AHIMA Distance Education
Career-building Resources

HIPAA Security: What Everyone Should Know

Webinar

January 17, 2008

Practical Tools for Seminar Learning

Disclaimer

The American Health Information Management Association makes no representation or guarantee with respect to the contents herein and specifically disclaims any implied guarantee of suitability for any specific purpose. AHIMA has no liability or responsibility to any person or entity with respect to any loss or damage caused by the use of this audio seminar, including but not limited to any loss of revenue, interruption of service, loss of business, or indirect damages resulting from the use of this program. AHIMA makes no guarantee that the use of this program will prevent differences of opinion or disputes with Medicare or other third party payers as to the amount that will be paid to providers of service.

As a provider of continuing education the American Health Information Management Association (AHIMA) must assure balance, independence, objectivity and scientific rigor in all of its endeavors. AHIMA is solely responsible for control of program objectives and content and the selection of presenters. All speakers and planning committee members are expected to disclose to the audience: (1) any significant financial interest or other relationships with the manufacturer(s) or provider(s) of any commercial product(s) or services(s) discussed in an educational presentation; (2) any significant financial interest or other relationship with any companies providing commercial support for the activity; and (3) if the presentation will include discussion of investigational or unlabeled uses of a product. The intent of this requirement is not to prevent a speaker with commercial affiliations from presenting, but rather to provide the participants with information from which they may make their own judgments. This seminar's faculty have made no such disclosures.

Faculty

Angela Dinh, MHA, RHIA

Angel Dinh is a manager of professional practice resource at AHIMA, where she provides professional expertise to develop AHIMA products and services aimed at furthering HIM, with a focus on HIPAA security. Prior to joining AHIMA, Ms. Dinh was a consultant with Precyse Solutions, Inc., and worked in various HIM roles including management in a healthcare software company. In addition, she is an adjunct instructor for the St. Petersburg College HIT program in St. Petersburg, Florida.

Tom Walsh, CISSP

Tom Walsh is president of Tom Walsh Consulting, LLC, in Overland Park, Kansas, conducting security training, risk analysis, and remediation activities for healthcare clients. He is a nationally recognized speaker and author on health information security topics. Prior to launching his own firm, Mr. Walsh held consulting positions with other firms, was an information security manager for a healthcare system, and worked as a contractor in the Department of Energy's nuclear weapons program.

Table of Contents

Disclaimer i
Faculty ii
Objectives 1
Polling Question #1 2
HIPAA Structure 2-3
The Security Rule 3
Security Overview 4-5
Required vs. Addressaable 5
Organizational Requirements 6
Documentation Requirements 6
Administrative Safeguards 7-8
Physical Safeguards 8-9
Technical Safeguards 9-10
Policies and Procedures 10-11
Polling Question #2 12
Q&A Session 12
Consider: How will you know if your info security program is compliant 13
#1 Assign Responsibility 14
#2 Set Standards 14
#3 Awareness and Training 15
#4 Incident Reporting 15
#5 Incident Response 16
#6 Auditing and Monitoring 16
#7 Corrective Actions 17
Polling Question #3 17
Other Thoughts 18
Auditing – Key Concepts 18-19
What to Audit? 20
Reviewing Audit Data 20
Summary 21
Resource/Reference List 21-22
Audience Questions 23
Audio Seminar Discussion and Audio Seminar/Webinar Information Online 24
Upcoming Audio Seminars and Webinars 25
AHIMA Distance Education online courses 25
Thank You/Evaluation Form and CE Certificate (Web Address) 26

Appendix 27
- Resource/Reference List 28
- Sample Information Security Incident Report Form
- Sample Audit Data Management Requirements
- CE Certificate Instructions

Objectives

1. **Learn what's addressable vs. what's required as defined by the HIPAA Security standards**

2. **Understand what policies and procedures must be in place for compliance**

1

Objectives

3. **Learn the integral parts to ensuring a successful HIPAA Security Compliance Plan**

4. **Learn how to create and maintain an audit program for verification and validation of security control**

2

Polling Question #1

How many of you have:

a) **Read the entire Security Rule**

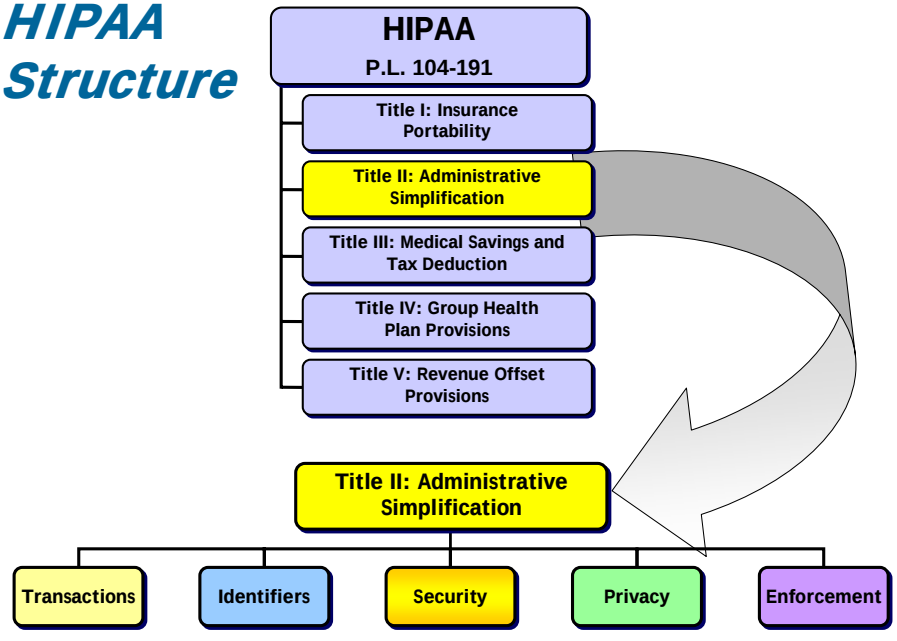
b) **Read portions of it**

c) **Heard of it**

d) **Asked, "What is it?"**

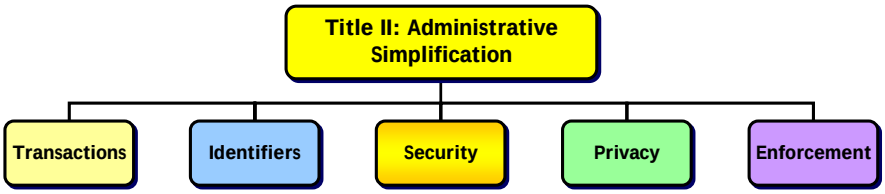
3

HIPAA Structure



4

HIPAA Structure



5

The Security Rule

- **The Security Rule**
  - **Effective in April 2005, except for small health plans.**
  - **Purpose of the Security Rule: to provide standards for administrative, physical and technical safeguards for the protection of *electronic* protected health information (ePHI).**

6

Security Overview

- **The HIPAA Security Standards**
  - **Organizational Standards**
  - **Documentation**
  - **Administrative Safeguards**
  - **Physical Safeguards**
  - **Technical Safeguards**

7

Security Overview

- **Overview of Requirements**
  - **Assignment of organizational responsibility for the security of its health information;**
  - **Provision of reasonable and appropriate safeguards**
    - to ensure the integrity and confidentiality of all healthcare information that is maintained or transmitted in electronic form,
    - to protect against reasonable anticipated threats or hazards to the confidentiality, integrity, and availability of the information,
    - to protect against reasonably anticipated unauthorized uses or disclosures of the information by the organization

8

Notes/Comments/Questions

Security Overview

- **Overview of Requirements**
  - Formal assessment of risks to the confidentiality, integrity, and availability of health information by the organization
  - Implementation and documentation of specific administrative procedures, physical safeguards, technical services for protecting data at rest, and technical security mechanics for protecting data in transit.
  - Personnel Training

9

Required vs. Addressable

- **Required Specifications**
  - Must be implemented
- **Addressable Specifications (3 possible courses of action)**
  - Implement
  - Implement alternative
  - Do not implement

10

Organizational Requirements
§ 164.314, p.8379

- **Business Associates Contracts or Other Arrangements (1R)**
  - **Contracts must comply with the rule.**
  - **Other arrangements must comply with the rule**
- **Group Health Plans (1R)**
  - **Implement appropriate safeguards for ePHI**

11

Documentation Requirements
§ 164.316, p.8379-8380

- **Policies and Procedures (0)**
  - **Reasonable and appropriate**
  - **Complies with the standards, implementation specifications, and other requirements of the security rule**
- **Retention (3R)**
  - **6 years from creation date or last effective date, whichever is later**

12

Administrative Safeguards
§ 164.308, p.8377-8378

1. **Security Management Process (4R)**
   - Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.
2. **Assigned Security Responsibility (0)**
   - Standard: Designate an individual to be Security Officer to ensure compliance with the rule
3. **Workforce Security (3A)**
   - Standard: Make sure those who need access have it and those who don't can't get it.

13

Administrative Safeguards
§ 164.308, p.8377-8378

4. **Information Access Management (1R/2A)**
   - Standard: Implement policies and procedures for the authorization of access to ePHI.
5. **Security Awareness and Training (4A)**
   - Standard: Security training program provided for all staff
6. **Security Incident Procedures (1R)**
   - Standard: Implement policies and procedures to address security incidents

14

Administrative Safeguards
§ 164.308, p.8377-8378

7. Contingency Plan (3R/2A)

- Standard: Establish and implement (as needed) policies and procedures for responding to emergencies or other occurrences (i.e. fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

8. Evaluation (0)

- Perform a periodic technical and non-technical evaluation

9. Business Associates Agreements (1R)

- Standard: obtains satisfactory assurances, in accordance with the rule that the business associate will appropriately safeguard the information.

15

Physical Safeguards
§ 164.310, p.8378

1. Facility Access Controls (4A)

- Standard: Implement policies and procedures that allows access to electronic information systems and to the facilities in which the systems are housed to those authorized for access.

2. Workstation Use (0)

- Standard: Implement policies and procedures to specify the proper functions to be performed, the manner in which they are performed, and the physical attributes of the surroundings of workstations that can access ePHI.

16

Physical Safeguards
§ 164.310, p.8378

3. Workstation Security (0)

- Standard: Implement physical safeguards to all workstations with access to ePHI.

4. Device and Media Controls (2R/2A)

- Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

17

Technical Safeguards
§ 164.312, p.8378-8379

1. Access Control (2R/2A)

- Standard: Implement policies and procedures for systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights

2. Audit Controls (0)

- Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

18

Technical Safeguards
§ 164.312, p.8378-8379

3. Integrity (1A)

- Standard: Implement policies and procedure to protect ePHI from improper alteration or destruction.

4. Person or Entity Authentication (0)

- Standard: Implement policies and procedures to verify that someone accessing ePHI is who they say they are.

5. Transmission Security (2A)

- Standard: Implement technical measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.

19

Policies and Procedures

- ✓ **Access to ePHI**
  - **Granting/Removing Access**
  - **Modification of User Access**
  - **Termination of Access**
- ✓ **User IDs and Passwords**
- ✓ **Contingency Plans (Emergency, Disaster Recovery, and Data Back Up)**
- ✓ **Media and Device Controls**

20

Policies and Procedures

- ✓ **Appropriate Use of Technology**
- ✓ **Workstations Use and Security**
  - **What is acceptable? What is not?**
  - **Logoff Guidelines**
  - **Locking Computers**
- ✓ **Physical Access (badges, keys, etc.)**
  - **Facility Security Plan**

21

Policies and Procedures

- ✓ **Information Security Policy Waivers**
- ✓ **Security Incidents (Sanctions)**
- ✓ **Protection of Confidential Information**

22

Polling Question #2

How many people in the audience are actively contributing to a security role with or without the title?

a) **Yes, I actively contribute**

b) **No**

c) **Unsure if my contributions directly support security**

23

Q&A Session…

Topic: Administrative, Physical and Technical Safeguards

To ask a question:

- **Click the "Q&A" button near the upper-left**
- **Click "NEW"**
- **Type your question in the white box**
- **Click "SEND"**

(For LIVE seminar only)

24

Consider...

How will you know if your information security program is compliant with the various regulations?

25

Compliance Program Elements

1. **Appointment of an official to oversee the program (Privacy and Security Officer)**
2. **Set standards of expected conduct (Policies and Procedures)**
3. **Training, education, and awareness (Training)**
4. **Process for receiving reports of violations (Incident Reporting)**
5. **Response to reports (Incident Response)**
6. **On-going auditing and monitoring for compliance (Audits and Evaluation)**
7. **Take appropriate corrective actions (Sanctions, risk management, security controls, etc.)**

26

#1 Assign Responsibility §164.308(a)(2)

- **Provide high visibility for the Information Security Officer (ISO) position**
  - **Distribute an executive memo to the entire workforce formally announcing the appointment of the ISO**
- **Include the ISO's name and contact information as part of the training and awareness**

27

#2 Set Standards §164.316(a)

- **Provide easy access to policies**
- **Policies written specifically for target audiences:**
  - **All users or workforce members**
  - **IT or system administrators for department applications and systems**
- **Enforce policies and apply sanctions**

"If it hasn't been documented, it hasn't been done"!

28

#3 Awareness & Training §164.308(a)(5)

- **Establish a formal information security training program**
  - **Document audiences, content and delivery methods**
  - **Syllabus, attendance sheets, handouts, etc.**
- **Create detailed security training for specific audiences**
  - **Example: Incident response teams**
- **Create periodic security awareness for everyone**

29

#4 Incident Reporting §164.308(a)(6)(ii)

- **Create a process for workforce members to report security incidents**
  - **What? How? Who? When? Where? Why?**
- **Create a way to track information security incidents**
- **Verify that Business Associates also know how to report incidents**

See supplemental resource:

SAMPLE - Info Sec Incident Report Form

30

#5 Incident Response §164.308(a)(6)(ii)

- Create incident response procedures
- Create an incident response team (IRT)
- Train IRT members and other IT staff, especially on collecting and handling evidence during an investigation
- Establish remediation or action plans to prevent similar incidents in the future

31

#6 Auditing and Monitoring §164.312(b)

- Determine user activities and events that trigger an audit log entry
- Implement procedures to periodically review
- Establish an audit logs retention schedule
- Establish an evaluation and validation process (technical and non-technical review) §164.308(a)(8)

32

#7 Corrective Actions §164.308(a)(1)(ii)(C)

- **Sanctions**
  - **Consistently enforce policies**
- **Risk Management**
  - **Manage risks to an acceptable level;**
- **Security Safeguards and Controls**
  - **Administrative**
  - **Physical**
  - **Technical**

33

Polling Question #3

Based upon the seven elements of a compliance program just presented, how would you rate your organization?

a) Documented evidence of all seven

b) Some evidence exists; but not all

c) Practices are in place, but may not be documented

d) We have compliance gaps

34

Notes/Comments/Questions

Other Thoughts...

- Compliance is not the only driver for security
- Information security makes good business sense and needs to be implemented based upon risks
- Documentation and demonstrated practices along with management support are the best indicators of a real information security program

35

Auditing – Key Concepts

- Define the purpose of auditing
- Determine what types of audit activities can be supported on applications and systems
- Determine user activities and events that trigger an audit log entry
- Perform periodic audits:
  - When there is a problem
  - Randomly by user
  - Randomly by customer, patient, or transaction

36

Notes/Comments/Questions

Auditing – Key Concepts

- Determine the retention of audit logs
  - HIPAA does not specify a length of time to keep an audit trail
  - Retention depends on the types of audit trails
- Evaluate the impact of auditing on system performance
  - Auditing can slow a system down
- Verify that the appropriate warning banners and policies are in place to monitor user activity

37

Auditing – Key Concepts

- Protect audit logs from tampering or unauthorized access
  - Store on a separate server and restrict access
  - Hackers try to erase audit logs to cover up their activities and avoid detection
- Consider using a 3rd party tool to analyze audit log data
  - Clinical systems
  - Servers and operating systems

38

What to Audit?

- Network activity
  - Logon, logoff
  - Errors: Failed logon attempts
- Clinical application – by patient
  - Browse or view (VIP, family, employee)
  - Changes to patient information
  - Exceptions and/or discrepancies
- Clinical application – by user
  - Suspected misconduct
  - Random selection

39

Reviewing Audit Data

- Repetitive mistakes
- Exceeding authority for access
- Patterns – hackers, disgruntled employees
- System administrator access

See supplemental resource:

SAMPLE Audit Data Management Requirements

40

Summary

During this webinar we:

- Explained addressable vs. required
- Suggested policies and procedures that, at a minimum, must be in place
- Described the seven core elements of a compliance program and how they relate to the Security Rule
- Discussed how to create and maintain an audit program

41

Resource/Reference List

- **CMS Final Security Rule**
http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf

- **CMS security series of white papers; download at:**
http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp

- **AHIMA Article: "Kick Starting the Security Risk Analysis"**
http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_023619.hcsp

- **Basics of Risk Analysis and Risk Management**
http://www.cms.hhs.gov/EducationMaterials/Downloads/BasicsofRiskAnalysisandRiskManagement.pdf

42

Resource/Reference List

- **Information Systems Disaster Recovery Plan Template**
http://library.ahima.org/xpedio/groups/secure/documents/external/bok1_034559.doc

- **An IT Contingency Plan to Meet HIPAA Security Standards**
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022417.hcsp

- **A Resource for Privacy and Security Programs: Version 5.0 of HIMSS CPRI Toolkit Expands to Include Privacy Topics**
http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_031660.hcsp

43

Resource/Reference List

- **Amatayakul, Margret; Steven Lazarus, Tom Walsh, Carolyn Hartley. *Handbook for HIPAA Security Implementation* published by the American Medical Association. (ISBN 1-57947-357-1)**
- **Walsh, Tom. "The 26.2-mile Security Rule" *Journal of AHIMA* (Volume 76, Number 3, March 2005) published by the American Health Information Management Association**
- **Walsh, Tom. "Tips and Techniques for Layering Security Controls" *HIPAA Security Compliance Insider* (October 2004) Brownstone Publishers**

44

Resource/Reference List

- **Walsh, Tom. "Best Practices for Compliance with the Final Security Rule" *Journal of Healthcare Information Management* (Volume 17, Number 3, Summer 2003) published by Healthcare Information and Management Systems Society**
- **NIST Special Publication 800 series: http://csrc.nist.gov/publications/nistpubs/index.html**
- **Peltier, Thomas R. *Information Security Risk Analysis*. New York: Auerbach Publications, 2001**

45

Audience Questions

Audio Seminar Discussion

Following today's live seminar
Available to AHIMA members at
www.AHIMA.org

"Members Only" Communities of Practice (CoP)
AHIMA Member ID number and password required

Join the e-HIM Community from your Personal Page. Look under Community Discussions for the *Audio Seminar Forum*

You will be able to:

- discuss seminar topics
- network with other AHIMA members
- enhance your learning experience

AHIMA Audio Seminars and Webinars

Visit our Web site
http://campus.AHIMA.org
for information on the 2008 seminar schedule. While online, you can also register for seminars and webinars or order CDs and Webcasts of past seminars.

AHIMA Distance Education
Career-building Resources

Upcoming Audio Seminars and Webinars

- **EHR Coding Practices**
  February 7, 2008
- **Inpatient EHR Product Certification– Advantages for Quality HIM**
  February 19, 2008
- **Hybrid Medical Records: A Management Tool**
  March 18, 2008

AHIMA Distance Education

Anyone interested in learning more about e-HIM® should consider one of AHIMA's web-based training courses.

For more information visit http://campus.ahima.org

Thank you for joining us today!

Remember – visit the AHIMA Audio Seminars/Webinars Web site to complete your evaluation form and receive your CE Certificate online at:

http://campus.ahima.org/audio/2008seminars.html

Each person seeking CE credit must complete the sign-in form and evaluation in order to view and print their CE certificate.

Certificates will be awarded for AHIMA CEUs and ANCC Contact Hours.

Appendix

Resource/Reference List 28
Sample Information Security Incident Report Form
Sample Audit Data Management Requirements
CE Certificate Instructions

Appendix

Resource/Reference List

CMS Final Security Rule
http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf

CMS security series of white papers; download at:
http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp

AHIMA Article: "Kick Starting the Security Risk Analysis" (member login required)
http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_023619.hcsp

Basics of Risk Analysis and Risk Management
http://www.cms.hhs.gov/EducationMaterials/Downloads/BasicsofRiskAnalysisandRiskManagement.pdf

Information Systems Disaster Recovery Plan Template
http://library.ahima.org/xpedio/groups/secure/documents/external/bok1_034559.doc

An IT Contingency Plan to Meet HIPAA Security Standards
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_022417.hcsp

A Resource for Privacy and Security Programs: Version 5.0 of HIMSS CPRI Toolkit Expands to Include Privacy Topics (member login required)
http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_031660.hcsp

Amatayakul, Margret; Steven Lazarus, Tom Walsh, Carolyn Hartley. *Handbook for HIPAA Security Implementation* published by the American Medical Association. (ISBN 1-57947-357-1)

Walsh, Tom. "The 26.2-mile Security Rule" *Journal of AHIMA* (Volume 76, Number 3, March 2005) published by the American Health Information Management Association

Walsh, Tom. "Tips and Techniques for Layering Security Controls" *HIPAA Security Compliance Insider* (October 2004) Brownstone Publishers

Walsh, Tom. "Best Practices for Compliance with the Final Security Rule" *Journal of Healthcare Information Management* (Volume 17, Number 3, Summer 2003) published by Healthcare Information and Management Systems Society

NIST Special Publication 800 series: http://csrc.nist.gov/publications/nistpubs/index.html

Peltier, Thomas R. *Information Security Risk Analysis*. New York: Auerbach Publications, 2001

Information Security Incident Report Form

Date and time of report:	Author of incident report:
Date, time and location (department) of when and where the incident occurred:	Incident discovery date and time: Incident was first reported to:
Persons involved, their job titles and phone or pager numbers:	
Check all that apply: ☐ Hardware type and asset tag number: _____ ☐ Software and Operating System: _____ ☐ Application: _____ Data Owner: _____	
Description of incident: *(What and how did it happen? How was it detected? Why did it happen?)*	
How did the incident occur?	
Has this happened before? ☐ No ☐ Yes If "Yes," when? _____	Describe any evidence collected and actions taken to contain or minimize the damage caused by the incident:
Risk to organization ☐ High ☐ Medium ☐ Low ☐ Unknown	
Person(s) responsible for follow-up and date of follow-up:	Actions taken to prevent similar incidents from occurring again:
Date incident was closed and by whom:	

SAMPLE – Audit Data Management Requirements

Audit Log Type [Purpose of Audit]	Reviewed (Frequency)		Reviewed (Responsibility)		Retention*	
	Current	Suggested	Current	Suggested	Current	Suggested
Clinical applications containing protected health information (PHI) [Validate the appropriateness of access]	Ad hoc to respond to requests or whenever inappropriate access is suspected or a known breach has occurred Employees examining their own record on-line	Random selection of employees and/or by patient to be reviewed monthly When a manager requests an audit	System administrator	Application specialist and employee's manager ISO and Privacy Official if any inappropriate access is suspected.		6 to 18 months
Financial applications [Monitor for errors or fraud]	Ad hoc	Daily or weekly When requested by an external auditor	System administrator	Application specialist, Internal auditor, or CFO's staff		6 to 18 months Accounting practices may determine length of retention
Other applications	Ad hoc	Semi-annually	System administrator	Application specialist and employee's manager		6 to 18 months
File Servers [Ensure that all group members assigned to a directory and access rights are appropriate; Ensure content of public folders do not contain confidential information]	Ad hoc	Semi-annually When group membership changes such as when employees are hired or terminated When a problem is suspected	System administrator	System administrator in conjunction with departmental leadership [Content of Public folders] ISO or their designee		12 to 18 months
Firewall [Monitor events log]	Ad hoc	Daily using automated monitoring and alarm notification	Network engineer	Network engineer		1 month

Audit Log Type [Purpose of Audit]	Reviewed (Frequency)		Reviewed (Responsibility)		Retention*	
	Current	Suggested	Current	Suggested	Current	Suggested
Internal Network [Monitor events and performance such as bandwidth]	Ad hoc	Daily using automated monitoring and alarm notification	Network engineer	Network engineer		3 months
Internet [Monitor use of the Internet for time spent and appropriateness of website visits]	Ad hoc	Weekly When requested by a manger	Firewall administrator	Firewall administrator and/or ISO or their designee		1 month
Remote Access [Monitor for appropriate access by workforce and vendors and failed attempted logons]	Ad hoc	Daily When a problem is suspected	Network engineer	Network engineer		6 months
Intrusion prevention and/or detection system (IPS or IDS) [Monitor system to ensure that no intrusion has occurred]	Ad hoc	Daily When a problem is suspected	Network engineer	Network engineer		1 month
Physical Access [Monitor badge reader – door access]	Ad hoc	Monthly When a problem is suspected	Security manager	Security manager		6 months

*** Retention**

- Retention for all audit trails may also be defined by backup procedures and tape rotation
- If the audit trails are used in an incident investigation then the legal department determines retention requirements
- Proof that audits were being performed (such as the cover sheet to audit reports) must be retained for a minimum of six years to comply with HIPAA's Security Rule

AHIMA
Distance Education
Career-building Resources

To receive your

CE Certificate

Please go to the AHIMA Web site

http://campus.ahima.org/audio/2008seminars.html
click on the link to
"**Sign In and Complete Online Evaluation**"
listed for this webinar.

You will be automatically linked to the
CE certificate for this webinar after completing
the evaluation.

Each participant expecting to receive continuing education credit must complete the online evaluation and sign-in information after the webinar, in order to view and print the CE certificate.