Auditing for Privacy and Security Compliance

Webinar
June 23, 2009

Practical Tools for Seminar Learning
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 service(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 has made no such disclosures.
Carol Ann Quinsey, RHIA, CHPS

Carol Ann Quinsey has over 30 years experience in the HIM profession, including time spent as a manager in community hospitals and specialty settings; an organizational leader for medical records, transcription, quality improvement, utilization management, and medical staff services in acute and corporate care settings; and a practice manager for AHIMA. Ms. Quinsey is currently serving as associate director of HIM operations at Group Health Cooperative.

Tom Walsh, CISSP

Tom Walsh is president of Tom Walsh Consulting, LLC, in Overland Park, KS, 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclaimer</td>
<td>i</td>
</tr>
<tr>
<td>Faculty</td>
<td>ii</td>
</tr>
<tr>
<td>Objectives</td>
<td>1-2</td>
</tr>
<tr>
<td>Terminology</td>
<td>2</td>
</tr>
<tr>
<td>Reasons for Conducting an Audit</td>
<td>3</td>
</tr>
<tr>
<td>Polling Question #1</td>
<td>3</td>
</tr>
<tr>
<td>Results from Polling Question #1</td>
<td>4</td>
</tr>
<tr>
<td>Designing Auditing Programs</td>
<td>4-5</td>
</tr>
<tr>
<td>Establishing Priorities</td>
<td>5-6</td>
</tr>
<tr>
<td>Polling Question #2</td>
<td>7</td>
</tr>
<tr>
<td>Results from Polling Question #2</td>
<td>7</td>
</tr>
<tr>
<td>Techniques for Reducing Impact</td>
<td>8-10</td>
</tr>
<tr>
<td>Optimizing Audit Practices</td>
<td>10</td>
</tr>
<tr>
<td>Audit Logs</td>
<td>11-12</td>
</tr>
<tr>
<td>Polling Question #3</td>
<td>13</td>
</tr>
<tr>
<td>Results from Polling Question #3</td>
<td>13</td>
</tr>
<tr>
<td>Enforcement and Sanctions</td>
<td>14</td>
</tr>
<tr>
<td>Improving Existing Programs</td>
<td>14-15</td>
</tr>
<tr>
<td>Polling Question #4</td>
<td>15</td>
</tr>
<tr>
<td>Results from Polling Question #4</td>
<td>16</td>
</tr>
<tr>
<td>Impact of Organizational Philosophy</td>
<td>16</td>
</tr>
<tr>
<td>ARRA Impact on Audit Programs</td>
<td>17</td>
</tr>
<tr>
<td>Resource/Reference List</td>
<td>17-18</td>
</tr>
<tr>
<td>Audience Questions</td>
<td>18</td>
</tr>
<tr>
<td>Audio Seminar Discussion</td>
<td>19</td>
</tr>
<tr>
<td>Become an AHIMA Member Today!</td>
<td>19</td>
</tr>
<tr>
<td>Audio Seminar Information Online</td>
<td>20</td>
</tr>
<tr>
<td>Upcoming Webinars</td>
<td>20</td>
</tr>
<tr>
<td>AHIMA Distance Education online courses</td>
<td>21</td>
</tr>
<tr>
<td>Thank You/Evaluation Form and CE Certificate (Web Address)</td>
<td>21</td>
</tr>
<tr>
<td>Appendix</td>
<td>22</td>
</tr>
<tr>
<td>Resource/Reference List</td>
<td>23</td>
</tr>
<tr>
<td>CE Certificate Instructions</td>
<td></td>
</tr>
</tbody>
</table>

AHIMA 2009 HIM Webinar Series
Objectives

- Designing privacy and security monitoring and auditing programs
- Establishing priorities
- Employing techniques for reducing impact
- Optimizing audit practices to accommodate technology and organizational nuances
- Addressing sticky enforcement and sanction issues

Objectives

- Evaluating the impact of organizational philosophy on an effective privacy audit program
- Improving existing privacy and security audit programs
- Providing overall recommendations for effective organizational philosophy, program design, prioritization of issues, and enforcement and application of sanctions
Objectives

- Sharing initial impressions about how the American Recovery and Reinvestment Act (ARRA) will impact privacy and security audit programs

Terminology

- Audit – a planned evaluation or review
  - “Audit” can have a negative connotation
- Types of audits we’ll focus on:
  - Investigations
    - Suspected breach to privacy and information security incidents
  - Random audits of user activities
    - By patient or by user
  - Routine audits (Internal audit or Evaluation)
    - Usually planned and scheduled in advance
**Reasons for Conducting an Audit**

- Investigate reports of inappropriate behavior
- Detect and prevent unauthorized access or fraud
  - Identity theft (Medical or financial)
- Confirm that policies are consistently being followed
- Verify compliance or identify gaps
- Comply with HI PAA Security Rule

**Polling Question #1**

Does your organization currently have an established privacy and information security auditing program?

A) Yes
B) No
C) In progress
Results from Polling Question #1

At a minimum, you should be...
- Validating user access privileges to clinical information systems
  - Directors, managers, or data owner approve
- Conducting walkthrough inspections
- Conducting an evaluation of your Privacy and Security programs at least once within three years

Designing Auditing Programs

- Defining the goals and objectives
  - Investigations
    - To determine if a breach occurred
  - Random audits of user activities
    - To create a culture of accountability
    - To avoid possible legal problems
  - Routine audits (Internal audit or Evaluation)
    - To evaluate or verify compliance
- Assigning responsibilities
  - Who will review audit logs?
**Designing Auditing Programs**

- **Estimating the resources needed**
  - Staff, tools, time, support, and etc.
- **Creating a plan**
  - Random audits
    - Determining randomness for sample selection
  - Routine audits
    - Areas of risk or follow up audits
- **Obtaining management’s approval**

**Establishing Priorities**

- System capability and functionality
- Organizational history
- Legal & risk management issues
Establishing Priorities

- Foci from previous audits or incidents
- Security overrides
- Special cases
  - Employees
  - Records restricted by patient request
- High profile cases
  - Public, celebrities and sports figures
  - Newsworthy cases

Establishing Priorities

- Remote and other access
  - Employees
  - Clinicians
  - Business Associates
  - Vendors
- Clinical situations
  - Mental or behavioral health records
  - Reproductive health records
  - Substance abuse records
Polling Question #2

If your facility has defined policy and procedures for conducting audits, is it followed rigorously?

A) Yes
B) No
C) Unknown

Results from Polling Question #2

At a minimum, you should be...
- Following a consistent process for auditing user behavior
  - Have Human Resources involved in the process in the event that sanctions will be applied
Techniques for Reducing Impact

Investigations
- Alleged or known information incidents and breaches
- Objectives include:
  - Sequential evaluation of events
  - Determine whether an individual’s conduct violated policy, the code of conduct, or was in violation of the law
  - Determine the root cause
    (Example: Poor access controls)

Techniques for Reducing Impact

Investigations
- Get Human Resources involved
- Properly handle information
  - Information obtained during investigations should be treated as if it will end up as evidence in a court case
  - Maintain a “chain of custody”
  - Protect the integrity of any evidence
  - Maintain confidentiality
Techniques for Reducing Impact

Random Audits

- Users
  - Employ a random number generator to select by employee number, badge number, or from a list of names
  - “Periodic” versus “quarterly”

- Patients
  - Establish audit log triggers
    - Same last name as workforce member
    - Discharged patient (over 30 days)
    - Certain types of procedures/tests

Routine Audits

- Planning (“Doing your homework”)
  - Define specific objectives
  - Notification of audit
  - Request documentation in advance
  - Requested interviews and tours

- Organizing
  - Condense interviews and tours

- Meeting
  - Go to their office or department
Techniques for Reducing Impact

Routine Audits

- Fieldwork – “data gathering phase”
  - Start with a short kickoff meeting
    - Have a written agenda for the meeting
  - Interviews
  - Tours – Walkthrough inspections
  - Validating technical and physical controls
  - End with an “Exit Briefing”

Goal: Minimize the interruption of staff

Optimizing Audit Practices

- Tools typically make it easier for an auditor to accomplish their objectives
  - Equipment or software used to monitor
    - Intrusion prevention systems (IPS)
    - Intrusion detection systems (IDS)
  - Vulnerability scanners
  - Forms or checklists
  - Social engineering exercise
  - Audit logs
Questions to ask:
- What activities need to be captured in an audit log?
- How long will you want to retain the audit logs?
- What performance impacts are acceptable?
- Who will review audit logs?

Determine what user activities should trigger an audit log entry
- Successful logon, logoff, and unsuccessful logon attempts
- Screens viewed and reports printed
- Data changes (additions, edits, deletions)

See the Certification Commission for Healthcare Information Technology (CCHIT) Security Criteria for recommended audit log capability of an Electronic Health Record (EHR)
www.cchit.org
### Audit Logs

- Centralized storage of audit logs
  - Maintain audit log integrity
  - Running audit log analysis programs
  - Audit log correlation
  - Audit log archiving and retention

There are no specifications for audit log retention within the HIPAA Security Rule. A retention schedule should be based upon the types of audit information being logged, your storage capability, and possible need of the information at a later date.

### Warning banners

- Should appear at network and application logon to notify users that auditing and monitoring is occurring
- Create awareness and a culture of accountability
- In case of litigation

WARNING! Use of this system constitutes consent to security monitoring and testing. All activity is logged by your User ID.
Polling Question #3

Has your organization had to apply sanctions related to breaches of confidentiality or loss of PHI?

A) Yes
B) No
C) Unknown

Results from Polling Question #3

At a minimum, you should be...
- Following the recently released AHI MA Practice Brief: Sanction Guidelines for Privacy and Security Breaches
  - Using a tier approach to sanctions based upon severity and intentions
- Applying sanctions consistently across the organization
**Enforcement and Sanctions**

- Policies and Procedures
  - Investigators
  - Decision Makers
  - Relation to other sanction policies
- Equity and Fairness
  - Role vs. Role
- Investigation and Follow-Through

**Improving Existing Programs**

- Periodically review reports and audit logs (versus only when there is a problem)
  - Establish procedures and responsibilities to regularly review records of reported breaches, incidents and audit logs
  - Provide sample audit reports to managers of their employees’ activities
  - Information system activity review (Required) §164.308(a)(1)(ii)(D)
Improving Existing Programs

- Conduct a periodic evaluation
  - Conduct internal audits in key areas
  - Consider having a third party perform an evaluation of the programs
    Evaluation §164.308(a)(8)
  - Use the CMS sample checklist - *Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews* for verifying the required compliance documentation

Polling Question #4

Has your organization mapped out your compliance documentation against the CMS sample checklist - *Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews*?

A) Yes
B) No
C) In progress
Results from Polling Question #4

At a minimum, you should be...

- Working to map out existing documentation that would be used as evidence in the event that your organization is audited by CMS
  - *Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews*
- Working to fill in any existing gaps

Impact of Organizational Philosophy

- Tie to organizational compliance
- Attitude of leadership and managers
- Work environment
- Consistency and constancy of privacy and security messages
ARRA Impact on Audit Programs

- **Breach notification**
  - Key concept, “…should reasonably have been known…” (implies active auditing, monitoring, and investigative processes)

- **Accounting of Disclosures**
  - Old “…except for TPO”
  - New - If the Covered Entity uses or maintains an electronic health record (EHR), then the exception for Accounting of Disclosures for TPO no longer applies

Resource/Reference List

- AHI MA HI PAA Community of Practice
- AHI MA Body of Knowledge
- AHI MA Distance Education. “Building an Effective Security Audit Program to Improve and Enforce Privacy Protections.”
  

- ISACA – Previously known as the Information Systems Audit and Control Association
  
  [www.isaca.org](http://www.isaca.org)
Resource/ Reference List

- Centers for Medicare and Medicaid Services (CMS), “HI PAA Compliance Review Analysis and Summary of Results” -- HI PAA compliance reviews conducted in 2008
  

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

Become an AHIMA Member Today!

To learn more about becoming a member of AHIMA, please visit our website at www.ahima.org/ membership to join now!
AHIMA Audio Seminars and Webinars

Visit our Web site http://campus.AHIMA.org for information on the 2009 seminar schedule. While online, you can also register for seminars and webinars or order CDs, MP3s, and webcasts of past seminars.

Upcoming Webinars

ARRA Town Hall
June 25, 2009

MPI Clean Up: It’s a Must!
July 21, 2009

Preparing to Implement ICD-10-CM/PCS
July 30, 2009
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:


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.
Appendix

Resource/Reference List .................................................................................................................. 23
CE Certificate Instructions
Appendix

Resource/Reference List

https://campus.ahima.org/abo/catalog/lms/Products/DisplayProduct.aspx?ProductId=1598&CategoryId=176&CatalogId=2


www.isaca.org
To receive your

**CE Certificate**

Please go to the AHIMA Web site


and 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.