The HHS Breach Final Rule Is Out - What’s Next?

Webinar
September 16, 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.
Harry Rhodes, MBA, RHIA, CHP, CHPS, is director of practice leadership at AHIMA, serving as a professional resource to HIM professionals and organizations, and the media on health information professional practice guidelines. Mr. Rhodes is an active member of the Health Information Technology Standards Panel (HITSP) serving on the Security, Privacy, and Infrastructure Technical Committee. He also received the Illinois Health Information Management Association's 2003 Professional Achievement Award and the 2003 Chicago Area Health Information Association Distinguished Member Award.
Table of Contents

Disclaimer ................................................................................................................... i
Faculty ...................................................................................................................... ii
Polling Question #1: Who’s Here ..................................................................................... 1
Our Agenda ................................................................................................................... 1
Eye on the Prize ............................................................................................................. 2
Challenge Defining: Access & Disclosure ..................................................................... 2
Breach as Defined in ARRA ............................................................................................. 3
Breach of Unsecured PHI ................................................................................................. 3
The Harm Threshold ....................................................................................................... 4
Polling Question #2: Harmful Breach ............................................................................... 4
Unsecured PHI ............................................................................................................... 5
Limited Data Set Not Protected ....................................................................................... 5
Defining the Scope of Information .................................................................................. 6
NIST Healthcare Guidance ............................................................................................ 6
HHS Regs Now Part of HIPAA ....................................................................................... 7
Effective Dates ............................................................................................................... 8
180 Day Pre-compliance Period ..................................................................................... 8
The Planning Process ..................................................................................................... 9
Revising BA Agreements ................................................................................................ 9
Agent versus Contractor .............................................................................................. 10
Staff Training, Education, & Rights 164.530 – Administrative Requirements ............... 10
Risk Assessment ........................................................................................................... 11
Risk Assessment Factors ............................................................................................. 11
Security Incident Response Team .................................................................................. 12
Polling Question #3: Response Team .............................................................................. 12
Notification Methodology ............................................................................................ 13
Required Notification Content ...................................................................................... 13
Notification Format & Media ......................................................................................... 14
Substitute Notice ........................................................................................................... 14
Delivery to Proxy/Personal Representative .................................................................... 15
Notification of the Media ............................................................................................. 15-16
Notification to Secretary - 164.408 ............................................................................. 16
Walking the Line .......................................................................................................... 17
Expanding Scope of Protected Data in State Breach Law ................................................. 17
Variation Between HHS, FTC, & State ......................................................................... 18
SB 20: California – Notification Letter Requirements .................................................... 18
Breach Notification Triggers ......................................................................................... 19
Resource/Reference List .............................................................................................. 19

Audience Questions ..................................................................................................... 20
Audio Seminar Discussion ............................................................................................. 20

(CONTINUED)
# Table of Contents

- Become an AHIMA Member Today! ................................................................. 21
- Audio Seminar Information Online ............................................................. 21
- Upcoming Audio Seminars .......................................................................... 22
- AHIMA Distance Education online courses .................................................. 22
- Thank You/Evaluation Form and CE Certificate (Web Address) ..................... 23

## Appendix ...................................................................................................... 24
  - Resource/Reference List ............................................................................ 25
  - CE Certificate Instructions
Polling Question #1: Who’s Here

Your “status” under HIPAA/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

Our Agenda

- Areas of HIM most affected by Breach Notification
- Identify unsecure PHI
- Understand risk assessment & related harm thresholds
- Security guidance for breach prevention
- What we should do first
- Open Q&A
“Moreover, requiring breach notification creates an incentive on all covered entities to invest in data security improvements in efforts to minimize the possibility of reportable data breaches.”

**Challenge Defining: Access & Disclosure**

From the Privacy Rule:

164.524 - Access by individuals to protected health information

- To inspect and obtain from the designated record set

160.103 - Definitions - Disclosure

- The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information
Breach as Defined in 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

Breach of Unsecured PHI

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

- Except where:
  - 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.
The HHS Breach Final Rule Is Out – What’s Next?

The Harm Threshold

- State laws require harm thresholds be met before providing notification.
- HHS clarifies - a breach is a use or disclosure that “compromises the security or privacy of the protected health information” means “poses a significant risk of financial, reputational, or other harm to the individual.”
- Must perform & document a risk assessment
- Burden of proof on CE/BA

Polling Question #2: Harmful Breach

Has your organization ever experienced an harmful breach event?

a) Never
b) Not that I know of
c) Yes, Financial harm
d) Yes, Reputational harm
e) Yes, Other harm to the individual
f) Yes, All of the above
**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).

- CE and BA that implement the specified technologies and methodologies with respect to PHI are not required to provide notification in the event of a breach of such information.

---

**Limited Data Set Not Protected**

- LDS Contains:
  - Dates
  - Zip codes
  - City/town

- High risk of possible re-identification

- If breached - risk assessment required

- LDS may only be used or disclosed as permitted by the Privacy Rule (data use agreements)
Defining the Scope of Information

- **NIST Guidance:**
  - **Data in motion**
    - Moving thru a network, includes wireless & e-mail
  - **Data at rest**
    - Databases, file systems, flash drives, memory
  - **Data in use**
    - CRUD – created, retrieved, updated, deleted
  - **Data disposed**
    - Includes discarded paper or recycled electronic media

NIST Healthcare Guidance

- **NIST SP 800-111, Encryption Guidance**
- **NIST SP 800-52, Transport Layer Security (TLS)**
- **NIST SP 800-77, Guide to IPsec VPNs**
- **NIST SP 800-113, Guide to SSL VPNs**

HHS Regs Now Part of HI PAA

- Rule adopted terminology to conform with HI PAA
- Expansion of certain HI PAA provisions to business associates
- Personal health record information protections
- Regional privacy advisors for HHS regional offices, education campaign
- Breach notification requirements

HHS Regs Now Part of HI PAA

- 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
Effective Dates

- HHS - September 23, 2009
- FTC - September 24, 2009
- Section 164.400 - Rule applies to breaches occurring on or after 30 days from the interim final rule publication date

180 Day Pre-compliance Period

- HHS to employ enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from the publication of the rule, or February 22, 2010
  - Will work with CE:
    - Technical Assistance
    - Voluntary corrective action
The Planning Process

- **BA contracting process**
  - Volume of BA contracts
  - Focus on required elements of BAA
- **Security administration**
  - Converting requirements into Policies and Procedures
  - Documentation requirements
- **Breach planning, training, and education**
  - Triggers
  - Investigation
  - Communication

Revising BA Agreements

- **All BAAs should be reviewed**
- **Two difference opinions:**
  - No need to revise if BAA contains clause that BA will comply with “all present and future laws and regulations.”
  - All BAA must be updated to address requirements of breach notification rule.
Agent versus Contractor

- Federal common law of agency
- BA as agent – breach imputed to CE; 60 days begins with discovery
- BA as independent contractor – 60 days begins with notification of CE
- Revise notification timing in BA contracts
- BA provides CE immediate notification of breach
- FU with detailed information about individuals

Staff Training, Education, & Rights
164.530 - Administrative Requirements

- CE required to train workforce on breach policies and procedures, in line with their duties (policies and procedures must be complaint with rules)
- As employees change duties, they must be trained within a reasonable period of time of the change
- CE must establish a process to allow employees to complain about CE’s security breach policies and procedures
- CE must establish an employee sanctions procedure for breach notification non-compliance
- CE must establish a policy to protect employees exercising their rights to file complaints, and may not require individuals to waive any of these rights
- CE demonstrate compliance through documentation sufficient to support burden of proof
Risk Assessment

- Prepare policies and procedures for the detection and investigation of data breaches, for determining whether they are reportable, and identifying the individuals involved in mitigation.
- A premium is placed on effective detection and investigation of possible breaches.
- CE & BA must document risk assessments and demonstrate, if necessary, that no notification was required.

Risk Assessment Factors

- To whom the data was disclosed
- Whether or not immediate mitigation was possible
- Type and amount of information breached
Security Incident Response Team

- HIM
- Privacy officer
- Information systems
- IT security
- Risk management/ legal
- Physical security
- Admitting staff
- Nurse auditors
- Compliance staff
- Clinicians involved in chart clean-up issues
- Administration

Polling Question #3: Response Team

Does your organization have a Security Incident Response Team established under HIPAA?

a) Yes
b) No
### Notification Methodology

- Following discovery of a breach of unsecured PHI 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
- 60 day discovery calendar starts the first day the CE is aware of the breach or would have been aware had it exercised reasonable diligence.
- Notification must be made “without unreasonable delay” and never later than 60 calendar days after discovery, unless there’s a law enforcement delay

### Required Notification Content

- Written in Plain language;
- 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.)
Notification Format & Media

- 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)
- Provide translating the notice into frequently encountered languages.
- Make notice available in alternate formats, such as Braille, large print, or audio.

Substitute Notice

- Substitute notice should be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information for one or more affected individuals.
- For fewer than 10 individuals e-mail or telephone call is appropriate.
- For 10 or more individuals substitute notice through the Web site or media requires the covered entity to have a toll-free phone number, active for 90 days.
Delivery to Proxy/Personal Representative

- Notice to parent if individual is a minor
- Notice to proxy or personal representative if individual lacks legal capacity due to mental or physical condition
- Notice to next of kin or personal representative if individual is deceased

Notification of the Media

- If breach involves 500 or more individuals of any one State or jurisdiction
- BA with multiple CE is only required to report breach of 500 or more occurring at one CE
- Notice provided to prominent media serving State or Jurisdiction
- Intended to supplement not substitute the individual notice
Notification of the Media

- Must be within the 60 days following discovery
- Media notice differs from substitute media notice

Notification to Secretary - 164.408

- 500 or more individuals - immediately
- Less than 500 individuals - annually
- In manner specified on HHS Website
- Notification to Secretary still required if 500 or more individuals split between more than one State
- CE must maintain internal log or documentation for 6 years
Walking the Line

Balancing breach response between:
- HHS Breach Notification Rule
- FTC Breach Notification Rule
- State Breach Notification Laws

Expanding Scope of Protected Data in State Breach Law

- Personal information
- Individually identifiable health information
- Health insurance information
- Genetic information
- Biometric data
Variation Between HHS, FTC, & State

- Definition of protected information
- Identification of individuals and/or agencies to be notified
- Process for breach notification
- Triggers for reporting and providing consumer notice of security breach

SB 20: California - Notification Letter Requirements

- Whether there was a delay in notification because of investigations
- Estimated number of persons affected
- Contact info for credit reporting agencies
Breach Notification Triggers

- Acquisition-based triggers
- Risk-based triggers

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
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 AHI MA Member Today!

To learn more about becoming a member of AHI MA, please visit our website at www.ahima.org/membership to join now!

AHI MA Audio Seminars and Webinars

Visit our Web site http://campus.AHI MA.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**

Curriculum Approval to Accommodate ICD-10-CM/PCS  
**October 13, 2009**

Transitional Instructional Design to Accommodate ICD-10-CM/PCS  
**October 15, 2009**

---

**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:


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.
Resource/Reference List

www.ahima.org/arra/

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

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.*