ARRA: What's Next for HIM and Privacy?

Webinar
August 25, 2009

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.

Usage Rights

This document is exclusively for use by individuals attending the associated audio seminar or webinar (named on the first page of this document), in conjunction with their attendance of the live or recorded version of the presentation. All material herein is copyright 2009 American Health Information Management Association (AHIMA), except where otherwise noted. It may not be redistributed without prior written permission from AHIMA.
Faculty

Jill Callahan Dennis, JD, RHIA

Jill Callahan Dennis is a principal of Health Risk Advantage, a risk-management consulting firm that assists healthcare organizations nationwide to minimize their risk of liability.

Ms. Dennis served on AHIMA’s Board of Directors from 2002 through 2007, and as president in 2006. She has 30 years of experience in the HIM profession, and is a frequent speaker and author on risk management, privacy, and electronic health information management topics.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclaimer</td>
<td>1</td>
</tr>
<tr>
<td>Faculty</td>
<td>ii</td>
</tr>
<tr>
<td>Our Agenda</td>
<td>1</td>
</tr>
<tr>
<td>Polling Question#1: Who's Here</td>
<td>1</td>
</tr>
<tr>
<td>Impact of ARRA: HIM in General</td>
<td>2</td>
</tr>
<tr>
<td>Key Privacy/Security Impacts</td>
<td>2</td>
</tr>
<tr>
<td>Business Associates</td>
<td>3</td>
</tr>
<tr>
<td>PHR Information Protections</td>
<td>3</td>
</tr>
<tr>
<td>Stepped-up Role for HHS Regional Offices</td>
<td>4</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>4</td>
</tr>
<tr>
<td>Restriction Requests</td>
<td>5</td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>5</td>
</tr>
<tr>
<td>Access to Information: Electronic Format</td>
<td>6</td>
</tr>
<tr>
<td>Limited Data Set; Minimum Necessary</td>
<td>6</td>
</tr>
<tr>
<td>Enhanced Enforcement</td>
<td>7</td>
</tr>
<tr>
<td>Online Q&amp;A: Key Privacy Provisions</td>
<td>7</td>
</tr>
<tr>
<td>Polling Question #2: Biggest Challenge</td>
<td>8</td>
</tr>
<tr>
<td>New and Expected Regulations</td>
<td>8</td>
</tr>
<tr>
<td>HHS Regs: Breaches of Unsecured PHI</td>
<td>9-12</td>
</tr>
<tr>
<td>HHS Regs: Breach Notifications</td>
<td>13</td>
</tr>
<tr>
<td>HHS Regs: Administrative Requirements</td>
<td>13</td>
</tr>
<tr>
<td>PHR Breaches: Health Breach Notification Rule (FTC)</td>
<td>14</td>
</tr>
<tr>
<td>FTC Health Breach Notification Rule</td>
<td>14</td>
</tr>
<tr>
<td>FTC Rule Definitions</td>
<td>15</td>
</tr>
<tr>
<td>FTC Health Breach Notification Rule</td>
<td>16</td>
</tr>
<tr>
<td>Online Q&amp;A: New and Upcoming Regulations</td>
<td>17</td>
</tr>
<tr>
<td>Preparing for the Near-Term Future</td>
<td>17</td>
</tr>
<tr>
<td>Polling Question #3: How Ready</td>
<td>18</td>
</tr>
<tr>
<td>Resource Links</td>
<td>18</td>
</tr>
<tr>
<td>Online Q&amp;A: Anything We've Covered</td>
<td>19</td>
</tr>
<tr>
<td>Audience Questions</td>
<td>19</td>
</tr>
<tr>
<td>Thank You</td>
<td>20</td>
</tr>
<tr>
<td>Audio Seminar Discussion and Webinar Information Online</td>
<td>20-21</td>
</tr>
<tr>
<td>Upcoming Audio Seminars</td>
<td>21</td>
</tr>
<tr>
<td>AHIMA Distance Education Online Courses</td>
<td>22</td>
</tr>
<tr>
<td>Thank You/Evaluation Form and CE Certificate (Web Address)</td>
<td>22</td>
</tr>
<tr>
<td>Appendix</td>
<td>23</td>
</tr>
<tr>
<td>Resource/Reference List</td>
<td>24</td>
</tr>
<tr>
<td>CE Certificate Instructions</td>
<td>25</td>
</tr>
</tbody>
</table>
Our Agenda

- Areas of HI PAA and HIM most affected
- Key privacy provisions of ARRA
  - Brief opportunity for questions
- New and impending regulations, key effective dates
  - Another pause for questions
- What can we do to prepare
- Open Q&A

Polling Question #1: Who’s Here

Your “status” under HI PAA/ARRA:

a) Work for “covered entity”
b) Work for “business associate”
c) Consult/advise CEs and/or BAs
d) Work for PHR vendor/related business
e) Work for EHR software vendor
f) Work for HIE
g) None of the above
**Impact of ARRA: HIM in General**

- The goal - economic stimulus - but impacts go beyond
- Effect on HIM generally: an EHR “growth spurt”
  - ONC codified - HIT Policy, HIT Standards
  - NIST standard testing
  - Grant and loan funding
  - HIT regional extension centers
  - Expansion of health informatics education
  - Incentives to adopt and “meaningfully” use EHRs

**Key Privacy/Security Impacts**

- Expansion of certain HIPAA provisions to business associates
- Personal health record information protections
- Regional privacy advisors for HHS regional offices, education campaign
- Breach notification requirements
- Restriction requests
- Accounting of Disclosure obligation expands
- Access to information in electronic format
- Use of “limited” data set, and coming changes to “minimum necessary”
- Stiffer enforcement
**Business Associates**

- Previously were only indirectly affected by HIPAA’s privacy and security rules (via BAA)
- Now directly accountable to comply with certain provisions
- Must report security breaches of “unsecured PHI” to CE
- Must comply with administrative, technical, and physical safeguards of security regs
- May be responsible for accounting of disclosures for their disclosures (CE option if EHR)
- Permit patient access in e-format

**PHR Information Protections**

- Requirements for security breach notification
- Rules for their vendors as well
- Federal Trade Commission reporting
- Breach definition is broader than the one for CEs and BAs
  - Security breach – acquisition of unsecured PHR-identifiable health information of individual without their authorization
- FTC regs just now coming out; effective 30 days after publication
- Will sunset if Congress enacts new legislation on point
Stepped-up Role for HHS Regional Offices

- Regional privacy advisors
- Offer guidance and education to CEs, BAs, the public
- National education programs in 2010 - focus on public
  - Would this aid in your patient education?

Breach Notification

- What is a “breach” - ARRA
  - Unauthorized acquisition, access, use, or disclosure that compromises the privacy or security of the information, except where the party would not reasonably have been able to retain the information
  - May not agree with state statute definitions
  - Good faith exceptions and caveats
- Must notify patient/next of kin without unreasonable delay, but no later than 60 calendar days after you knew (or should have known) - content requirements for notice
- First-class mail (can also call if speed is needed); email option if patient prefers
- Posting on website if ten or more patients, notice to media if more than 500
- Reporting requirements to Secretary
Restriction Requests

- We must accept requests to restrict payment- and healthcare operations-related disclosures to health plan, if that information pertains solely to an item/service for which you have been paid out of pocket in full
- Why this won’t be easy

Accounting of Disclosures

- If CE uses/maintains EHR, the TPO exception no longer applies
  - For disclosures made “through” an electronic record! (Sec. 13405(c)(1)(A)
  - Not all disclosures are made this way!
- Can request for up to three years prior
- Regs expected this month (stay tuned)
- Effective date varies with when you started using EHR
**Access to Information: Electronic Format**

- Patient can obtain information in electronic format if you have an EHR
- Fee cannot exceed your labor costs
- How will this square with various state copy cost provisions?
- Can your applications easily do this?

**Limited Data Set; Minimum Necessary**

- New preference for use of “limited data set”
  - Stripped of names, addresses, telephone numbers, fax numbers, email address, medical record numbers, social security, health plan numbers, account numbers, certificate/license numbers, vehicle identifiers, device and serial numbers, URL/IP identifiers, biometric data, full face photos and comparable images
- If not practicable, use “minimum necessary” to accomplish purpose
- How will you first consider whether limited data set is practicable?
**Enhanced Enforcement**

- More “active” stance
- Audits, not just complaint-driven
- Can enforce against people, not just organization
- Increased fines/penalties, depending on level of intent or neglect
- Penalty required unless violation was made without knowledge
- Collected penalties will support enforcement actions
- Still no private right of actions, but State Attorneys General can sue

---

**Q&A ...**

- **Topic: Key Privacy Provisions**

  **To ask a question:**
  - Click the “questions” button near upper-right
  - Click “NEW”
  - Type your question in the white box
  - Click “SEND”

  *(For LIVE seminar only)*
**Polling Question #2: Biggest Challenge**

*Your biggest challenge is likely to be:*

- a) Breach notification
- b) Accounting of disclosures
- c) Providing access in electronic format
- d) Handling restriction requests
- e) Updating business associate agreements
- f) Minimum necessary
- g) Getting staff educated and compliant

**New and Expected Regulations**

- **This month**
  - Guidance on minimum necessary?
  - Accounting of Disclosures?
  - Sale of PHI?
  - Interim final rule: breaches (HHS, plus final rule from FTC re: PHR info)

- **August 2010**
  - “Willful neglect”

- **Other “guidances” coming**
HHS Regs: Breaches of Unsecured PHI

- Interim Final Rule with Request for Comments
- Applies to covered entities and their business associations
- 8/24/09 Federal Register; effective for breaches occurring on or after 9/23/09 (sanction delay)
- Includes updated guidance on what renders PHI unusable, unreadable, or indecipherable to unauthorized individuals
- Comments due within 60 days of publication; 14 day deadline for comments on information collection requirements
- Applies to covered entities and their business associates

HHS Regs: Breaches of Unsecured PHI

- Unsecured PHI = PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance (to render PHI unusable, unreadable, or indecipherable to unauthorized individuals)
- If CE/BAs implement the specified technologies and methodologies called for in the guidance, they are NOT required to provide notification of breaches
- Original guidance was in 4/27/09 Federal Register; named “encryption” and “destruction” as acceptable methods
- The new regs update this guidance
ARRA: What's Next for HIM and Privacy?

HHS Regs: Breaches of Unsecured PHI

- Regs answered many questions:
  - Is encryption required? No
  - Is redaction of paper records enough to render it secure? No (only destruction); but notification may not be necessary if the redaction renders it “deidentified” under HIPAA
  - Destruction of electronic media must be done in manner consistent with NIST “Guidelines for Medical Sanitization”, special publication 800-88.
  - CEs/BAs should keep encryption keys on a separate device from the data they encrypt/decrypt
- There will be annual updates to the guidance; next is April 2010.

HHS Regs: Breaches of Unsecured PHI

- Restates ARRA definition of “breach”:
  - The acquisition, access, use, or disclosure of PHI in a manner not permitted [by the privacy rule], which compromises the security or privacy of the PHI
  - Exceptions for:
    - Unintentional acquisition, access, or use of PHI by workforce member or person acting under authority of CE or BA, if such acquisition/access/use was made in good faith and within the scope of authority, and does not result in further use of disclosures in a manner not permitted [by the privacy rule];
    - Inadvertent disclosure of PHI between persons authorized to access PHI in the same CE or BA, or within the same OHCA, and the information is not further use of disclosed in a manner not permitted [by the privacy rule];
    - A disclosure of PHI where a CE/BA has good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain it.
HHS Regs: Breaches of Unsecured PHI

- This definition has TWO parts
- Not all violations of the privacy and security rule will be breaches. But for something to be considered a breach, it MUST be a violation of the privacy rule and is MUST compromise the security or privacy of the PHI
  - Example: Incidental disclosures. A use or disclosure of PHI that is “incident to” an otherwise permissible use or disclosure, and occurs despite reasonable safeguards and proper minimum necessary procedures, is NOT a violation and is NOT a breach.

Don't forget the second part

- What “compromises the security or privacy of the PHI”?  
  - It “poses a significant risk of financial, reputational, or other harm to the individual” 
  - Risk assessment of these events to see if they qualify as breaches 
  - Impermissible uses/disclosures of “limited data set”, including DOB and zip codes, does not compromise security or privacy (is not a breach)
**HHS Regs: Breaches of Unsecured PHI**

- Burden of proof on CE/BA
- Document the risk assessment
- In case of the limited data set exception, need documentation that the information did not include those impermissible data elements (16 elements, plus zip codes or date of birth)

---

**HHS Regs: Breaches of Unsecured PHI**

- If breach occurs:
  - Notify each individual whose info has been (or reasonably believed by CE to have been) accessed, acquired, used, or disclosed as a result of that breach
  - Unless there's a law enforcement delay, notification must occur “without unreasonable delay” and in no case later than 60 calendar days after discovery
  - Discovery “clock” is triggered on first day breach is actually known, or would have been known by exercising reasonable diligence, by any person (other than person committing breach) who is a workforce member or agent of the CE
- If breach occurs at BA, notify CE (within 60)
HHS Regs: Breach Notifications

- “Plain language” notification must include, to extent possible:
  - Brief description of what happened, including date of breach and discovery (if known);
  - Description of types of unsecured PHI involved in the breach;
  - Steps individual(s) should take to protect themselves;
  - Brief description of what the CE is doing to investigate, mitigate harm, and protect against further breaches; and
  - Contact procedures for questions or more information (shall include toll-free telephone, email address, web site, or postal address).
  - Note: these elements may be provided in one or more mailings as information is available. (Need not be all in one.)
- Written notice by first-class mail to individual at last-known address or, if individual agrees, by email.
- Provisions for “substitute” notice methods if contact information is unknown or out of date (telephone, posting on home page, broadcast media, etc., method options vary with number of people affected by breach)
- Provisions for notice to Secretary of HHS. (< 500 log and annual report; 500 or more requires contemporaneous notice to Secretary)

HHS Regs: Administrative Requirements

- CE must train workforce on breach policies and procedures, as necessary and appropriate to their duties (and must HAVE compliant policies and procedures)
- If this changes their duties, they must be trained within a reasonable period of time of the change
- CE must have process for individuals to complain about CE’s breach-related policies and procedures
- CE must apply appropriate sanctions against workforce members who don’t comply
- CE may not retaliate against anyone for exercising their rights or filing complaint, and may not require individuals to waive any of these rights
- Must maintain documentation sufficient to meet burden of proof (of compliance)
PHR Breaches: Health Breach Notification Rule (FTC)

- Final Rule should be in Federal Register any day (review copy up on FTC website)
- Requires vendors of personal health records (PHRs) to notify consumers when the security of their individually-identifiable health information has been breached
- Rule does not apply to CEs or their BAs
- A few organizations will be subject to both the FTC and HHS rules

FTC Health Breach Notification Rule

- Will be effective 30 days after FR publication
- FTC attempted to harmonize rule with HHS
- Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third party service providers, that maintain information of US citizens or residents
- Does not apply to CEs, or to “any other entity to the extent that it engages in activities as a BA of a CE”
FTC Rule Definitions

- “Breach of security” means, with respect to unsecured PHR identifiable health information of an individual in a personal health record:
  - Acquisition of such information without the authorization of the individual
  - Unauthorized acquisition is presumed to include unauthorized access to unsecured PHR identifiable health information

- “PHR identifiable health information” means “individually identifiable health information” that:
  - is provided by or on behalf of the individual; and
  - that identifies the individual (or there is a reasonable basis to believe the information can be used to identify the individual).

FTC Rule Definitions

- “Vendor of personal health records” means:
  - An entity (other than a HIPAA-covered entity or BA) that offers or maintains a personal health record.

- “PHR-related entity” means:
  - An entity (other than CE or BA) that offers products or services through the website of a vendor of PHRs; offers products or services through websites of HIPAA-covered entities that offer individuals PHRs; or accesses information in a PHR or sends information to a PHR.

- “Third-party service provider” means:
  - Entity that provides services to vendor of PHRs in connection with the offering or maintenance of a PHR or to a PHR-related entity in connection with a product or service offered by that entity; and
  - Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.
**FTC Health Breach Notification Rule**

- If breach by PHR vendor or PHR-related entity, each must notify individual whose unsecured PHR identifiable info was acquired by an unauthorized person as a result of the breach; and
- Must also notify the FTC
- Third-party service providers must notify the vendor or the related entity as specified in their contracts (if no contract designation, then to a senior official at vendor or related entity)

**FTC Health Breach Notification Rule**

- Discovery “clock” and standards are consistent with HHS rules
- Notification methods also consistent with HHS rules
  - e.g., written notice by first-class mail, provisions for substitute notice; notice to FTC; media notice if 500 or more involved, etc.)
- Plain language required; elements specified
- Violations treated as unfair or deceptive acts or practices under the FTC Act.
Q&A ...

• **Topic: New and Upcoming Regulations**

To ask a question:
• Click the “questions” button near upper-right
• Click “NEW”
• Type your question in the white box
• Click “SEND”

*(For LIVE seminar only)*

---

**Preparing for the Near-Term Future**

• What policy/procedural changes will be needed?
• Will you ask business associates to take on AoD responsibilities?
• Will you revise BAAs?
• Can you parse information for items or services paid in full by patient?
• Can you provide copies to patient in electronic format?
• Who will shepherd the changes?
• Effective dates can help prioritize
• Don’t forget staff education
Polling Question #3: How Ready

How far along are you in dealing with ARRA?:

a) Still gathering background information
b) Have a basic understanding, haven’t really started planning
c) Planning is underway
d) We’ve begun implementing some of the necessary changes

Resource Links

- AHI MA’s ARRA website
  - www.ahima.org/arra/
- ARRA (the law itself)
  - http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f%3Ah1enr.txt.pdf
- HHS ARRA Resources
- FTC rules on Health Breach Notification
  - www.ftc.gov, under “quickfinder” click on “Privacy and Data Security”
Q&A …

Topic: Anything We’ve Covered

To ask a question:
• Click the “questions” button near the upper-right
• Click “NEW”
• Type your question in the white box
• Click “SEND”

(For LIVE seminar only)

Audience Questions
Thank you!

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 2009 seminar schedule. While online, you can also register for seminars and webinars or order CDs, MP3s, and webcasts of past seminars.

Upcoming Webinars

- Managing Privacy through Systems Access Policy: Mitigating Medical Identity Theft
  September 22, 2009
- The Legal Health Record: Copy and Paste Guidelines
  November 17, 2009
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

Thank you for joining us today!

Remember – visit the AHI MA 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 AHI MA CEUs.
Appendix

Resource/Reference List .................................................................................................24
CE Certificate Instructions ..............................................................................................25
Resource/ Reference List

AHIMA’s ARRA website
www.ahima.org/arra/

ARRA (the law itself)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f%3Ah1enr.txt.pdf

HHS ARRA Resources

FTC rules on Health Breach Notification
www.ftc.gov, under “quickfinder” click on “Privacy and Data Security”
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 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.*