Access and Control in Electronic Health Records

Audio Seminar/ Webinar

November 20, 2007

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 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.
Aviva Halpert, MA, RHIA, CHPS

Ms. Halpert is the Chief HIPAA Officer at Mount Sinai Medical Center in New York. Ms Halpert has over 25 years experience in health information management (HIM), and is a frequent speaker and author on both HIPAA and HIM topics. During her career, she has served as a Privacy and Compliance Officer, Director of Clinical Information Resources, and Director of Special Projects for Mount Sinai. She is a very active member with AHIMA, the Health Information Management Association of New York City, and the NYC Metro Infragard Members Alliance.

Kenny Chu, JD, CISSP, CISA

Mr Chu is the Senior Director for IT Security at Mount Sinai Medical Center in New York. Mr. Chu has 20 years experience in Information Technology. During his career, he has supported nearly all aspects of Information Technology operations; ranging from Desktop support, Systems Administration, and Network Management. He is a member of ISACA and the NYC Metro Infragard Members Alliance.
## Table of Contents

Disclaimer .................................................................................................................... i
Faculty ....................................................................................................................... ii
Legal Requirements..................................................................................................... 1-4
Polling Question #1........................................................................................................ 3
Getting Started
  Establish your philosophy.......................................................................................... 3
  Basic principles ....................................................................................................... 4
  Develop policies and procedures .......................................................................... 4
  Prepare the groundwork .......................................................................................... 5
  Functionality and user access rights ...................................................................... 6-8
  Role-based definition grid (also in appendix)....................................................... 6-7
Goals .......................................................................................................................... 9
Technology Solutions....................................................................................................10
Identity Management ..................................................................................................10-11
ID Provisioning ......................................................................................................... 11-12
Single Sign On .......................................................................................................... 12-13
Enterprise Directory System .................................................................................... 13
Audit Log .................................................................................................................... 14
AAA .......................................................................................................................... 14
Polling Question #2.....................................................................................................15
Resources/References .................................................................................................15-16
Audience Questions....................................................................................................17
Audio Seminar Discussion and Audio Seminar Information Online..........................17-18
Upcoming Audio Seminars .........................................................................................18
AHIMA Distance Education online courses (and course discount)...............................19
Thank You/Evaluation Form and CE Certificate (Web Address)..................................20
Appendix .....................................................................................................................21
  Resource/Reference List .........................................................................................22
  Role-based definition grids .................................................................................... 23-24
  CE Certificate Instructions
Legal Requirements

• **HIPAA**
  • Privacy Rule – 164.530(2)(1)
    - Safeguards
    - Definitions of who should have access to what

Legal Requirements (Continued)

• Security Rule –
  - 164.308(6)(4) – technical solutions
  - 164.312(a)(1) – Access Control
    (access to ePHI must be restricted to those who have been granted access rights)
  - 164.312 (d) – Person or Entity Authentication (covered entities must have procedures to verify the identity of anyone attempting to access ePHI)
Legal Requirements

(Continued)

- Joint Commission -
  - IM 2.10 - general standard
  - IM 2.10.7 - must provide
    “Protection against unauthorized intrusion, corruption or damage”

Legal Requirements

(Continued)

- Varies by individual state
e.g., NY - 405.10
- Good business practice - control of the environment
Polling Question #1

Are you involved in access management?

*1 Yes
*2 No

Getting Started
—Establish your philosophy

- All or nothing access vs. access to specific data elements, chart portions
- Balance increased security against increased maintenance
- If you tighten screws too much people will find work-arounds - share logons, not log off, etc.
Getting Started
—Basic principles

- Access to any electronic medical record/database must be driven by role-based definitions
- The tasks associated with each role should be tied to system functionality, corresponding access type and patient view necessary to perform each task
- Use the least number of categories that accomplishes the goal
- Tables should take into account both your need and system capability

Getting Started
—Develop policies and procedures

- Evaluate each employee to insure appropriate level of access is provided.
- If the employee is a transfer from another department, evaluate existing access rights and reconcile with new job functionality.
- If it is a new employee
  - authenticate employment status.
  - determine if an existing role exists to cover assigned tasks or whether a new role must be created.
- If the employee's role has changed within the department, evaluate existing rights and reconcile with new job functionality.
**Getting Started**
—Prepare the groundwork

- A system administrator should be identified to assume responsibility for
  - Authorizing new roles and new staff
  - Verifying employee status
  - Maintaining a list of outbound interfaces
  - Terminating access when employee leaves
  - Monitoring access

(Continued)

- An administrator/administrative body should be identified that will
  - Develop/approve policy
  - Mediate exceptions to policy

Notes/Comments/Questions
## Getting Started
—Functionality and user access rights

- Develop a grid of system functionality and user access rights
  - **List user roles**
    - Clinicians (MD, RN, ancillary, etc)
    - Operations (HIM, QA, RM, Credentialing, etc.)
    - Payment
    - Outside reviewer

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
<th>Functionality Needed</th>
<th>Population Segment</th>
<th>View</th>
<th>Access Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Getting Started
—Functionality and user access rights

(Continued)

- **Define job functions**
  - Chart review
  - Correspondence
  - Order entry
  - Data entry
  - Data QA
  - Audit access
Getting Started
—Functionality and user access rights

(Continued)

• **List system functionality**
  - Data capture
  - Data retrieval
  - Data analysis
  - Order entry
  - Imaging (capture, process, display)
  - PACS (capture, process, display)

Getting Started
—Functionality and user access rights

(Continued)

• **Tie appropriate functionality to each role including**
  - **Access type**
    - Read only
    - Enter/ modify data
    - Print
  - **Population segment**
    - Inpatient
    - OPD
    - Protected population
    - Specified patient list
• **Determine appropriate View**
  - Current
  - Archived
**Goals**

- Verify that established procedures are followed when creating account

- Track access provided -
  - Recertify access
  - Terminate all accounts when necessary

**Goals**

- Reduce the likelihood that accounts are shared by users

- Audit access to verify compliance with institutional policies
Technology Solutions

- ID management
- ID provisioning
- Single sign on
- Audit log analysis

Identity Management

- Know who your users are
  - Employment term - FT, Contractor
  - Contact Information
  - Responsible Party
  - Access given
Identity Management

- Periodic Recertification of Access
- Timely Termination of Access Privileges

ID Provisioning

- Automate account management
  - Create
  - Modify *
  - Delete
**ID Provisioning**

- Automation of procedures and workflows assumes that there are defined procedures and workflows in place.

- Relies on Identity Management to be fully effective

**Single Sign On**

- System records and stores credentials to other IT systems

- User only needs to provide SSO credentials, the SSO system will automatically log the user in as they access other systems.
Single Sign On

- Keys to the Kingdom
  - Any access should be properly managed, whether it is to one or a dozen systems
  - More consistent application of access controls
  - Reduces the likelihood of account sharing

Enterprise Directory System

- Addresses some of the needs of Identity Management, ID Provisioning, and Single Sign On
- Unify access control into one system
- Active Directory becoming the predominant commercial Directory
- Open source - LDAP, Kerberos
Audit Log

- Systems to aggregate logs from multiple systems
- Help facilitate a global picture of access
- Automate some access review tasks

AAA

- Triple A - The three major aspects of access control
  - Authentication
  - Authorization
  - Accounting
Polling Question #2

Does your institution have remote access functionality?

*1 Yes
*2 No

Resources/References — Web Sites

American Health Information Management Association (AHIMA)
www.ahima.org

Centers for Medicare and Medicaid Services (CMS)
www.cms.hhs.gov/HIPAAGenInfo

Code of Federal Regulations (CFR)
www.gpoaccess.gov/cfr/index.html

Electronic Privacy Organization (EPIC)
www.epic.org/

National Council on Vital Health Statistics (NCVHS)
www.ncvhs.hhs.gov/

Office of Civil Rights (OCR)
www.hhs.gov/ocr/hipaa/
Resources/References
—Web Sites

State privacy law summaries maintained on the Health Privacy Project Web site:
www.alllaw.com/state_resources

AHIMA State Associations:
http://www.ahima.org/directory/csa.asp
Search by state for links or information on state regulations

HIPAA 42 CFR 164

Privacy rule:
www.hhs.gov/ocr/hipaa/finalreg.html

Security Rule:

Resources/References
—Publications

• HIPAA Security Series: 2 — Security Standards, Administrative Safeguards,
  www.cms.hhs.gov/EducationMaterials

• AHIMA Practice Brief: “HIM Principles in Health Information Exchange”, eHIM Workgroup on HIM in Health Information
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035095.hcsp

• “Access Controls,” The Best of In Confidence: Selected Readings, AHIMA, pp. 171-187
  https://imis.ahima.org/orders/productDetail.cfm?pc=AB104105
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

Visit our Web site http://campus.AHIMA.org for information on the 2007 and 2008 seminar schedules. While online, you can also register for seminars or order CDs and Webcasts of past seminars.

Upcoming Audio Seminars

- HI PAA Security: What Everyone Should Know
  January 17, 2008
- EHR Coding Practices
  February 7, 2008
- Inpatient EHR Product Certification—Advantages for Quality HIM
  January 17, 2008
Anyone interested in learning more about e-HIM® should consider one of AHI MA's web-based training courses.

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

Participants in today's audio seminar can receive a 20% discount on registration in the following AHI MA distance education program:

Electronic Records Management

For program details and to receive discount, visit
http://campus.ahima.org/promotion/himerm
Coupon code: 23701

Thank you for joining us today!

Remember – visit the AHIMA Audio Seminars 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 and ANCC Contact Hours.
Appendix

Resource/Reference List ................................................................. 22
Role-Based Definition Grids ........................................................... 23-24
CE Certificate Instructions
Resource/Reference List

Web Sites

American Health Information Management Association (AHIMA)
www.ahima.org

Centers for Medicare and Medicaid Services (CMS)
www.cms.hhs.gov/HIPAAGenInfo

Code of Federal Regulations (CFR)
www.gpoaccess.gov/cfr/index.html

Electronic Privacy Organization (EPIC)
www.epic.org/

National Council on Vital Health Statistics (NCVHS)
www.ncvhs.hhs.gov/

Office of Civil Rights (OCR)
www.hhs.gov/ocr/hipaa/

State privacy law summaries maintained on the Health Privacy Project Web site:
www.alllaw.com/state_resources

AHIMA State Associations:
http://www.ahima.org/directory/csa.asp
Search by state for links or information on state regulations

HIPAA 42 CFR 164:

Privacy rule:
www.hhs.gov/ocr/hipaa/finalreg.html

Security Rule:

Publications

HIPAA Security Series: 2 — Security Standards, Administrative Safeguards,
www.cms.hhs.gov/EducationMaterials

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035095.hcsp

“Access Controls,” The Best of In Confidence: Selected Readings, AHIMA, pp. 171-187
https://imis.ahima.org/orders/productDetail.cfm?pc=AB104105
## ROLE-BASED DEFINITION GRID

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
<th>Functionality Needed</th>
<th>Population Segment</th>
<th>View</th>
<th>Access Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ROLE-BASED DEFINITION GRID
Shared system

System: ________________________________

Owner: ________________________________ Other User Departments: ________________________________

Administrator: __________________________ Other Department Contacts: ________________________________

Technical Administrator: ____________________

<table>
<thead>
<tr>
<th>Dept.</th>
<th>Role</th>
<th>Function</th>
<th>Functionality Needed</th>
<th>Population Segment</th>
<th>View</th>
<th>Access Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To receive your CE Certificate

Please go to the AHIMA Web site


click on the link to “Sign In and Complete Online Evaluation” listed for this seminar.

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

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