Management
  - Training and Awareness
  - Risk Management
  - Accounting of Disclosures
  - Workstation Security, etc.





Employee acceptance of HIPAA security and privacy responsibilities



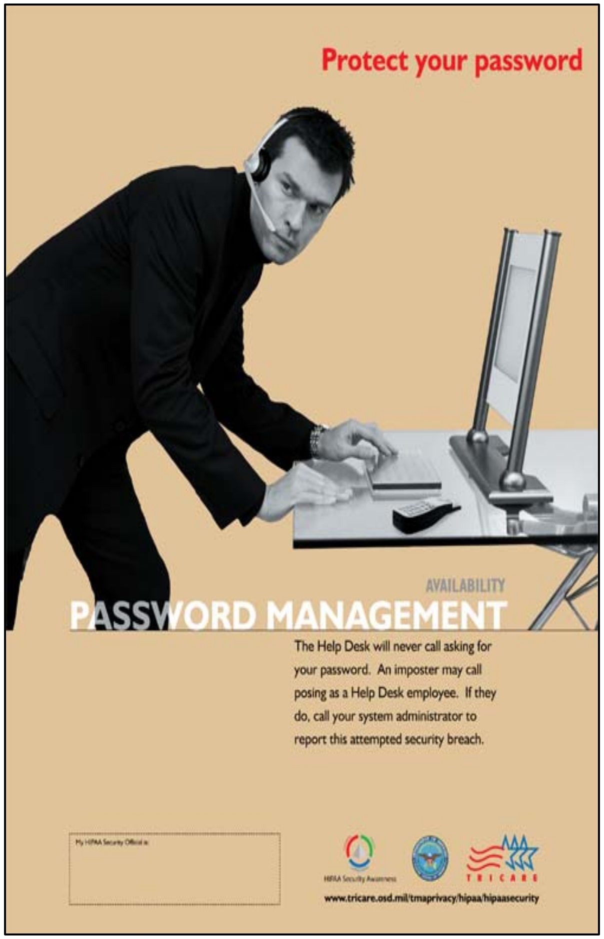
Sharing your password with forgetful or new employees does no one any favors. Although they may get their work done, you and your patient risk harm from damaged data or unauthorized disclosure. Refer them to the Help Desk for a reminder or a new password. Do not write passwords and leave them where they can be found and used by others.

My HIPAA Security Official is:

HIPAA Security Awareness

TRICARE

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



The Help Desk will never call asking for your password. An imposter may call posing as a Help Desk employee. If they do, call your system administrator to report this attempted security breach.

My HIPAA Security Official is:

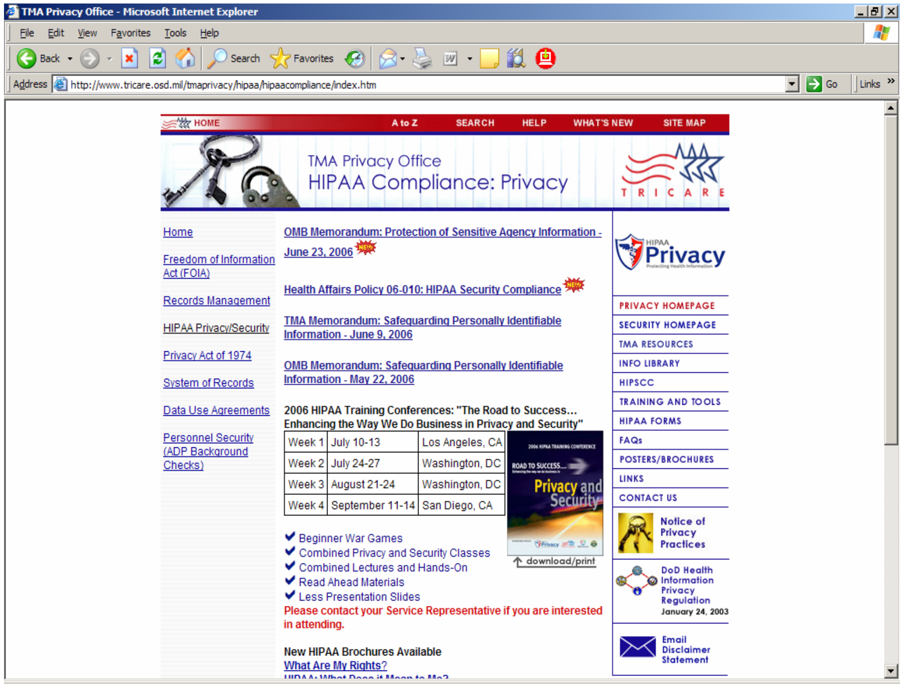
HIPAA Security Awareness

TRICARE

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

Risk management program underway

- The key to compliance is risk management. To correctly implement the security standards and establish compliance, each covered entity must:


TMA Privacy Office - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.tricare.osd.mil/tmaprivacy/hipaa/hipaacompliance/index.htm
Go Links
HOME A to Z SEARCH HELP WHAT'S NEW SITE MAP
TMA Privacy Office
HIPAA Compliance: Privacy
TRICARE
Home
Freedom of Information Act (FOIA)
Records Management
HIPAA Privacy/Security
Privacy Act of 1974
System of Records
Data Use Agreements
Personnel Security (ADP Background Checks)
HIPAA Privacy Protecting Health Information
PRIVACY HOMEPAGE
SECURITY HOMEPAGE
TMA RESOURCES
INFO LIBRARY
HIPSCC
TRAINING AND TOOLS
HIPAA FORMS
FAQs
POSTERS/BROCHURES
LINKS
CONTACT US
Notice of Privacy Practices
DoD Health Information Privacy Regulation January 24, 2003
Email Disclaimer Statement
NEW
2006 HIPAA TRAINING CONFERENCE
ROAD TO SUCCESS...
Privacy and Security
download/print

OMB Memorandum: Protection of Sensitive Agency Information - June 23, 2006

Health Affairs Policy 06-010: HIPAA Security Compliance

TMA Memorandum: Safeguarding Personally Identifiable Information - June 9, 2006

OMB Memorandum: Safeguarding Personally Identifiable Information - May 22, 2006

2006 HIPAA Training Conferences: "The Road to Success... Enhancing the Way We Do Business in Privacy and Security"

Week 1	July 10-13	Los Angeles, CA
Week 2	July 24-27	Washington, DC
Week 3	August 21-24	Washington, DC
Week 4	September 11-14	San Diego, CA

✓ Beginner War Games
✓ Combined Privacy and Security Classes
✓ Combined Lectures and Hands-On
✓ Read Ahead Materials
✓ Less Presentation Slides

Please contact your Service Representative if you are interested in attending.

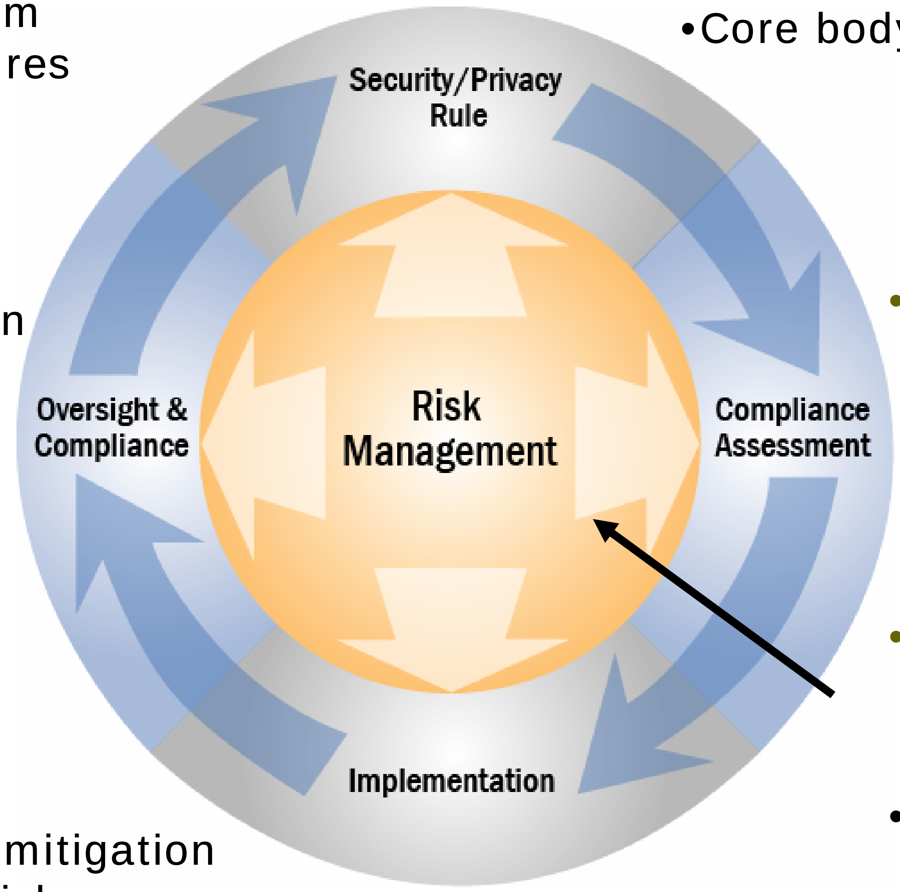
New HIPAA Brochures Available
What Are My Rights?

- Assess potential risks and vulnerabilities to ePHI
- Develop, implement, and maintain appropriate security measures given those risks
- Document those measures and keep them current

Continuous cycle of improvement tracking

- Metrics Program guides, measures and reports effectiveness of HIPAA implementation

- Core body of knowledge



- Self-assessment tool: initial compliance assessment

- Ongoing cycle of risk management and improvement

- Institutionalizes activities of risk management

- Prioritized mitigation based on risk analysis

What Happened?

Data breaches occurred – TMA was not exempt

TRICARE

TRICARE
Management
Activity

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

Marriott

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

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

Fidelity
INVESTMENTS

American
Red Cross

1 million personal records **stolen**

573,000 state employee records **stolen**

GTA
Georgia Technology Authority

United States
Department of Veterans Affairs

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

One in five American affected this year

TRICARE

TRICARE Management Activity

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

Marriott

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

196,000 customer s
security numbers, n
birthdates and addr

Fidelity INVESTMENTS

Since January 1, 2006 more than 63.7 million Americans – 21% of the population – have had their personal information lost or stolen.

personal
ds **stolen**

573,000 state employee records **stolen**

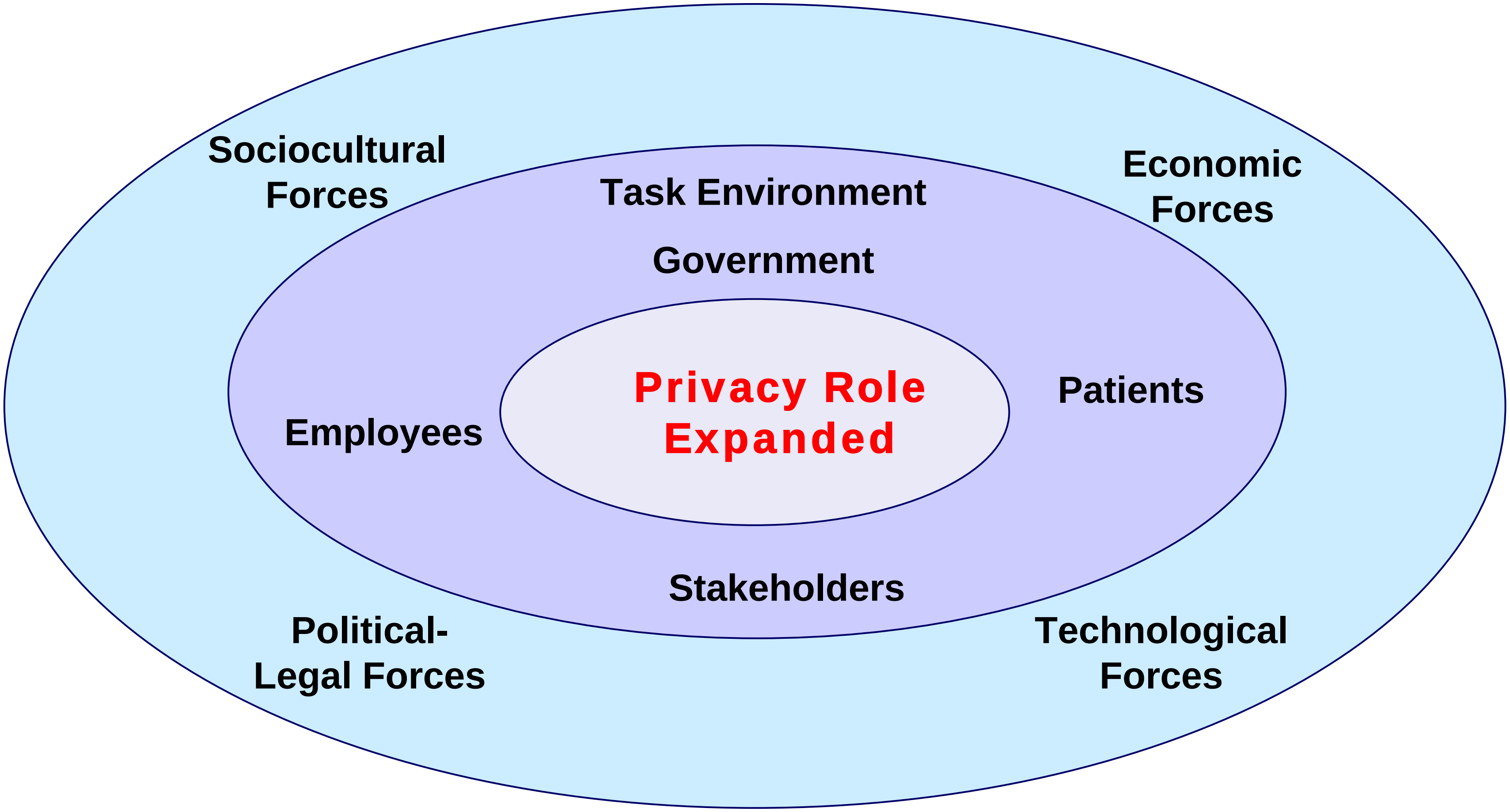
GTA

Georgia Technology Authority

United States Department of Veterans Affairs

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

Societal environment changed – we are all now more on guard



Source: Adapted from Wheelen, T.L. and Hunger, J.D. (2004). Strategic Management and Business Policy. New Jersey: Prentice Hall.

Snapshot of our reality- Data breaches are expected

Economic:

- Military Deployments
- Resource Constraints
- Rising healthcare costs
- Global Pressures

Technological:

- Regulations on Technology
- More Remote Access
- Skill Level of Workforce
- Technology Availability

Political – Legal:

- Regulations – FISMA, OMB
- Mandates
- More data sharing Other Government Policies
- Legal Implications

Sociocultural:

- Lifestyle – More telecommuting
- Attitudes and Beliefs – 24/7
- Demographics – Aging workforce
- Status Symbols - Blackberry

Snapshot of our reality- Data breaches are inevitable

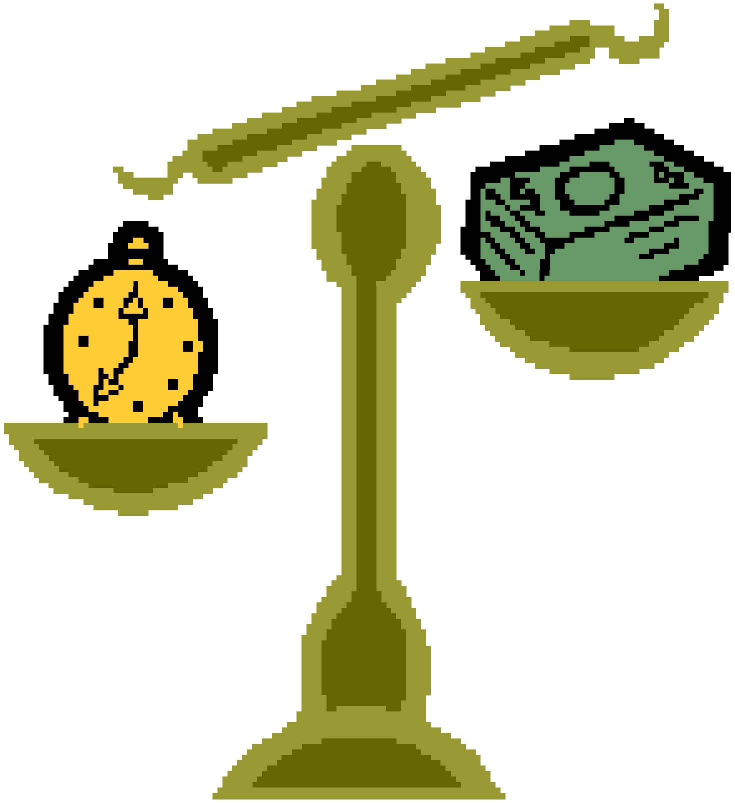
Entity*	Type of Breach	# of Individuals Affected
Department of Justice	Stolen laptop (5/7/05)	80,000
Minnesota Department of Revenue	Data tape backup package missing	50,400
U.S. Navy	Files on civilian web site	30,000
Equifax	Stolen company laptop	2,500
American Red Cross	Dishonest employee (5/24/06)	1,000,000
Kent State University	Stolen laptop (6/17/05) Stolen computers (9/10/05)	1,400 100,000
CitiFinancial	Lost backup tape (6/6/05)	3,900,000
DSW	Hacking (3/8/05) Hacking (4/18/05)	100,000 1,300,000

**Source: Estimates based on various news media reports*

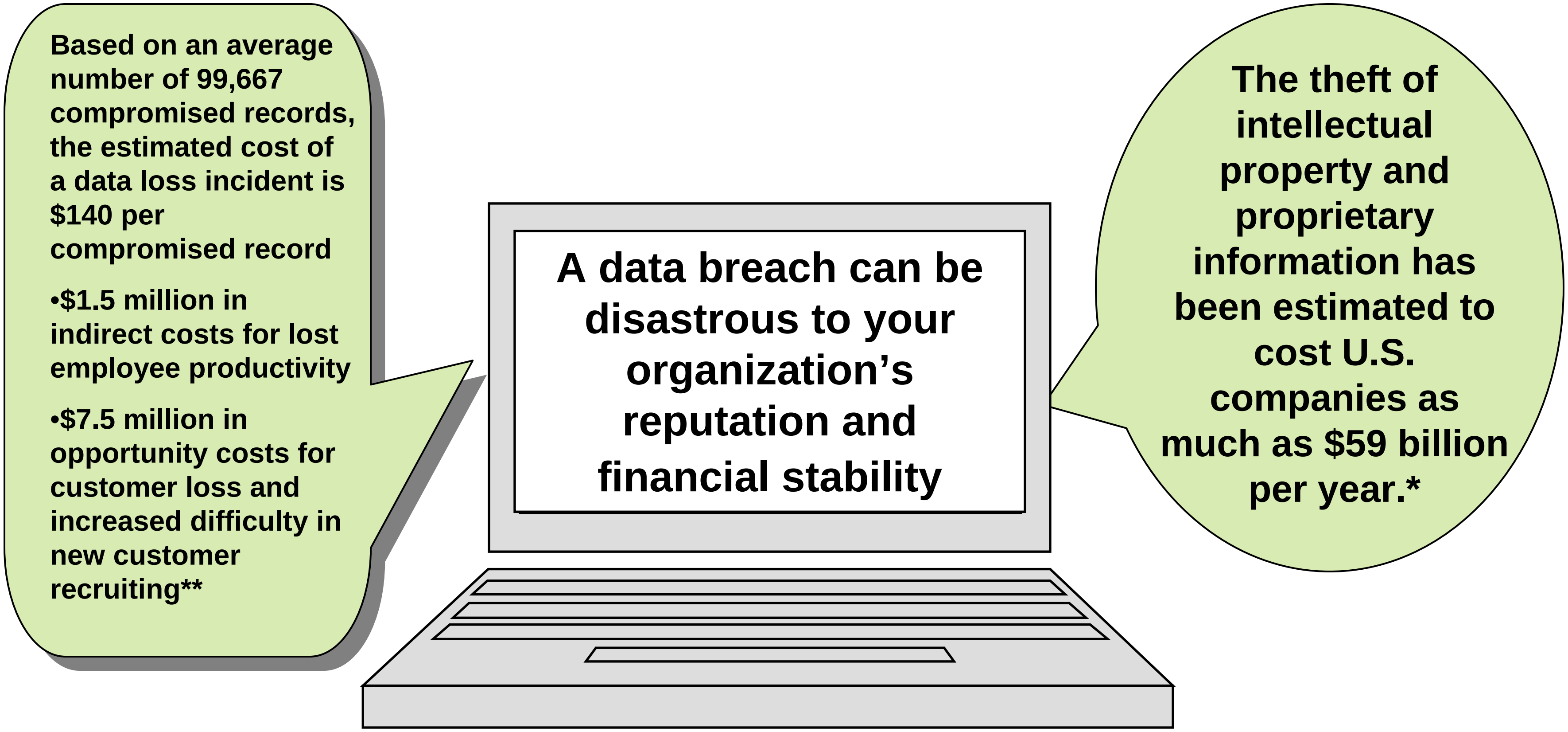
Result: Tangible and intangible costs

If a data breach does occur, the costs will likely overwhelmingly outweigh the costs of implementing remediation efforts.

- Loss of current and future customers
- Tarnished reputation
- Lawsuit/legal fees
- Fines and penalties
- Administrative Costs (letters, stamps, call centers, credit monitoring)



Preventing a data incident is less costly…



Based on an average number of 99,667 compromised records, the estimated cost of a data loss incident is $140 per compromised record

•$1.5 million in indirect costs for lost employee productivity

•$7.5 million in opportunity costs for customer loss and increased difficulty in new customer recruiting**

A data breach can be disastrous to your organization's reputation and financial stability

The theft of intellectual property and proprietary information has been estimated to cost U.S. companies as much as $59 billion per year.*

*Source: Trends in Proprietary Information Loss Survey Report, PricewaterhouseCoopers, U.S. Chamber of Commerce, American Society for Industrial Security, September 2002

**Source: Lost Customer Information: What Does a Data Breach Cost Companies? Ponemon Institute PGP® Research Report, November 2005

…than the costs for 'clean-up'

A Gartner study indicates:
It is markedly less expensive to invest in new security and encryption technologies than it is for them to respond to a data breach.

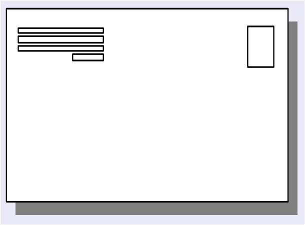
<u>Costs include:</u>

- Approximately $6 per year per user for encryption tools; or
- $16 per user per year for intrusion prevention software licenses
- $90 per user to address problems after a breach has occurred*

**Source: Gartner Says Rash of Personal Data Thefts Shows Social Security Numbers Can No Longer Be Sole Proof of Identity for Enterprises, Gartner, June 5, 2006*

Remediation costs can multiply*

Notification Letter



$1.50-2.00 per individual

Call Center

$10 to $31 per call

Legal Fees

$1,000+ per case

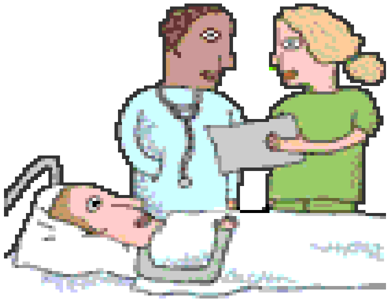
Fines / Penalties

$1000-$250,000
per incident

Credit monitoring

$60 per person

Loss of consumer confidence



Priceless

**Source: Estimates based on various news media reports*

Recent data breach costs have reached approximately $30+ Million…and rising*

ChoicePoint

- Legal Fines = **$15 Million**
- Contacting consumers and credit monitoring = **$2 Million**
- Other
  - Market capitalization loss = **$720 Million**
  - Direct breach charges, excluding fines = **$11.5 Million**

TOTAL: over **$?? Million**

Department of Veterans Affairs

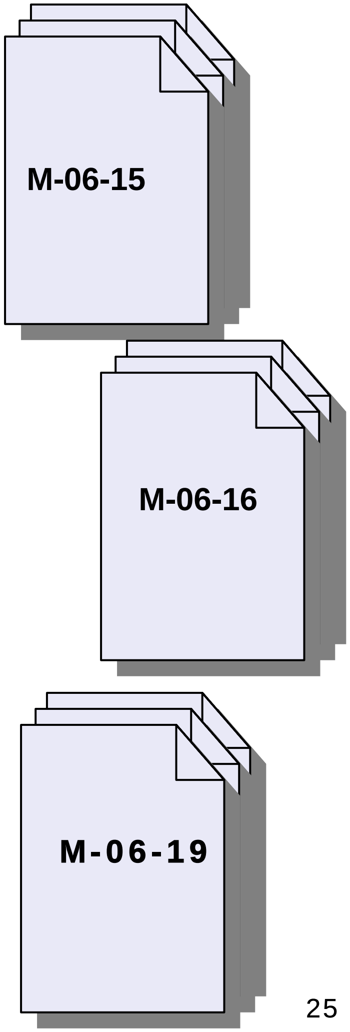
- Notification letters to 17.5 million veterans = **$7 Million**
- Legal Fines
  - Lawsuit filed requesting $1,000 per victim = **$26.5 Billion**
- Credit Monitoring **(N/A)**
- Call Center = **$200,000 per day ($10+Million)**

TOTAL: over **$?? Million**

Source: Estimates based on various news media reports

New mandates from OMB

- To date, OMB has issued three memoranda establishing requirements and providing guidance on protecting PII
  - On May 22, 2006, OMB issued **M-06-15**, *Safeguarding Personally Identifiable Information*
  - On June 23, 2006, OMB issued **M-06-16**, *Protection of Sensitive Agency Information*
  - On July 12, 2006, OMB issued **M-06-19**, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
- Several pieces of legislation on data breach notification are currently pending



OMB goal: Safeguarding 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

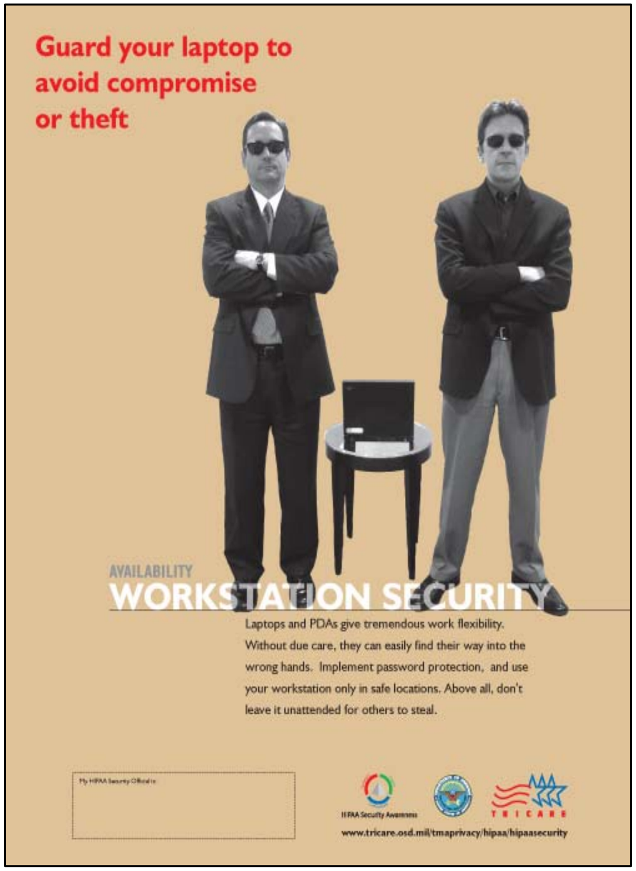
- Revises current reporting requirements to require agencies to report **all** (electronic and physical form) incidents involving personally identifiable information to US-CERT **within one hour** of discovery (both suspected and confirmed breaches)
- Privacy and Security Funding Reminder

How Did We Respond?

Prevention 101
Lessons Learned

We took a good look at ourselves based on what was happening to others

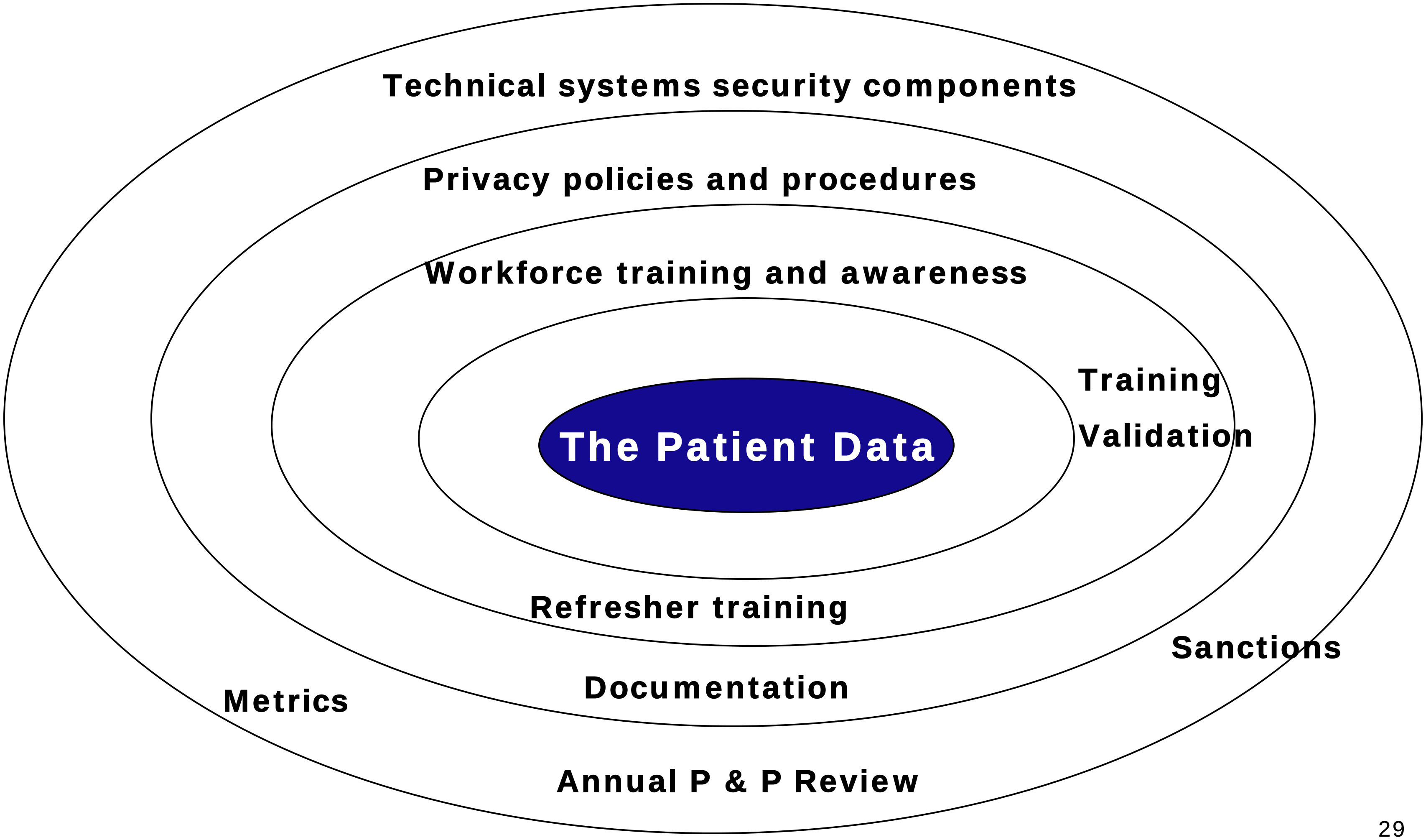
- "If it can happen to them, it can happen to me …"
- The greatest risk to safeguarding our data is the human factor



Laptops and PDAs give tremendous work flexibility. Without due care, they can easily find their way into the wrong hands. Implement password protection, and use your workstation only in safe locations. Above all, don't leave it unattended for others to steal.

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

We implemented and reinforced complementary protection processes



Technical systems security components
Privacy policies and procedures
Workforce training and awareness
Training
Validation
The Patient Data
Refresher training
Sanctions
Documentation
Metrics
Annual P & P Review

We took a proactive stance to prevent data breaches

- We investigated potentially risky business practices, and took actions, such as:
  - Reviewed teleworking arrangements
  - Managed portable storage devices
  - Stopped unencrypted data transmission
  - Confirmed system access privileges
  - Implemented all new government privacy requirements in timely manner

Privacy Act of 1974
FOIA of 1966
E-Government Act of 2002
FISMA

Action required

Reviewed Teleworking Arrangements

Risks	Mitigation Strategies
• 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.

Action required

Managed Portable Storage Devices

Risks	Mitigation Strategies
• 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.

Action required

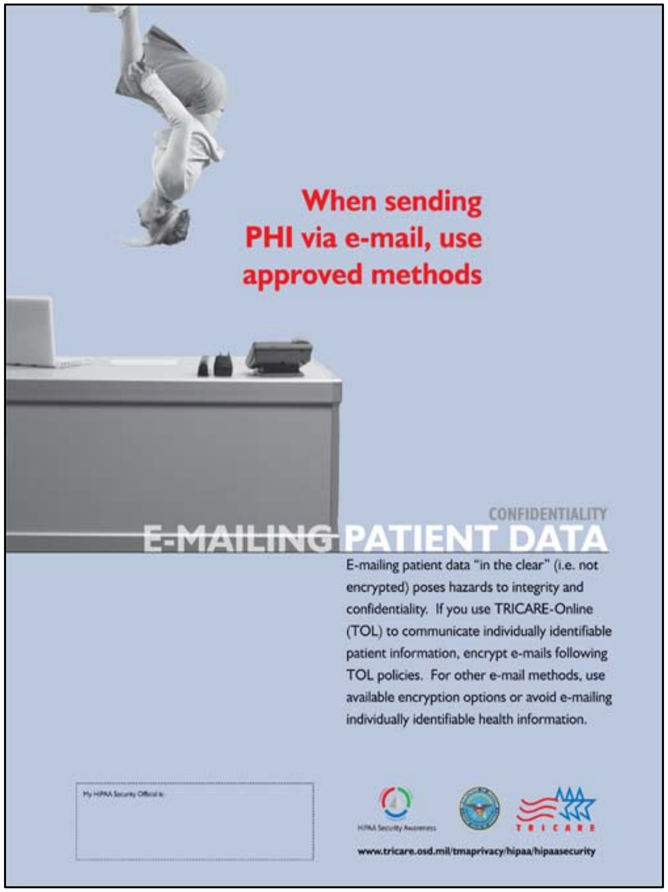
Stopped Unencrypted Data Transmission

Risks

- Data can be intercepted by unauthorized persons.

Mitigation Strategies

- Mandate the encryption of all data transmissions.



When sending PHI via e-mail, use approved methods

CONFIDENTIALITY

E-MAILING PATIENT DATA

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:

HIPAA Security Awareness

TRICARE

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

Action required

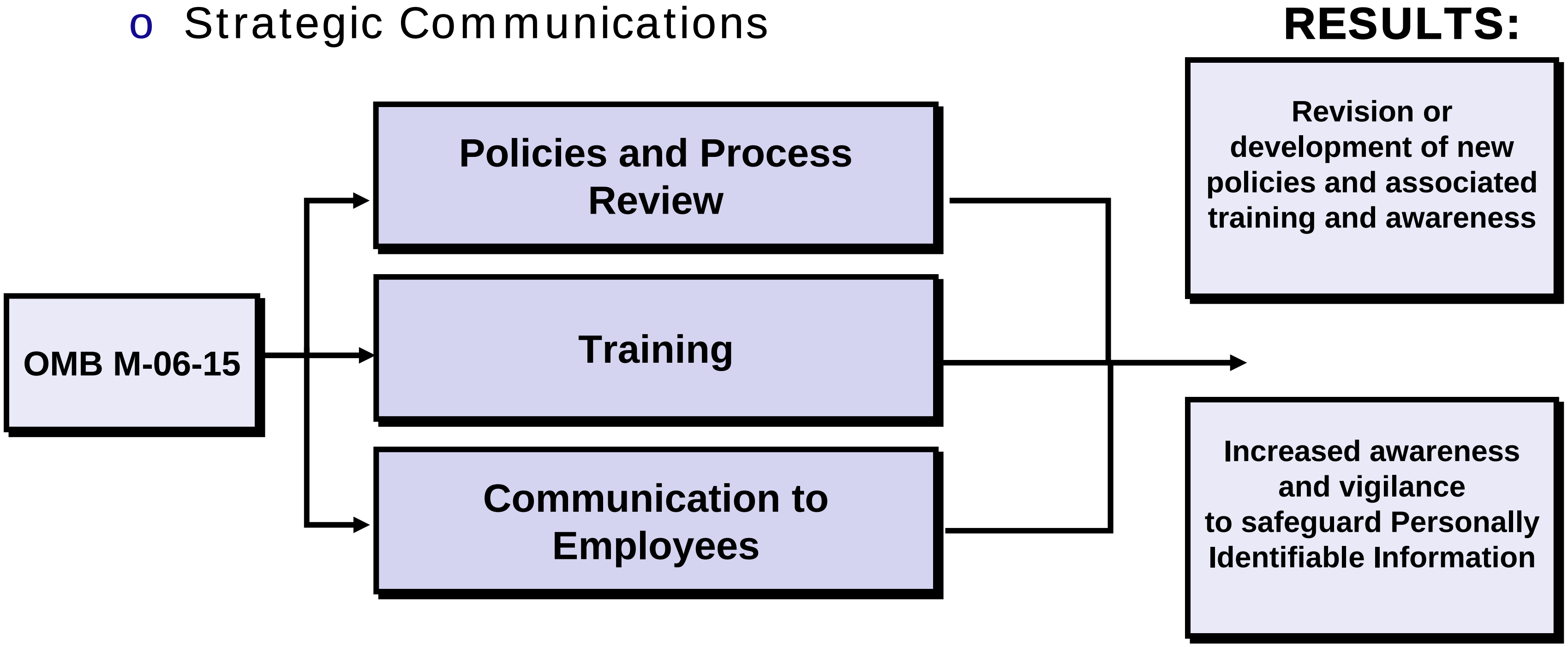
Confirmed System Access Privileges

Risks	Mitigation Strategies
• Employee access privileges frequently 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.

Action required

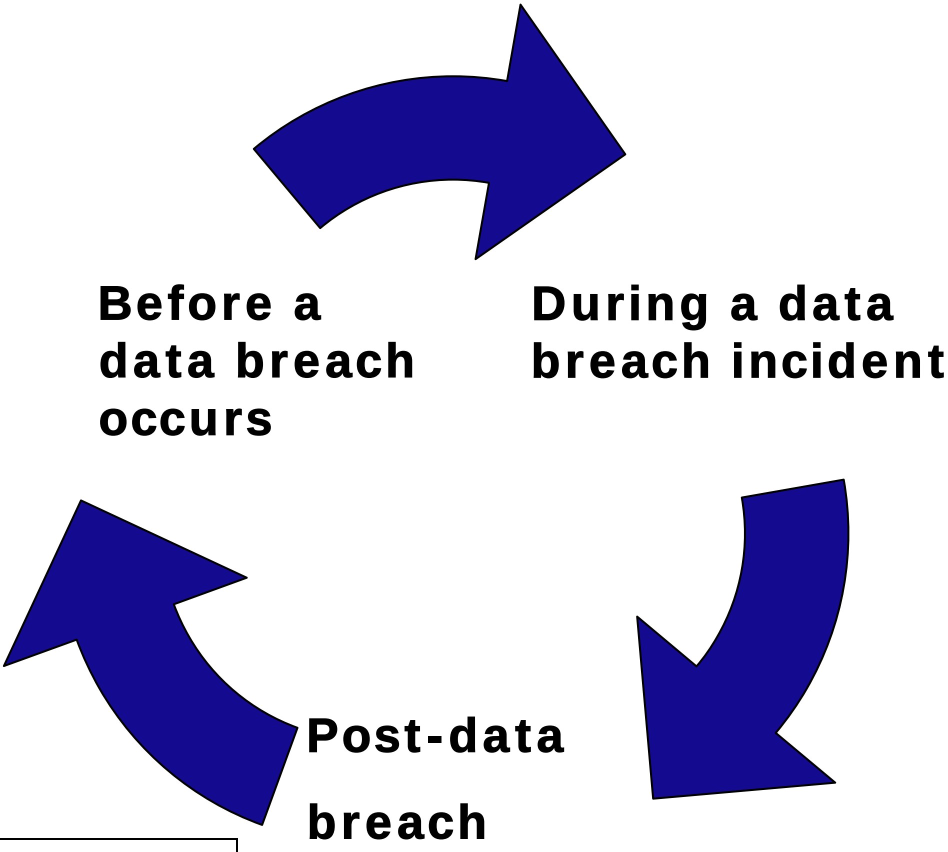
Implemented OMB M-06-15

- Our three pronged approach met, and exceeded, stated requirements
- Activities included:
  - Policies and Process Review
  - Mandatory Training
  - Strategic Communications


RESULTS:
OMB M-06-15
Policies and Process Review
Training
Communication to Employees
Revision or development of new policies and associated training and awareness
Increased awareness and vigilance to safeguard Personally Identifiable Information

Prevention activities are ongoing

- Establish policies and procedures
- Define roles and responsibilities
- Train employees
- Implement administrative, physical and technical controls



Before a data breach occurs

During a data breach incident

Post-data breach

- Coordinate with public affairs and legal
- Keep leadership appraised
- Inform affected individuals

- Document lessons learned

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.

Due Diligence:
How Do You Know You Are Safe?

- ***What are your policies and procedures related to the protection of data and PHI?***
- ***Have you mapped the flow of data in your organizations?***
- ***Have you expanded your HIPAA and other Privacy and Security training to include related responsibilities?***
- ***Do you have an incident response plan?***

CONFIDENTIALITY

PASSWORD MANAGEMENT

DoD regulations require passwords of eight or more characters that have a mixture of upper and lower case letters, numbers, and special characters. To help you remember multiple passwords, develop an easily remembered system or pattern. Follow the rules and change your password regularly. Do not write passwords and leave them where they can be found and used by others.

My HIPAA Security Official is:

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

Due Diligence:
How Do You Know You Are Safe?

- ***Are you aware of the issues your HIPAA Privacy and Security Officers are facing?***
- ***Are there enough resources? Do you have the time, personnel, and money to effectively execute and monitor a comprehensive Privacy and Security program?***
- ***Are we doing enough to prevent a data breach from happening?***

Question visitors
to protect patient
privacy and safety

INTEGRITY

VISITOR CONTROL

Hospitals and clinics fill with people everyday. Take the time to ask lost or otherwise out-of-place individuals if they need assistance in finding their way. They won't mind if they have genuine reasons for visiting your facility. Patient privacy and safety will be ensured if you turn away persons who may have bad intentions.

My HIPAA Security Official is:

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

Resources

- TMA Privacy Web Site: www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- Contact us at the TMA Privacy Office: privacymail@tma.osd.mil

THANKS!!!