Veterans Health Administration

STAYING AHEAD OF THE GAME: HIPAA Audit and Implementation Monitoring at the Largest Integrated Health System

Lydia Duckworth, CISSP

Reba White

HIPAA Program Management Office

Veterans Health Administration

Washington, DC

April 10, 2006

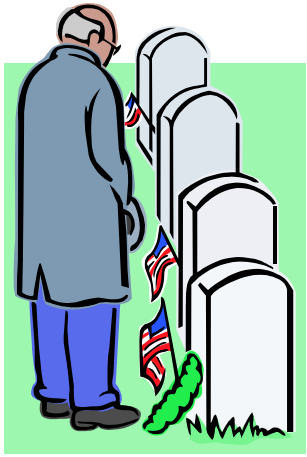
Agenda

- About VA and VHA
- HIPAA Security and Privacy Compliance in a Government Agency
  - Considerations and HIPAA Implications
  - Compliance Strategies
- Privacy Rule
  - Privacy Rule Vs. VHA Privacy Policy
  - VHA Privacy Initiatives
    - Assessment Tools
  - Complaint resolution
- Security Rule
  - Definitions and Requirements
  - Implementation and Compliance
  - Assessment and Policies and Procedures Tools
  - Findings
  - Complaint Resolution
- Tips
- Questions?

VA's Organizations

VA – The Department of Veterans Affairs (parent organization)

VHA – Veterans Health Administration (health care components of VA)



VBA – Veterans Benefits Administration (Determines veterans benefits and administers non-medical benefits) –VA Loans, Education, etc.

NCA – National Cemetery Administration (Manages national cemeteries and burial benefits)

VA's Organizations

VA – The Department of Veterans Affairs

- Centralized Security Program – VA Office of Cyber and Information Security

- Decentralized Privacy Program – Both the VA and VHA have Privacy Programs that work collaboratively

VA/VHA Background

- Veterans Health Administration (VHA)
  - Nation's largest integrated health system
  - Operates more than 1300 points of care nationwide
  - Submits health care reimbursement claims to 1600+ payers
  - VHA and VA Medical Centers (VAMC) serve a single covered entity
    - Primary Role: providing health care to veterans
      - VAMCs (Veterans Affairs Medical Centers)
      - CBOCs (Community Based Outpatient Clinics)
      - Provider programs
    - VHA also operates as traditional health plan
      - HAC (Health Administration Center)
      - Fee Basis

HIPAA Security and Privacy Compliance in a Government Agency

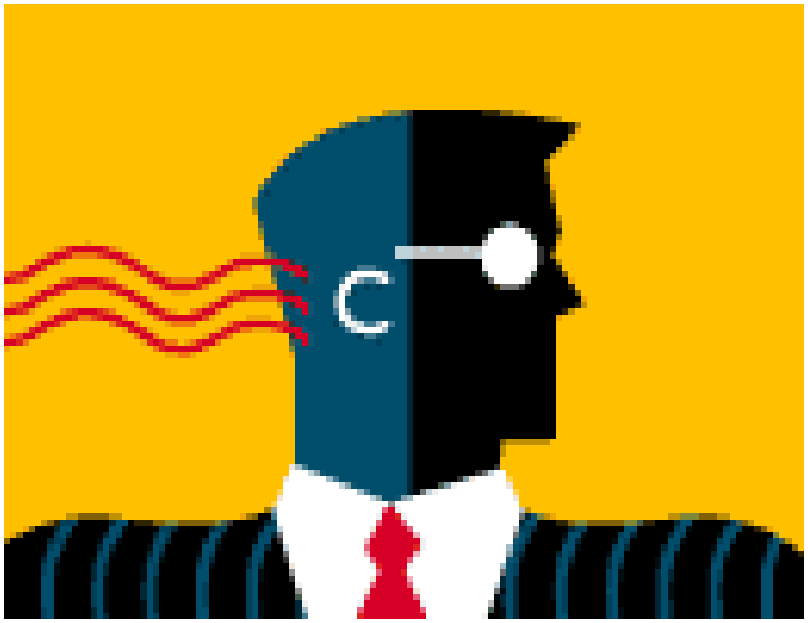
Primary Business Models:

- VHA Chief Business Office (CBO)
  - HIPAA Program Management Office (PMO)
    - Responsible for VHA's compliance across all components of HIPAA, Title II, Administrative Simplification
    - Works with VA OCIS, VA Enterprise Privacy Program, VHA Privacy Office, VA Office of Information, and other programs across the organization to fulfill compliance requirements

Role of the HIPAA Program Management Office

- The major communications and information forum for HIPAA; coordinates VHA's efforts with the Department
- Represents VHA at national conferences and forums
- Clearinghouse for FAQs, best practices, and cross-service Privacy and Security initiatives
- Catalyst for ensuring that HIPAA compliance strategies are implemented across multiple programs and services, including Research
- Single Point of Contact for Department of Health and Human Services (HHS), Office for Civil Rights (OCR) HIPAA Complaints

The HIPAA Privacy Rule



VHA and Privacy

- VHA Privacy Policy is not identical to the HIPAA Privacy Rule: VHA policy is more restrictive and is built on six federal statutes:
  - The Freedom of Information Act (FOIA), 5 U.S.C. 552
  - The Privacy Act (PA), 5 U.S.C. 552a
  - The VA Claims Confidentiality Statute, 38 U.S.C. 5701
  - Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection With the Human Immunodeficiency Virus (HIV), and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332
  - The Health Insurance Portability and Accountability Act (HIPAA)
  - Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705

VHA Privacy Compliance

- VHA Compliance with Privacy Rule in April 2003
  - On-site Assessments
  - Self Assessment Tool for Facilities
    - Policy and Procedure Questionnaire
    - Interactive Self Assessment web site (in development)
  - Release of Policy and Procedure Templates
  - Privacy Tool Kit

VHA and Privacy Office Joint Efforts
High-Level Assessment Process

- Assess
- Measure Objectives
- Conduct Physical Walkthrough
- Develop Report
- Report Back to Facility Leadership
- Provide a Mitigation Strategy and Tools with which to Remediate
- Allow 90-day timeline for remediation

Privacy Assessment Tools

Assessment tool

- Policy and procedure questionnaire.
- Privacy process questionnaire – review consistency and appropriateness of privacy activities
- Conduct a physical walk-through of the facility evaluating current Privacy practices, policies, and procedures.

Comment: Most facilities follow Privacy regulations, but many are lacking documentation of their policies and procedures.

Joint Efforts – Privacy Assessment Activities

On-site Activities:

- Review the facilities' uses and disclosures of individually identifiable information.
- Audit facility compliance with the applicable privacy statutes, including HIPAA, the Privacy Act, and Title 38 regulations.
- Review administrative safeguards for all related areas in which individually identifiable information is used, processed, disclosed, stored, or destroyed.
- Ensure that appropriate privacy policies and procedures are in place, current, and consistent with VA/VHA-wide privacy directives, specifically VHA Directive and Handbook 1605.1.

Self Assessment Tool for Facilities

The web-based self assessment tool that is in development will allow facilities to:

- Complete a compliance assessment and determine baseline compliance levels
- Analyze risks and prioritize identified issues that will need to be mitigated
- Collect and aggregate data related to the effectiveness of their current privacy program
- Use assessment results to identify best practices and steps for improving compliance

Additional Privacy Initiatives

- Enforcement of Minimum Necessary Standard
- Facility Directory and Opt-Out Policies
- Business Associate Agreements – enterprise and national level
  - Established business process for business associate agreements and created template agreements for use at the national and local levels
  - Developed directive and handbook governing requirements for BAA's and the business process
  - Monitors business associate status

Additional Privacy Initiatives

- Privacy and Release of Information Policy
  - Documents VHA privacy and ROI policy
- Release of Information Software
- Updated research policies and procedures
- Implemented complaint tracking process

Privacy Initiatives, continued

HIPAA Training & Awareness

- Training is composed of three modules:
  - Introduction to HIPAA
  - Major Components of the Privacy Rule
  - Ensuring HIPAA Compliance
- General VHA Privacy Policy Training
  - Developed specifically for VHA
  - VHA Privacy Officer Training – focuses on providing facility Privacy Officers with a broad understanding and acute awareness of the requirements of the HIPAA Privacy Rule

Complaint Resolution

- The VHA HIPAA PMO serves as the single point of contact for HHS/OCR regarding HIPAA Complaint Resolution
- The HHS Office for Civil Rights (OCR) provides privacy complaint notification to the HIPAA PMO and sends a Privacy Violation Notification for each complaint.
- The VHA HIPAA PMO collaborates with:
  - VHA Privacy Office;
  - VAMC Medical Director and Privacy Officer;
  - the Enterprise Privacy Program; and
  - VA Office of General Counsel in assessing and responding to privacy complaint notifications.

Handling OCR Complaints

- Created secure Intranet-based web solution to store, document, and resolve privacy complaints
- Privacy officers work directly with Information Security offices to conduct investigations
- Interviews are conducted with relevant staff members
- Remediation is integral to complaint resolution

The HIPAA Security Rule

About the Security Rule

- Covers information in electronic form only -- Electronic Protected Health Information (ePHI)
- HIPAA is similar in requirements and scope to the Federal Information Security Management Act of 2002 (FISMA).
- Covered entities may use any security measures available to reasonably and appropriately implement the standards of the rule.

Managing Security Compliance

- Asking the right questions:
  - where is it stored (systems, applications, devices)
  - who owns the data (systems owners, IRM, ?)
  - where and how is the data transmitted
  - what is the impact to the organization if resources are not appropriately protected
  - use the rule as a tool to facilitate the organization's physical and technical security posture, not as a tool to encumber business processes

The Security Assessment

- Assist the facilities in compliance and remediation activities
- Generate a baseline of problematic areas for trending and project initiatives
- Look at facilities holistically in terms of strengths and weaknesses
- Identify best-practices, as well as local policies and procedures that can be leveraged and used by other facilities

On-site Assessment Process

- Complete a multipart self-assessment survey of facility in order to determine the appropriateness of facility practices specific to HIPAA Security Rule compliance
- Document the security posture of the facility

- Review all facility policies and procedures for completeness and applicability to the HIPAA Security Rule
  - This review is conducted in a group forum to include system administrators, health information managers, human resources, security, law enforcement, chief information officer, etc

- Physical security walkthrough

The Process

- The following personnel are recommended to participate:
  - Cyber Security Practitioner
  - Chief Information Officer
  - Facility Director
  - Compliance Officer
  - Privacy Officer
  - IRM Manager
  - HIMS Manager
  - HIPAA Implementation Coordinator
  - Contracting Officer
  - Chief of Law Enforcement

The Process: Day Two

Policy and Procedure Review:

Purpose—understand how the facility manages its security program and what activities we can anticipate from workforce members

Sample question:

1.1 Does the facility have an on-going risk management process for identifying, controlling, and mitigating information system-related risk including confidentiality, availability, and integrity (this includes both paper and automated systems)?

Yes

No

Do Not Know

Implementation Specification

(B) Risk management (Required).
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Sample Question 2

Sample question

2.1 Has your facility established a business continuity plan to enable continuation of critical business processes while operating in emergency mode? Check all applicable below:

2.1(a) Developed

2.1(b) Implemented

2.1(c) Tested

2.1(d) Updated

Implementation Specification:

(C) Emergency mode operation plan (Required).

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Findings – The Hot Spots

Assessments have revealed weaknesses in facility security programs related to policies, procedures, and processes.

- Specifics:
  - Procedures may be carried out, but they are often not documented
  - Auditing
  - Wireless
  - Data back-ups
  - Device and media controls (i.e. PDAs, Blackberrys, laptops, thumbdrives, CDs, DVDs)
  - E-mail

Sanctions and Complaints

- If one or more members of the workforce fail to comply with the security policies and procedures, and/or the security standards, appropriate actions toward resolution, including sanctions, will be taken.

- All identified security complaints lodged against the VHA and its facilities, whether from CMS/Office of E-Health Standards and Services or from local sources, will be investigated.

- VHA HIPAA PMO works directly with Information Security Officer to investigate, document, and mitigate or remediate complaints.

Continued Compliance Management

- Hold monthly calls – HIPAA Implementation Team calls
- Update templated policies and procedures to conform to new requirements, technologies, and business processes
- Monitor the security and privacy programs for quality improvement.
- Make tools available for self-assessment
  - Get participation in the assessment from appropriate facility personnel.

General Plan for Compliance

- Institute ongoing long-term processes
- Continue to define and refine HIPAA compliance best practices and provide guidance to VHA facilities on how to reach these goals across the enterprise
- Implement other components of HIPAA as they are finalized and released
- Manage and monitor changes and additions to the HIPAA legislation

Contact Information

Lydia Duckworth Security	lydia.duckworth@va.gov	202-254-0353
Reba White Privacy	reba.white@va.gov	202-254-0391
VHA HIPAA PMO	hipaa.pmo@va.gov http://vaww1.va.gov/cbo/hipaa.html	202-254-0385
Barbara Mayerick Director of Business Development	barbara.mayerick@va.gov	202-273-0339

Questions


QUALITY
CHIEF BUSINESS OFFICE
SIMPLICITY
VALUE
MEMBER SERVICES
REVENUE OPERATIONS
MANAGED CARE
VETERANS HEALTH ADMINISTRATION
ACCOUNTABILITY
CONSISTENCY
Putting Business to Work for America's Veterans