



HEALTH AFFAIRS



TRICARE
Management
Activity

A Tale of Two HIPAA Security Officers

2007 Quarterly Training

TMA Privacy Office



HIPAA Security

The Unknown

As we know,

There are known knowns.

There are things we know we know.

We also know

There are known unknowns.

That is to say
We know there are some things
We do not know.
But there are also unknown unknowns,
The ones we don't know
We don't know.

—Feb. 12, 2002, DoD news briefing

A Tale of Two Security Officers

Training Objectives

- Depict typical daily activities
- Present possible hurdles associated with handling an incident
- Provide insight into successes and pitfalls from two different approaches:
 - Laurel (IDEAL)
 - Meeting all requirements
 - Proactive
 - Hardy (REALITY)
 - Doing what's necessary
 - Reactive

A Tale of Two HIPAA Security Officers

Agenda

- In the Beginning
 - Roles and Responsibilities
 - Risk Management
- When It Hits the Fan
 - Detect
 - Manage
 - Notify
 - Handle
- Business As Usual
 - Follow-up Activities
 - Reporting

Presentation Layout

Before we begin...

- Three handouts
 - Tale of Two HIPAA Security Officers (this presentation)
 - Laurel's Survival Kit (companion presentation)
 - HIPAA Security Officer Appointment Letter (memorandum)
- For presentation purposes, this material has been augmented with excerpts from the other two documents
 - Injected excerpts of the Appointment Letter
 - Resource references from the Survival Kit

Appointment Letter References



**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS**

SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

**TRICARE
MANAGEMENT
ACTIVITY**

SEP 9 2004

**MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE**

**SUBJECT: Request to Appoint Medical Treatment Facility and Dental Treatment Facility
Health Insurance Portability and Accountability Act of 1996 Security Officials**

Survival Kit

See the bright background?

Resource

**incredibly rich, interactive
discussion ensues**

In the Beginning



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

SEP 9 2004

MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE

SUBJECT: Request to Appoint Medical Treatment Facility and Dental Treatment Facility
Health Insurance Portability and Accountability Act of 1996 Security Officials

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, administrative simplification provisions require the protection and privacy of individually identifiable health information. The HIPAA Security rule, signed in February 2003, mandates the standards for the integrity, confidentiality, and availability of electronically protected health information. Full compliance with its requirements must be met by April 21, 2005.

The purpose of this memorandum is to request the appointment of a HIPAA Security Official at each military treatment facility and dental treatment facility (MTF/DTF). HIPAA Security Officials will be responsible for managing the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule. Responsibilities also include managing and supervising the conduct of personnel in relation to those measures. Based on the size and complexity of the MTF/DTF, a HIPAA Security Official may be responsible for more than one facility in a geographic area when smaller facilities can share resources under a mutually acceptable agreement. The HIPAA Security Official will be the MTF/DTF point of contact for HIPAA Security implementation and receive training and guidance from the respective Service HIPAA Program Office. Suggested roles and responsibilities are described in the attachment to this memorandum. It is imperative that the person selected as the MTF/DTF



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

SEP 9 2004

MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE

SUBJECT: Request to Appoint Medical Treatment Facility and Dental Treatment Facility
Health Insurance Portability and Accountability Act of 1996 Security Officials

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, administrative simplification provisions require the protection and privacy of individually identifiable health information. The HIPAA Security rule, signed in February 2003, mandates the standards for the integrity, confidentiality, and availability of electronically protected health information. Full compliance with its requirements must be met by April 21, 2005.

The purpose of this memorandum is to request the appointment of a HIPAA Security Official at each military treatment facility and dental treatment facility (MTF/DTF). HIPAA Security Officials will be responsible for managing the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule. Responsibilities also include managing and supervising the conduct of personnel in relation to those measures. Based on the size and complexity of the MTF/DTF, a HIPAA Security Official may be responsible for more than one facility in a geographic area when smaller facilities can share resources under a mutually acceptable agreement. The HIPAA Security Official will be the MTF/DTF point of contact for HIPAA Security implementation and receive training and guidance from the respective Service HIPAA Program Office. Suggested roles and responsibilities are described in the attachment to this memorandum. It is imperative that the person selected as the MTF/DTF



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

SEP 9 2004

MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE

SUBJECT: Request to Appoint Medical Treatment Facility and Dental Treatment Facility
Health Insurance Portability and Accountability Act of 1996 Security Officials

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, administrative simplification provisions require the protection and privacy of individually identifiable health information. The HIPAA Security rule, signed in February 2003, mandates the standards for the integrity, confidentiality, and availability of electronically protected health information. Full compliance with its requirements must be met by April 21, 2005.

The purpose of this memorandum is to request the appointment of a HIPAA Security Official at each military treatment facility and dental treatment facility (MTF/DTF). HIPAA Security Officials will be responsible for managing the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule. Responsibilities also include managing and supervising the conduct of personnel in relation to those measures. Based on the size and complexity of the MTF/DTF, a HIPAA Security Official may be responsible for more than one facility in a geographic area when smaller facilities can share resources under a mutually acceptable agreement. The HIPAA Security Official will be the MTF/DTF point of contact for HIPAA Security implementation and receive training and guidance from the respective Service HIPAA Program Office. Suggested roles and responsibilities are described in the attachment to this memorandum. It is imperative that the person selected as the MTF/DTF

In the Beginning

You've Been Appointed HIPAA Security Officer – Now What?

- Is your appointment in writing?
- Was the workforce notified of your appointment?
- You're here: who's watching the shop back home?
- What kind of training have you received?

When leaving your workstation unattended, logoff to preserve confidentiality



CONFIDENTIALITY LOGOFF WORKSTATION

Many things can happen if you do not logoff your workstation when leaving. Unauthorized persons can view or modify patient information. An unsecured computer can compromise patient care, damage professional reputations, create extra work to repair the damage, and lead to lawsuits and fines. Take the time: logoff!

My HIPAA Security Official is:

YOUR Name Goes Here



HIPAA Security Awareness



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

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
MEDICAL TREATMENT FACILITY/DENTAL TREATMENT FACILITY
SECURITY OFFICIAL
ROLES AND RESPONSIBILITIES**

Organizational Need/Function: The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires Medical Treatment Facility and Dental Treatment Facility (MTF/DTF) personnel to be assigned the responsibility of managing and supervising the execution and use of security measures to protect data as well as the responsibility of managing and supervising the conduct of personnel in relation to those measures.

ROLES AND RESPONSIBILITIES

Policy Implementation, Oversight, Auditing and Compliance:

- Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule.
- Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassess status and updated security standards established by the facility.



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

TRICARE
MANAGEMENT
ACTIVITY

SEP 9 2004

MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE

SUBJECT: Request to Appoint Medical Treatment Facility and Dental Treatment Facility
Health Insurance Portability and Accountability Act of 1996 Security Officials

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, administrative simplification provisions require the protection and privacy of individually identifiable health information. The HIPAA Security rule, signed in February 2003, mandates the standards for the integrity, confidentiality, and availability of electronically protected health information. Full compliance with its requirements must be met by April 21, 2005.

The purpose of this memorandum is to request the appointment of a HIPAA Security Official at each military treatment facility and dental treatment facility (MTF/DTF). HIPAA Security Officials will be responsible for managing the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule. Responsibilities also include managing and supervising the conduct of personnel in relation to those measures. Based on the size and complexity of the MTF/DTF, a HIPAA Security Official may be responsible for more than one facility in a geographic area when smaller facilities can share resources under a mutually acceptable agreement. The HIPAA Security Official will be the MTF/DTF point of contact for HIPAA Security implementation and receive training and guidance from the respective Service HIPAA Program Office. Suggested roles and responsibilities are described in the attachment to this memorandum. It is imperative that the person selected as the MTF/DTF

In the Beginning

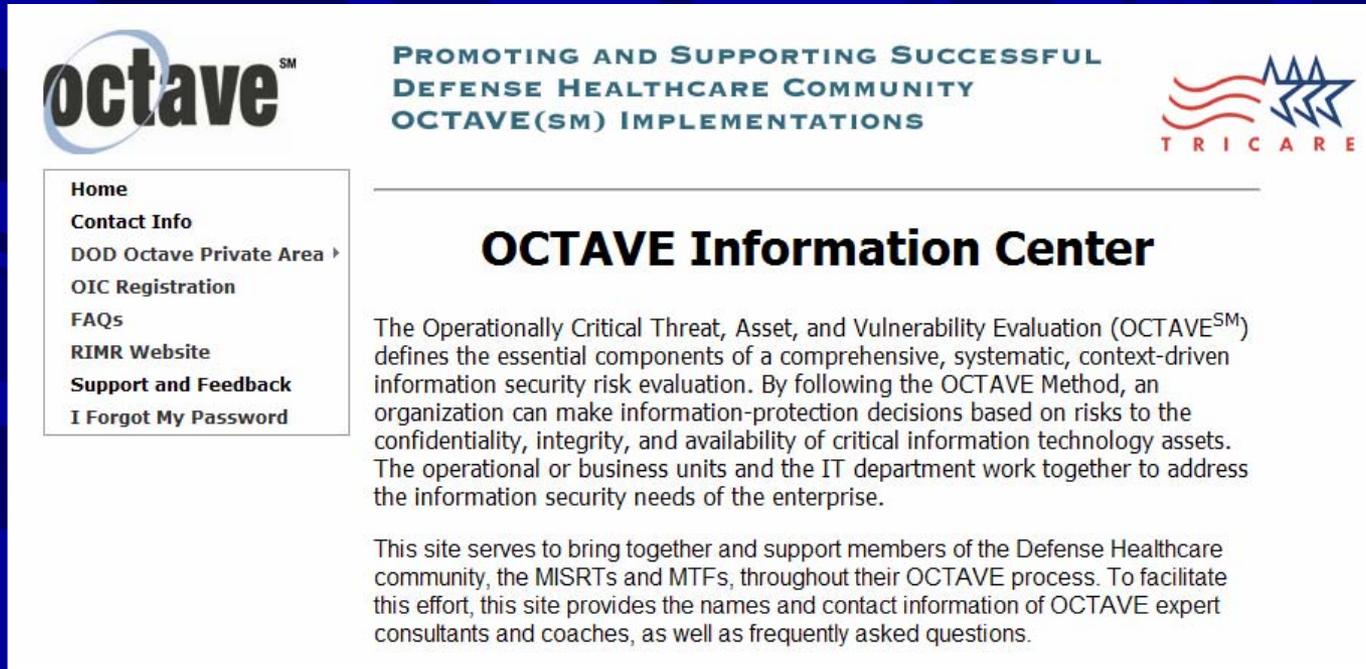
What's The Status of Your Program?

- Walkabout
- Coordination with other personnel with security responsibility
- Review of materials
- Transition Process/Binder
 - Date of last Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM)
 - OCTAVESM reports
 - Plans of Action and Milestones (POA&M)
 - Hot issues

Where Can You Find OCTAVESM?

<https://tmaoctave.aticorp.org>

Survival Kit



octaveSM

PROMOTING AND SUPPORTING SUCCESSFUL
DEFENSE HEALTHCARE COMMUNITY
OCTAVE(SM) IMPLEMENTATIONS



TRICARE

- Home
- Contact Info
- DOD Octave Private Area ▶
- OIC Registration
- FAQs
- RIMR Website
- Support and Feedback
- I Forgot My Password

OCTAVE Information Center

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVESM) defines the essential components of a comprehensive, systematic, context-driven information security risk evaluation. By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets. The operational or business units and the IT department work together to address the information security needs of the enterprise.

This site serves to bring together and support members of the Defense Healthcare community, the MISRTs and MTFs, throughout their OCTAVE process. To facilitate this effort, this site provides the names and contact information of OCTAVE expert consultants and coaches, as well as frequently asked questions.

Resource

In the Beginning

What's Your Job? (1 of 4)

■ Security Officer

- Responsible for the development, implementation, maintenance, oversight, and reporting of security requirements for Electronic Protected Health Information (ePHI)
- Provide strategic and tactical program direction, and exercise authority over all programmatic components as necessary to accomplish ePHI security compliance

In the Beginning

What's Your Job? (2 of 4)

■ Security Officer

- Ensure that requirements for ePHI are integrated into all policies and procedures for the planning, development, implementation, and management of the Department of Defense (DoD) infrastructure and information systems
- Perform internal audits of data access and use to detect and deter breaches of ePHI. Ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct

In the Beginning

What's Your Job? (3 of 4)

■ Security Officer

- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct involving PHI by evaluating or recommending the initiation of investigative procedures
- Ensure consistent action is taken for failure to comply with ePHI security policies for all employees on the workforce. Work in cooperation with human resources, administration, and legal counsel, as appropriate

From the Appointment Letter (page 3)

What's Your Job?

- Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance.
- Periodically assess current security compliance status vs. necessary status (gap analysis).
- Work with management, the medical staff, the director of health information management, the Privacy Officer, and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices.
- Develop and/or ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.
- Coordinate or oversee the filing of regulatory forms, reports, etc. Assist other departments in understanding and complying with regulatory requirements. Work with appropriate individuals to ensure facility implements and maintains appropriate security forms, materials, processes, procedures, and practices.
- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.
- Ensures consistent action is taken for failure to comply with security policies for all employees in the workforce. Works in cooperation with human resources, administration, and legal counsel, as appropriate.

From the Appointment Letter (page 4)

What's Your Job?

Education, Training and Communication:

- Provide the facility's information security policies and practices to employees and others with access to health information. Prepare and publish papers/articles on good security practices for the facility's employees and others. Ensure that training conforms to existing policies and procedures.
- Communicate the importance of compliance and the compliance program to senior management, the compliance committee, and health plan staff.
- Work with leadership to provide adequate information to ensure that they and their employees have the requisite information and knowledge of regulatory issues and requirements to carry out their responsibilities in a lawful and ethical manner.
- Provide input and/or direction to the employee performance appraisal and incentive programs to ensure improper conduct is reported and discouraged and that support of and conformity with the compliance program is part of any performance evaluation process for all employees.

Survival Kit

HOME A to Z SEARCH HELP WHAT'S NEW SITE MAP

TMA Privacy Office HIPAA Compliance: Privacy

Home
[Freedom of Information Act \(FOIA\)](#)
[Records Management](#)
[HIPAA Privacy/Security](#)
[Privacy Act of 1974](#)
[System of Records](#)
[Data Use Agreements](#)
[Personnel Security \(ADP Background Checks\)](#)

TRAINING AND TOOLS

The TMA HIPAA program is evolving from implementation to compliance. Are you ready? To support you in your HIPAA compliance efforts, TMA offers training options such as live webcasts and online courses, as well as additional documentation to assist you in the learning process. Our course offerings will be expanded this year to include courses that will focus specifically on compliance efforts. Stay tuned!

Go to Tools

[LMS](#) / [HIPAA BASICS](#) / [PHIMT](#)

Required HIPAA Refresher Training - 2006
Every year, as a requirement of the Department of Health and Human Services (DHHS) HIPAA Privacy and Security Rules, all TMA (including contractors) and MHS workforce members must complete annual HIPAA Refresher Training.

Before accessing the training, please make sure that your system satisfies the following technical requirements

- **Internet Explorer 5.5 or above (do not use Netscape)**
- **Macromedia Flash 6.0 or above (contact [HIPAA Support](#))**
- [click here for support guide](#)
- **Sun Java (contact [HIPAA Support](#))**
- [click here for support guide](#)

Refresher Training can be accessed at hipaatraining.tricare.osd.mil. For detailed instructions on how to take Refresher Training, see the "[Refresher Training Guide](#)".

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

Resource

From the Appointment Letter (page 4)

Are you going to do this all by yourself?

- ◆ Identify potential areas of compliance vulnerability and risk; develop/implement corrective action plans for the resolution of problematic issues and provide guidance on how to avoid or deal with similar situations.
- ◆ Establish and chair the interdisciplinary Medical Information Security Readiness Team. Ensure that that the team includes at least one clinical, one patient administration, and one information technology representative. The team is responsible for coordinating MIF/DIF implementation of HIPAA Security and protecting the confidentiality, integrity and availability of electronic protected health information.
- ◆ Perform internal audit of data access and use to detect and deter breaches.
- ◆ Receive reports of Security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

In the Beginning

Are you going to do this all by yourself?

- HIPAA Security Officer
- HIPAA Privacy Officer
- Medical Information Security Readiness Team (MISRT)
- Senior Executive Staff
- Covered entity workforce
- Physical Security Officer
- System Administrator
- Network Administrator
- Human Resources

- Legal
- Public Relations
- Training
- Information System Security Officer (ISSO)/ Information System Security Manager (ISSM)
- Incident response team:
 - multi-disciplinary team to ensure comprehensive preparation, response, and mitigation to incidents

In the Beginning

Laurel

- All appropriate personnel
 - Consider the MISRT: PAD, clinician, IT Personnel – why?
 - Defense in breadth and depth
 - Increased awareness and communication, decreased response time
- Backfilled responsibilities in case of emergency

Hardy

- HSO + Sys admin
 - Dual hatted
 - Collateral duty
 - Benefit: less money and effort up front
 - Minimum necessary to do the job
- Stays on call while away

From the Appointment Letter (page 4)
**Are you going to do this all by yourself?
Where is PHI? What are the risks?**

- ◆ Identify potential areas of compliance vulnerability and risk; develop/implement corrective action plans for the resolution of problematic issues and provide guidance on how to avoid or deal with similar situations.
- ◆ Establish and chair the interdisciplinary Medical Information Security Readiness Team. Ensure that that the team includes at least one clinical, one patient administration, and one information technology representative. The team is responsible for coordinating MIF/DIF implementation of HIPAA Security and protecting the confidentiality, integrity and availability of electronic protected health information.
- ◆ Perform internal audit of data access and use to detect and deter breaches.
- ◆ Receive reports of Security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

In the Beginning

Managing Your Day

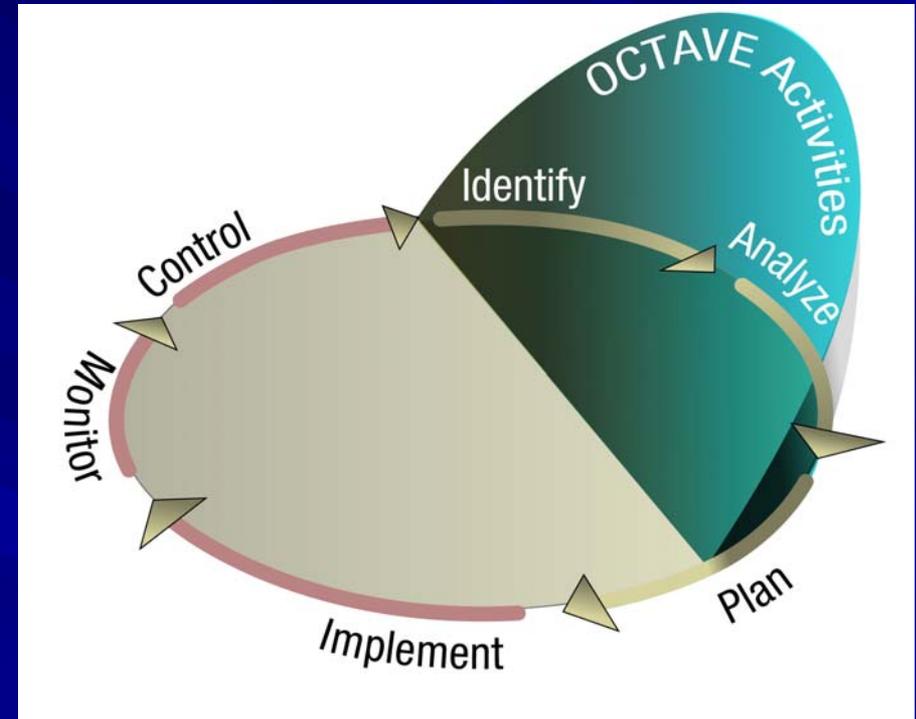
- Risk Management is the process of **identifying, mitigating,** and **monitoring** information system-related risks by applying the appropriate controls
- Risk Management is composed of three parts:



In the Beginning

How Do I Manage Risk? OCTAVESM

- Operationally Critical...OCTAVESM is at the center of a risk management approach to information security.
- Show of hands: how many have conducted an OCTAVESM assessment?



In the Beginning

Who's doing OCTAVESM at your MTF?

- OCTAVESM is a self-directed assessment
- You:
 - are actively involved in the decision-making process
 - manage the assessment process using your expertise
 - reach out to experts as needed
- Do you do this by yourself?

In the Beginning

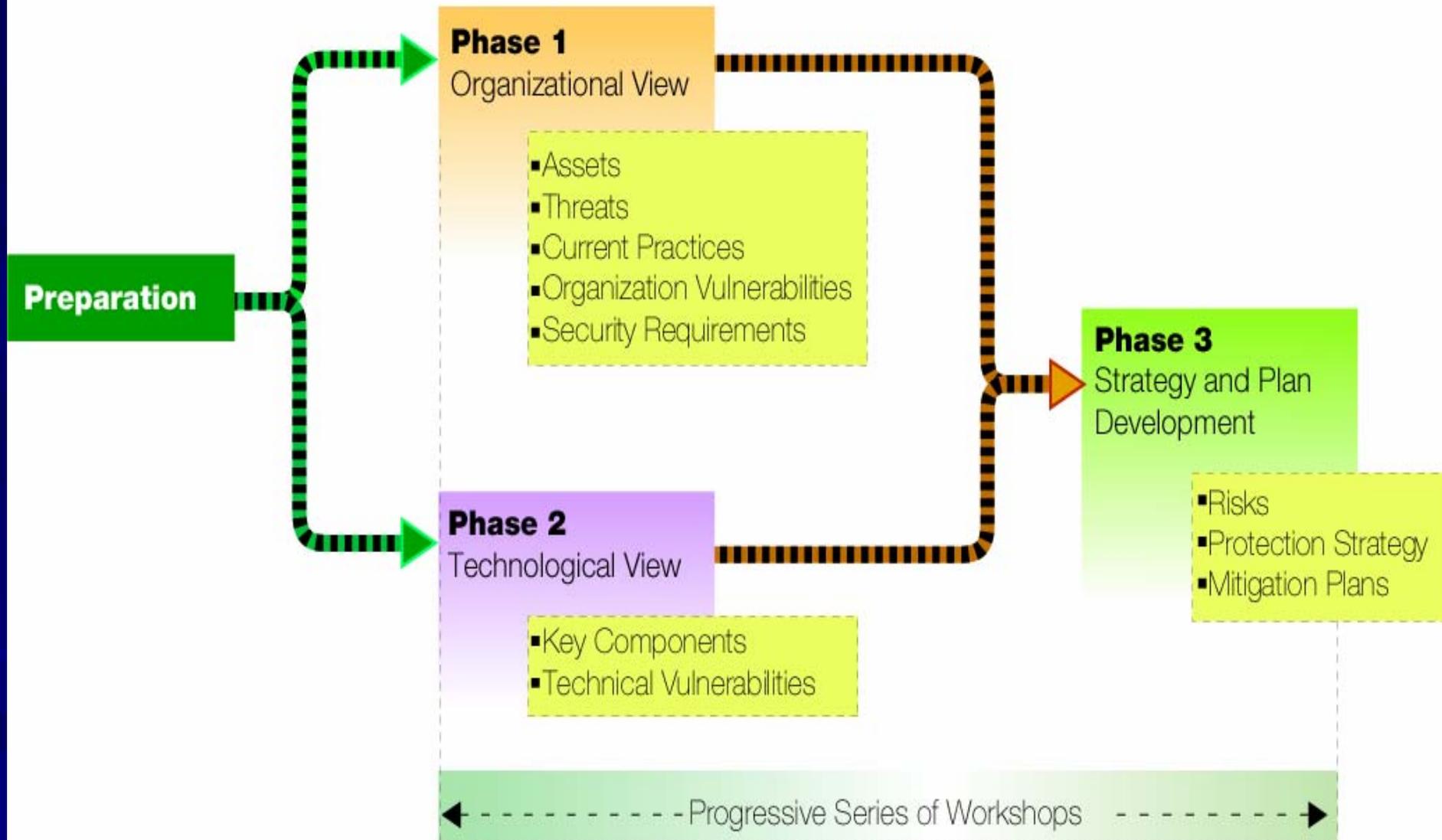
Doing OCTAVESM: Workshop Structure

- *Analysis team* facilitates the workshops
- *Contextual expertise* is provided by the site's staff
- Activities are driven by the site's staff
- Decisions are made by the site's staff

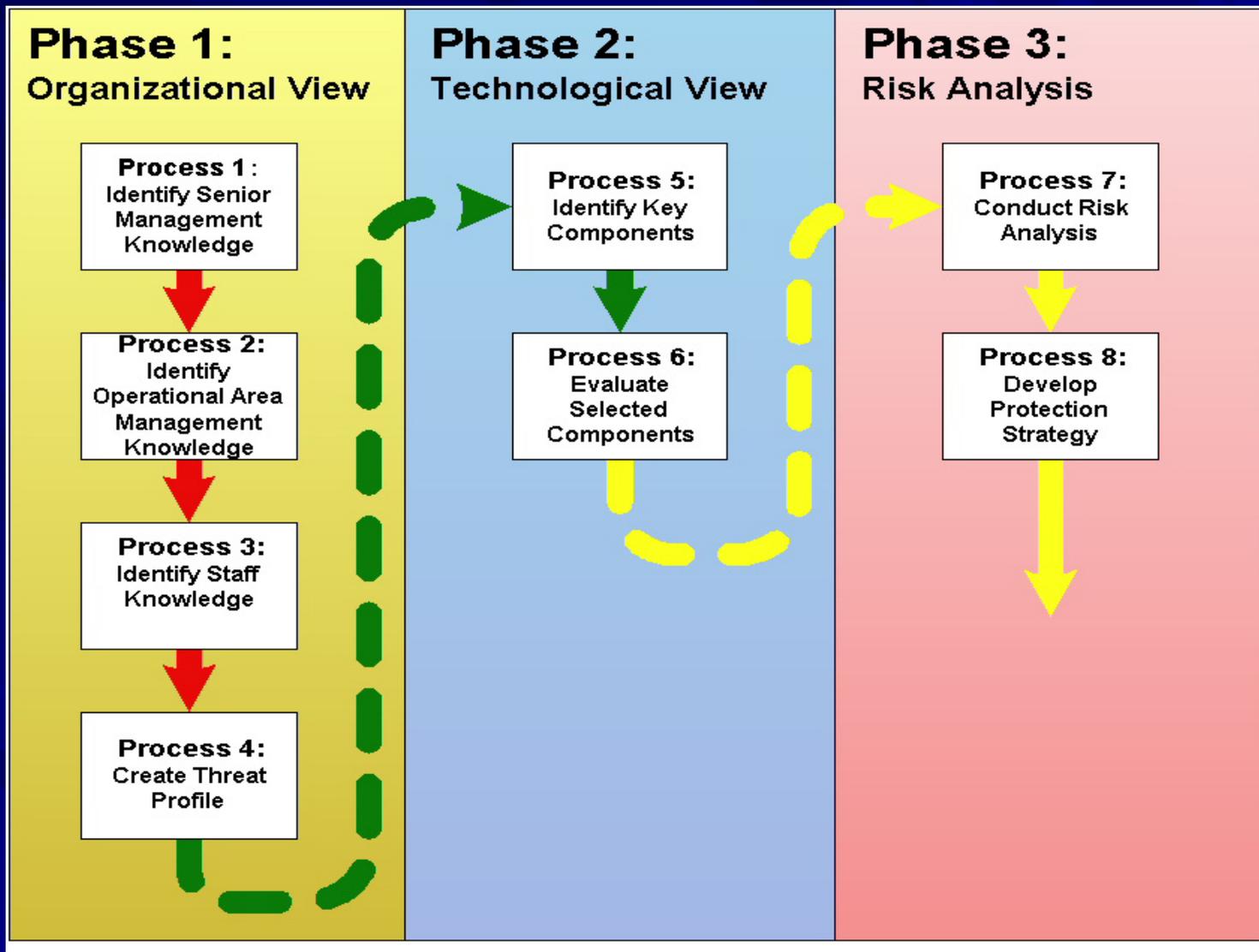
Biomedical devices

- Frequently store Electronic Protected Health Information (ePHI), and therefore, must be considered when implementing a comprehensive IT security program
- Designated and operated as special purpose computers
- More features are being automated and increasing amounts of PHI is being collected, analyzed, and stored
- Growing integration and interconnection of different biomedical devices and IT systems where ePHI is being exchanged

In the Beginning OCTAVESM Process



In the Beginning OCTAVESM Roadmap



From the Appointment Letter (page 3)

Update of policies and procedures following OCTAVESM

Organizational Need/Function: The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires Medical Treatment Facility and Dental Treatment Facility (MTF/DTF) personnel to be assigned the responsibility of managing and supervising the execution and use of security measures to protect data as well as the responsibility of managing and supervising the conduct of personnel in relation to those measures.

ROLES AND RESPONSIBILITIES

Policy Implementation, Oversight, Auditing and Compliance:

- Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule.
- Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassess status and updated security standards established by the facility.

From the Appointment Letter (page 3)

Update of policies and procedures following OCTAVESM

Organizational Need/Function: The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires Medical Treatment Facility and Dental Treatment Facility (MTF/DTF) personnel to be assigned the responsibility of managing and supervising the execution and use of security measures to protect data as well as the responsibility of managing and supervising the conduct of personnel in relation to those measures.

ROLES AND RESPONSIBILITIES

Policy Implementation, Oversight, Auditing and Compliance:

- Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule.
- Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassess status and updated security standards established by the facility.

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-401
1 NOVEMBER 2001



Security

INFORMATION SECURITY PROGRAM
MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://afpubs.hq.af.mil>.

OPR: HQ USAF/XOFI (Deborah Ross)
Supersedes AFI 31-401, 17 September 2001

Certified by: HQ USAF/XOF
(Brig Gen Richard A. Coleman)
Pages: 137
Distribution: F

It contains Air Force (AF) unique guidance needed to supplement Air Force Policy Directive (AFPD) 31-4, *Information Security*; Executive Order (EO) 12958, *Classified National Security Information*, 20 Apr 95; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information*, 13 Oct 95; and, Department of Defense (DOD) 5200.1-R, *Information Security Program*, 17 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, *Damage Assessments*, 23 Dec 91; and, DOD Directive (DODD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*, 15 Nov 91. All these references are listed at the end of each paragraph where applicable. HQ USAF/XOF is delegated approval authority for revisions to this AFI.

SUMMARY OF REVISIONS

This change is necessary to incorporate IC 2000-1 and 2000-2 which were inadvertently deleted when the last revision incorporated IC 2001-1. This revision incorporates Interim Change IC 2001-1. This change updates the table of contents to reflect new attachments for Original Classification Authorities, an Appointment of Inquiry Official Memorandum, and a Preliminary Inquiry of Security Incident Report; updates the office of primary responsibility for this Air Force Instruction (AFI); clarifies Standard Form (SF) 311, *Agency Information Security Program Data*, reporting requirements; clarifies authority for nuclear weapon security classification policy and how to obtain the policy; adds guidance for commanders and/or staff agency chiefs to process administrative sanctions; adds the requirement for HQ USAF/XOFI to conduct program reviews; completely replaces **Chapter 9**, Actual or Potential Compromise of Classified Information, to implement additional reporting and investigative procedures concerning security incidents; implements automatic declassification extensions; incorporates guidance on systematic declassification reviews; clarifies safeguarding requirements for secure rooms; and, updates handcarrying

In the Beginning

Laurel

- Why OCTAVESM?
 - More than Risk Analysis
 - Complete RM process
 - Supported, intellectual capital,
 - Designed to be used at MTFs
 - Progress: automated tool, OIC, RIMR
 - Centralized DB for trending and analysis

Hardy

- Why not OCTAVESM?
 - Local solution
 - Faster
 - Too complex
 - Pool of resources is limited

In the Beginning

Laurel

■ Risk Analysis?

- First Implementation Specification of HIPAA Security Rule – there's a reason for that!
- Tailors the amount and type of protection to your environment → cost-effective!

■ Considerations

- Biomedical Devices, CDs
- Not organizationally focused
 - does not talk to staff

Hardy

■ Without Risk Analysis

- DITSCAP already covers most of risk analysis required by HIPAA Security
- Centrally managed systems
- Network

When It Hits the Fan

What is an Incident? Black and White

■ Incident:

- “The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”

■ Information System:

- “An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.”

What is Compromised PHI? Not Exactly Black and White

- How does DoD define a “compromise”? Lost, stolen, compromised...
 - Required response depends on the definition.
- Examples:
 - Fax referral to wrong provider. MTF retrieves fax containing PHI
 - PHI thrown into garbage can, and retrieved *in time*?
- Latest definition:
Lost, Stolen, or Compromised Information. “Actual or possible unauthorized disclosure of personal information either to known or unknown persons whether or not a potential exists that the information may be used for unlawful purposes to the detriment of the individual.”

From the Appointment Letter (page 3)

Best defense is a good offense

- Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance.
- Periodically assess current security compliance status vs. necessary status (gap analysis).
- Work with management, the medical staff, the director of health information management, the Privacy Officer, and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices.
- Develop and/or ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.
- Coordinate or oversee the filing of regulatory forms, reports, etc. Assist other departments in understanding and complying with regulatory requirements. Work with appropriate individuals to ensure facility implements and maintains appropriate security forms, materials, processes, procedures, and practices.
- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.
- Ensures consistent action is taken for failure to comply with security policies for all employees in the workforce. Works in cooperation with human resources, administration, and legal counsel, as appropriate.

From the Appointment Letter (page 4)

Best defense is a good offense

- ◆ Identify potential areas of compliance vulnerability and risk; develop/implement corrective action plans for the resolution of problematic issues and provide guidance on how to avoid or deal with similar situations.
- ◆ Establish and chair the interdisciplinary Medical Information Security Readiness Team. Ensure that that the team includes at least one clinical, one patient administration, and one information technology representative. The team is responsible for coordinating MTF/DTF implementation of HIPAA Security and protecting the confidentiality, integrity and availability of electronic protected health information.
- ◆ Perform internal audit of data access and use to detect and deter breaches.
- ◆ Receive reports of Security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

When It Hits the Fan

Are All Incidents Created Equally?

- No standardized set of categories will apply to everyone
- Service specific criteria
- Categories based on risk assessment
- Critical systems versus general support systems
- Must be determined with the interdisciplinary team

From the Appointment Letter (page 3)

Detection

- Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance.
- Periodically assess current security compliance status vs. necessary status (gap analysis).
- Work with management, the medical staff, the director of health information management, the Privacy Officer, and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices.
- Develop and/or ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.
- Coordinate or oversee the filing of regulatory forms, reports, etc. Assist other departments in understanding and complying with regulatory requirements. Work with appropriate individuals to ensure facility implements and maintains appropriate security forms, materials, processes, procedures, and practices.
- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.
- Ensures consistent action is taken for failure to comply with security policies for all employees in the workforce. Works in cooperation with human resources, administration, and legal counsel, as appropriate.

From the Appointment Letter (page 4)

Detection

- ◆ Identify potential areas of compliance vulnerability and risk; develop/implement corrective action plans for the resolution of problematic issues and provide guidance on how to avoid or deal with similar situations.
- ◆ Establish and chair the interdisciplinary Medical Information Security Readiness Team. Ensure that that the team includes at least one clinical, one patient administration, and one information technology representative. The team is responsible for coordinating MTF/DTF implementation of HIPAA Security and protecting the confidentiality, integrity and availability of electronic protected health information.
- ◆ Perform internal audit of data access and use to detect and deter breaches.
- ◆ Receive reports of Security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

How Do You Know When an Incident Happens?

- Complaints
 - Received by you, Service, TMA, or HHS that
 - Reveal deficiency/inadequacy in compliance processes or products, based on
 - Investigation
- Audit/Activity log analysis
- Internal detection/review
- CNN

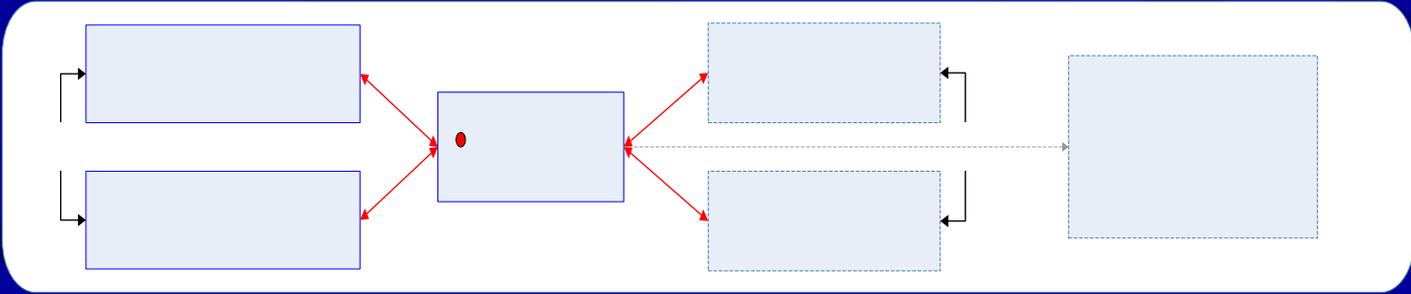
What's The First Thing You Should Do in Response to an Incident?

- Notify beneficiaries?
- Notify chain of command
- Rely on formal, documented procedures – an incident response plan
- Document everything!
- Identify the type, severity, and impact
 - If “critical”, stop the cause. How?
- Activate your response team
 - Comprised of whom?

Survival Kit

- Information Assurance Manager (IAM)/Information Assurance Officer (IAO)
- Network Administrator
- Commander
- HPO
- MISRT

- TMA Privacy Office
- Who else?
- Consider Backups, phone numbers, e-mails, etc.
- Chief Information Officer (CIO)



Resource

When It Hits the Fan

Laurel

- People aware of his/her assignment and responsibilities and contact info
- Checking of logs, trending analysis
- Fully trained on incident response plan
- Has coffee with HIPAA Privacy Officer regularly

Hardy

- Is notified if there is an outstanding problem or concern, several days after logged at helpdesk
- Make use of incident response plan produced for previous JCAHO inspection
- Call in all staff to assist - erring on side of caution
- Need some redundancy

From the Appointment Letter (page 3)

Incident response

- Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance.
- Periodically assess current security compliance status vs. necessary status (gap analysis).
- Work with management, the medical staff, the director of health information management, the Privacy Officer, and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices.
- Develop and/or ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct.
- Coordinate or oversee the filing of regulatory forms, reports, etc. Assist other departments in understanding and complying with regulatory requirements. Work with appropriate individuals to ensure facility implements and maintains appropriate security forms, materials, processes, procedures, and practices.
- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.
- Ensures consistent action is taken for failure to comply with security policies for all employees in the workforce. Works in cooperation with human resources, administration, and legal counsel, as appropriate.

When It Hits the Fan

Managing the Incident

- Mitigation is one of the “new” requirements, requiring special focus
- Multi Services with varying policies, processes, practices
- What happens when an incident affects more than one Service?
 - How many of you have clinics that branch off of your Hospital?
 - How many of you receive your CHCS / AHLTA from a different Services’ host server?
 - Do you treat only personnel members of your Service?
- POINT: Who takes the lead and coordinates response in light of varying response protocols?

When It Hits the Fan

When / How Do I Notify a Beneficiary?

- No longer than 10 days following incident, notify affected individuals
 - DoD Memorandum on Notification
 - NOTE: **some** notification must happen within the required time
- Recall the grey definition of compromised information
- You've already contacted chain of command:
 - Have you called Legal?
 - Is this your decision? Not likely
 - Informed decision must be made
 - Public Affairs



JUL 15 2005



MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF DEFENSE FIELD ACTIVITIES

SUBJECT: Notifying Individuals When Personal Information is Lost, Stolen, or
Compromised

This directive-type memorandum establishes a new Department of Defense policy. Whenever a DoD Component becomes aware that protected personal information pertaining to a Service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, or another individual affiliated with the DoD Component (e.g., volunteer) has been lost, stolen, or compromised, the DoD Component shall inform the affected individuals as soon as possible, but not later than ten days after the loss or compromise of protected personal information is discovered. At a minimum, the DoD Component shall advise individuals of what specific data was involved; the circumstances surrounding the loss, theft, or compromise; and what protective actions the individual can take. If the DoD Component can not readily identify the affected individuals, the DoD Component shall provide a generalized notice to the potentially affected population.

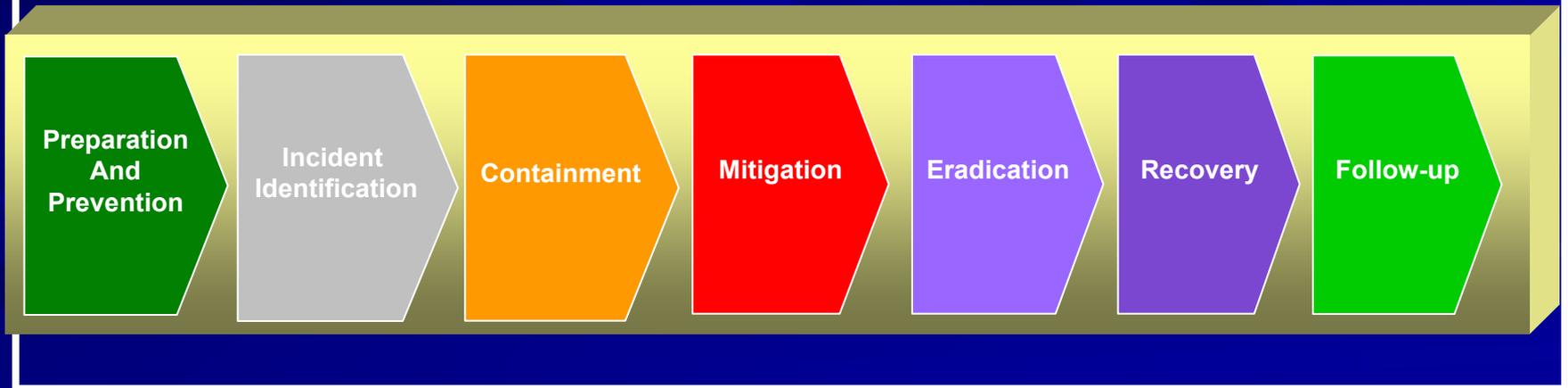
If a DoD Component is unable to comply with the notification requirements of this policy, the DoD Component shall inform me immediately of the reasons why notice was not provided to the affected individuals or population that their personal information has been lost, stolen, or compromised (e.g., delayed notification at request of law enforcement authorities).

This policy shall be made applicable to DoD contractors who collect, maintain, use, or disseminate protected personal information on behalf of a DoD Component.

When It Hits the Fan

At The Same Time, You Have to Respond to The Incident

- Assignment of Responsibility
- Mitigation
- Test and Evaluation
- Most of this will be done by other people...unless you are the other people



When It Hits the Fan

Laurel

- Participated in incident response exercises and tests
- Stopped the bleeding
- Clearly accepts or supports the incident manager responsibility
- Coordination and communication across roles
- Accurate and timely triage to determine course of actions

Knows what to do and when!

Hardy

- Incident response plan:
 - Searches for one in response to an incident
 - Utilizes more than one plan
 - Uses the plan of the compromised system
- Assumes responsibility
- Documents response activities after a week of putting out fires
- Includes incident in monthly status report

Business As Usual?

From the Appointment Letter (page 4)

Communication

Education, Training and Communication:

- Provide the facility's information security policies and practices to employees and others with access to health information. Prepare and publish papers/articles on good security practices for the facility's employees and others. Ensure that training conforms to existing policies and procedures.
- Communicate the importance of compliance and the compliance program to senior management, the compliance committee, and health plan staff.
- Work with leadership to provide adequate information to ensure that they and their employees have the requisite information and knowledge of regulatory issues and requirements to carry out their responsibilities in a lawful and ethical manner.
- Provide input and/or direction to the employee performance appraisal and incentive programs to ensure improper conduct is reported and discouraged and that support of and conformity with the compliance program is part of any performance evaluation process for all employees.

Business As Usual

Who Needs to Know About an Incident?

- What is considered “timely dissemination of information” for Incident reporting?
- Do you have a communications strategy?
- Does it include methods for both notifying and updating individuals?
- Do you include the appropriate people from all levels of the organization?
- Are you part of a multi-Service market?
 - How do you interface with the other Services?

Business As Usual

When Does TMA Need to Know?

- Is CNN calling you for interviews? Do you want that interview?
- What do you tell your providers when they can not access patient information? E.g., lab results, meds, corruption of database, etc.
- What do you tell your patients when referrals can not be sent out?
- How does the pharmacy process drug interaction checks?
- What if your supply department can not process orders?
- Can you handle a temporary loss of financial processing?

What About Attempted Incidents?

- Why do you care? Should you care?
 - Unsuccessful today, may be successful tomorrow
 - Unsuccessful at your MTF, may be successful at another

- Things to consider:
 - Patterns
 - Severity level
 - Sources / targets
 - Previously unidentified risks

From the Appointment Letter (page 4)

Evaluation and Improvement of the program

MITF Integration Activities:

- In coordination with key personnel, develop and implement the following plans and others as required:
 - Disaster plan, emergency mode operation plan, backup plan, physical security plan, personnel security plan, access policies, and others. Test and revise plans as necessary to ensure data integrity, confidentiality, and availability.
- Function as key representative/liaison in meetings regarding regulatory policy.

From the Appointment Letter (page 4)

Evaluation and improvement of personnel

Education, Training and Communication:

- Provide the facility's information security policies and practices to employees and others with access to health information. Prepare and publish papers/articles on good security practices for the facility's employees and others. Ensure that training conforms to existing policies and procedures.
- Communicate the importance of compliance and the compliance program to senior management, the compliance committee, and health plan staff.
- Work with leadership to provide adequate information to ensure that they and their employees have the requisite information and knowledge of regulatory issues and requirements to carry out their responsibilities in a lawful and ethical manner.
- Provide input and/or direction to the employee performance appraisal and incentive programs to ensure improper conduct is reported and discouraged and that support of and conformity with the compliance program is part of any performance evaluation process for all employees.

Follow-up Activities (1 of 2)

- Follow-up is a critical step in the security incident response process because it assists with the response to, and prevention of, future incidents
 - 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 ePHI security incident and to measure the effectiveness of response procedures. Provide this information to all appropriate individuals within the organization

Business As Usual

Follow-up Activities (2 of 2)

- Based on the lessons learned, generate recommendations that can assist with the response to, and prevention of, future incidents
 - Make improvements/modifications to ePHI security incident response procedures, and test as necessary
 - Follow existing local and higher authority guidance regarding any additional security incident follow-up requirements
- **Sharing Information**
- Sanitized lessons learned documentation
 - Share lessons learned with other MHS Components
 - Require an out-brief of effectiveness of response and improvement activities with required timeframe

Business As Usual

Laurel

- Identifies all affected parties
- Notifies all appropriate personnel. Conducts and confirms timely notification
- Conducts thorough investigation
- Identifies additional risks and updates health information risk management plan
- Updates and conducts local training and awareness
- Documents entire process and holds lessons learned with local staff and management

Hardy

- Concentrates resources and attention to the immediate fires. No foul, no harm
- Takes initiative to inform management
- Gathers local staff to discuss high impact attempted incident
- Sends email with details of incident to local staff and Base Command

A Tale of Two HIPAA Security Officers

Presentation Summary

- Now You Should Know...
 - How to find the potential HIPAA risks in daily activities
 - How to avoid possible hurdles associated with handling an incident
 - How to properly manage an incident

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- DoD 8580.X-R, DoD Health Information Security Regulation (Draft)
- <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
- <https://hipaasupport.tricare.osd.mil> for tool related questions
- Privacymail@tma.osd.mil for subject matter questions
- Service HIPAA Representatives



HEALTH AFFAIRS



TRICARE
Management
Activity

Please fill out your
critique
Thanks!

