

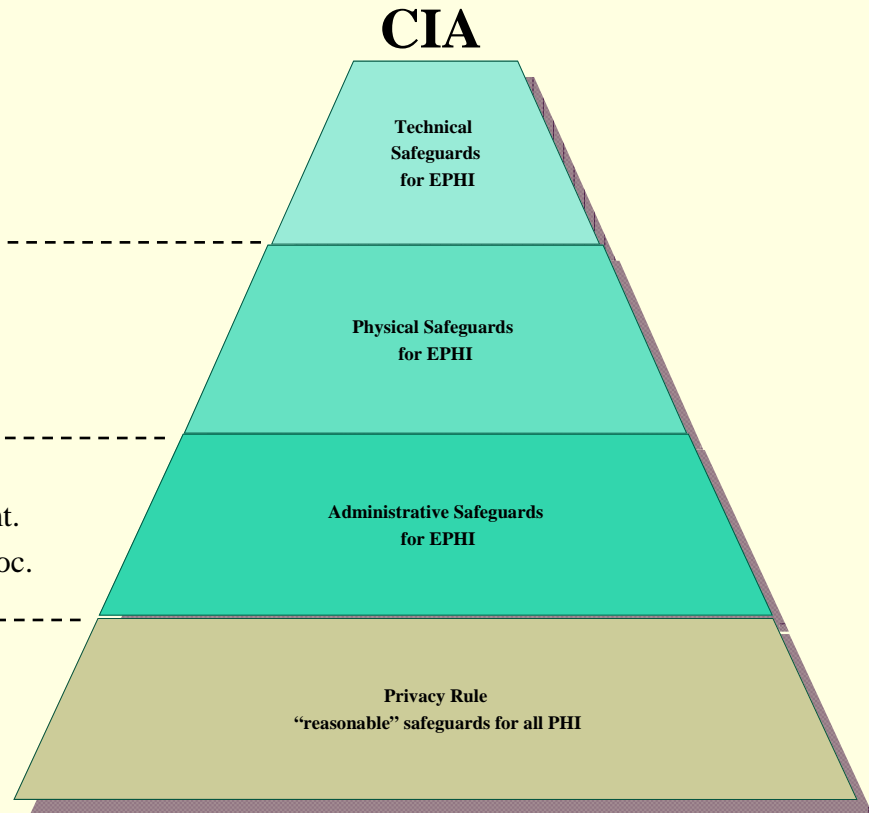
Preparing for a HIPAA Security Audit

Ali Pabrai, CISSP, CSCS
ecfirst, chairman & ceo



HIPAA Requirements

- Access Control
 - Audit Control
 - Integrity
 - Person or Entity Authentication
 - Transmission Security
-
- Facility Access Controls
 - Workstation Use
 - Workstation Security
 - Device & Media Controls
-
- Security Mgmt. Process, Sec. Officer
 - Workforce Security, Info. Access Mgmt.
 - Security Training, Security Incident Proc.
 - Contingency Plan, Evaluation, BACs



Healthcare Technology Challenges

State of the Infrastructure

- Too many servers, too many applications
- Too many credentials across multiple systems to manage
- Lack of expertise, resource availability to audit capabilities to track credential access
- Too many PCs to maintain and manage
- Mobility of devices is rapidly increasing
- Storage demands are increasing fast
- Highly specialized technical skills required
- Serious lack of redundancy



HIPAA Audit

People That May Be Interviewed

- President, CEO or Director
- HIPAA Compliance Officer
- Lead Systems Manager or Director
- Systems Security Officer
- Lead Network Engineer and/or individuals responsible for:
 - Administration of systems which store, transmit, or access EPHI
 - Administration of systems, networks (wired and wireless)
 - Monitoring of systems which store, transmit, or access EPHI
 - Monitoring systems networks
- Computer Hardware Specialist
- Disaster Recovery Specialist or person in charge of data backup
- Facility Access Control Coordinator (physical security)
- Human Resources Representative
- Director of Training
- Incident Response Team Leader
- Others as identified

HIPAA Audit

Documentation That May Be Requested

Policies and procedures that address:

- Prevention, detection, containment, and correction of security violations
- Employee background checks and confidentiality agreements
- Establishing user access for new and existing employees
- List of authentication methods used to identify users authorized to access EPHI
- List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
- List of software used to manage and control access to the Internet
- Detecting, reporting, and responding to security incidents
- Physical security
- Encryption and decryption of EPHI
- Mechanisms to ensure integrity of data during transmission - including portable media transmission

HIPAA Audit

Documentation That May Be Requested

Policies and procedures that address (contd.):

- Monitoring systems use - authorized and unauthorized
- Use of wireless networks
- Granting, approving, and monitoring systems access (for example, by level, role, and job function)
- Sanctions for workforce members in violation of policies and procedures governing EPHI access or use
- Termination of systems access
- Session termination policies and procedures for inactive computer systems
- Policies and procedures for emergency access to electronic information systems
- Password management policies and procedures
- Disposal of media and devices containing EPHI
- Secure workstation use

HIPAA Audit

Other Documentation That May Be Requested

- Entity-wide Security Plan
- Risk Analysis (most recent)
- Risk Management Plan (addressing risks identified in the Risk Analysis)
- Security violation monitoring reports
- Vulnerability scanning plans
 - Results from most recent vulnerability scan
- Network penetration testing policy and procedure
 - Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)
- Configuration standards to include patch management for systems which store, transmit, or access EPHI (including workstations)
- Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI

HIPAA Audit

Other Documentation That May Be Requested

- Organization chart to include staff members responsible for general HIPAA compliance to include the protection of EPHI
- Examples of training courses or communications delivered to staff members to ensure awareness and understanding of EPHI policies and procedures
- Policies and procedures governing the use of virus protection software
- Data backup procedures
- Disaster recovery plan
- Disaster recovery test plans and results
- Analysis of information systems, applications, and data groups according to their criticality and sensitivity
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain EPHI
- List of all Primary Domain Controllers (PDC) and servers
- Inventory log recording the owner and movement of media and devices that contain EPHI

Typical Security Initiatives

Emerging Best Practices

- Harden Firewall Solutions, IDS/IPS
- Secure Facilities & Server Systems
- Implement Identity Management Systems
 - Deploy Single Sign-On (SSO) Solution
 - Activate Auditing Capabilities to Manage/Track Access
- Schedule regular scans of the infrastructure
- Deploy Integrity Controls and Encryption
- Develop Contingency Plans
- Conduct Security Training & Awareness
- Update Security Policies

Getting Started...



About ecfirst



- Provider of compliance, cyber security and IT professional services
 - Managed Compliance Services Program (MCSP) for HIPAA
 - AuditShield™ service launched to support client audit efforts
 - BIA and Disaster Recovery Plan (DRP) development
 - Annual Risk Analysis and Quarterly Vulnerability Assessments
- Recognition
 - Achieved **Inc. 500** status in 2004
 - Exclusively endorsed by the American Hospital Association (AHA)
- Innovation: Launched *Certified Security Compliance Specialist™* (CSCS™) program addressing PCI, ISO, SOX, HIPAA and international security regulations
- 1400+ customers worldwide – www.ecfirst.com



Thank You!

- Join me, May 20th, *Realizing HIPAA Compliance for Credential Management Through SSO* – register at www.ecfirst.com
- Ali Pabrai, CISSP, CSCS
 - 949.260.2030
 - pabrai@ecfirst.com