# Breach Risk of Harm Assessment

## Safeguarding Health Information: Building Assurance through HIPAA Security

**Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA**

**Wednesday, May 11, 2011**

**3:00 pm – 3:45pm**

AHIMA
American Health Information Management Association®

# Our agenda today

- Breach notification one element of larger Security goal
- Emerging risk of harm assessment models
- Review of covered entity assessment practices
- Learn investigation practices, appropriate action steps, notification requirements, OCR reporting, and sanctions for staff
- Facing risk of harm assessment challenges

AHIMA

# Breach Notification Final Rule Pulled

- Published on August 24, 2009.
- Effective on September 23, 2009.
- 60 day comment period – HHS received 120 comments.
- Final Rule sent to Office of Management and Budget (OMB) on May 14, 2010.
- July 29, 2010 - HHS is withdrew final rule from OMB review.
  - Complex issue that requires further consideration.
- Interim Final Rule is still in effect

AHIMA

# THE BREACH NOTIFICATION RULE

- **Creates a requirement that "risk of harm" threshold assessment will be performed –significant risk of financial, reputational or other harm to the individual.**

- **Requires that the risk assessment be documented. Even if a decision is made not to issue a breach notification.**

# Breach Notification Triggers

- Acquisition -based triggers
  - Trigger present in majority of State breach notification laws.
- Risk-based triggers
  - HITECH “risk of harm” threshold requirement.

# The Harm Threshold

- HITECH requires harm threshold assessment to be performed to determine risk of harm.
- 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

AHIMA

# Improved Security Administration is the Ultimate Goal

"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."

AHIMA

# HIPAA Security Rule - 45 CFR 164.308(a)(6) - Requirements

- **Identify and respond to suspected or known security incidents;**
- **Mitigate, to the extent practicable, harmful effects of security incidents that are known to a covered entity; and**
- **Document security incidents and their outcomes.**

# Determining Harm is Subjective

**"The definition of harm is unique to each case and each patient."**

AHIMA

# Low-risk HIPAA violations- exempt from breach notification

- HITECH Guidance: Breach does not include
  - Good faith, unintentional acquisition, access, or use of PHI by a workforce member of a CE, BA, or BA subcontractor.
  - Inadvertent disclosure to another authorized person within the entity or its business associates.
  - Recipient could not reasonably have retained the data.
  - Data is limited to a limited data set that does not include dates of birth or zip codes.

# UNSECURED PHI

- **“Unsecured” PHI means PHI that “is not secured through the use of a technology or methodology specified by the Secretary”**
- **If a breach involves “secured” PHI, no notice or risk assessment is needed.**
- **Encryption plus destroyed plus ????**

AHIMA

# NCHICA Risk Assessment Tool

**North Carolina Healthcare Information and Communications Alliance. (NCHICA)**

"HITECH Act Breach Notification Risk Assessment Tool":

- Scoring system ranks incidents from low to high
- Sorts by variables of HIPAA violation:
  - Recipients
  - Circumstances of release
  - Disposition of information

- Provides a framework for assessment

# Capturing Investigation Details

- Incident / Name
- Date of event
- Number of individuals effected
- Point of Contact
- Phone number
- Brief Summary / Findings
- Final Decision
- Source of Incident: Who was responsible for the inappropriate access, use or disclosure (incident)? Business Associate?

AHIMA

# Determining if a Reportable Breach has Occurred

Does the incident violate the HIPAA Privacy rule?


Does it involve unsecured or unencrypted PHI?


Does the incident qualify as an exception?


Does this data breach "pose a significant risk of financial, reputational, or other harm to the individual affected?

AHIMA

# Risk of harm assessment variables

- Method of Disclosure
- Recipient(s)
- Circumstances of release
- Disposition (what happened to the information after the initial disclosure)
- Additional Controls

# Scoring Methodology

| Variable | Options | Score |
|---|---|---|
| Circumstances of Release | • Unintentional disclosure of PHI | 1 |
| | • Intentional use/access w/o auth<br>• Intentional disclosure w/o auth<br>• Theft – Device targeted<br>• Lost | 2 |
| | • Using false pretense to obtain or disclose<br>• Obtained for personal gain/malicious harm<br>• Hack<br>• Theft - data targeted | 3 |

# Risk of Harm Assessment Scoring

- Meant to guide your decision – not make your decision
- The range of scoring is 6 -18
- The scoring is subjective by design
  - entity should consider:
    - their own policies,
    - technical safeguards/constraints,
    - mitigation strategies,
    - and details specific to the incident reviewed.

# HIPAA Collaborative of Wisconsin – HIPAA COW

**Composed of:**

- **Examples of Breaches of Unsecured PHI**
- **Breach penalties**
- **Sample notification letter to patient**
- **Sample notification letter to Secretary of HHS**
- **Sample media notification statement/release**
- **Sample talking points**
- **Examples of violations and notification recommendations**
- **Sample breach notification log**
- **Risk assessment analysis tool**

AHIMA

# Maintenance of Breach Information/Log

In addition to incident reports created

- Description of what happened
  - Date of breach
  - Date of discovery
  - Number of patients affected
- Description of types of unsecured information breached
- Description of notification action taken
- Steps taken to mitigate breach

# Risk Assessment Checklist

- Was PHI breached unsecured ?
- Was PHI breached more than the minimum necessary?
- Was the PHI received and/or used by another HIPAA CE?
- Were immediate steps taken to mitigate breach?
- Was the PHI retrieved prior to improper use?
- Does the breach pose significant risk?
- Did improper use/disclosure only include name?
- Was information  stripped of limited data set identifiers?
- Is there a low risk of re-identification
- Was access unrelated to the workforce members duties?

AHIMA

# Aurora Health Care
## Breach Notification
## Assessment of Harm Guidance

**Each case is fact specific.**

**Analyze the violation from the following perspectives:**

- **Consider the recipient of the PHI and their reaction**
- **Consider the content of PHI**
- **Consider assurances received**
- **Consider motive**
- **Consider contact to the individual who is the subject of the PHI**

AHIMA

# Elements of a Harm Threshold Risk Assessment

- To whom was the information disclosed (or made accessible)?
- Who misused the information?
- What information was it? And how much PHI was involved?
- Likelihood the information could be misused
  - Calculate the Exposure Factor value.
    - Quantitative loss value
    - Qualitative lose value
- What was done to mitigate the potential harm?

AHIMA

# Consider the recipient of the PHI and their reaction

- What was their attitude?
- Protecting PHI a priority?
- Following discovery did they initiate contact?
- Realization of what they had.
- What is their relationship to the individual?
- Willingness to return the PHI?
- Unintended recipient or did they seek out the information?
- Was the recipient another covered entity?

AHIMA

# Consider the content of PHI

- What identifiers are present?
- Was the SSN disclosed?
- Was there detailed content disclosed? Any content typically considered "sensitive"?
- Is the PHI older, or current?
- In cases of family member as the recipient, is it likely that family member is already aware of the information?

# Consider assurances received

- Were immediate steps taken to mitigate the risk?
  - Not further used or disclosed
  - Immediately destroyed
  - Immediately returned
- Did the violation involve:
  - Covered entity
  - Another patient
  - Non-covered entity/business

AHIMA

# Consider motive

- Was the access or disclosure a mistake?
- Was the access or disclosure intentional?
- Was the access or disclosure intentional for self-serving, malicious, or harmful reasons?

AHIMA

# Contact the individual Weigh their reaction

When inconclusive information is available to make a harm determination; contacting the individual maybe an option.

- Opportunity to measure individual's reaction.
- When impermissible access involves a family member; individual may already be aware.
- Individual contact provides the opportunity to make apologies personal.

# Tools Provide a Common Ground

**Formal risk of harm assessment tools provide:**

- **Formal decision tree**
- **Consistent application**
- **Formal metrics**
- **Recordable methodology**
- **Flexible application for both State and Federal risk of harm assessments**

AHIMA

# Consistent Documentation

**Document risk analysis decision process; should breach notification decision be question.**

- **Formal**
- **Consistent**
- **Measurable**
- **Structured**
- **Backed by evidence**
- **Transparent**
- **Describes incident objectively**

AHIMA

# Your Next Steps Should Be

- Identify a process to carry out HITECH breach incident risk of harm assessments.
- Identify legal and breach services resources in advance.
- Selected Harm Threshold assessment tool that will quickly provide a consistent, reliable and valid determination.
- Accurately documenting the harm threshold assessment process.

AHIMA

# Ministry Health Care

## Breach Notification
## Assessment of Harm Guidance

- Utilize Existing Administrative Guidance and Documents
  - Security Incident Response/Reporting
  - HIPAA Sanctions/HR Corrective Action
- Supporting Forms
  - Investigation Report
  - Log
- Legal Counsel Review

AHIMA

# Policy – Supporting Documentation

- Investigation Report
- Log of Privacy Complaints/Concerns
- Breach Notification Template Letter

# "Form" Follows Function

- **Investigation Report**
  - Form Fosters Accurate and Complete Documentation
  - Provides Consistency
  - Supports HR Sanctions
  - Demonstrates Due Diligenc
  - OCR Reporting Tool

AHIMA

# Log of Complaints/Concerns

- Number
- Date
- Type
- Patient Name
- Explanation
- Organization
- Privacy Officer
- Mitigation
- Action/Resolution
- Breach Status
- OCR Reporting Date (if applicable)

*Maintained on Excel Spreadsheet*

AHIMA

# Investigative Team

- **Ad Hoc (Based on Scope)**
  - **Administration**
  - **Human Resources**
  - **Risk Management**
  - **Others as Needed**
- **Security Incident Response Team**

# Name a Lead Breach Investigator

- Manages breach investigation
- Facilitates breach notification processes
- Coordinates security incident response team
- Sole external spokesman for organization
- Oversees completion of risk assessment
- Manages breach investigation documentation
- Oversees six year retention of documentation
- Privacy officer, security officer, & risk manager

AHIMA

# Investigation

- Review the circumstances regarding the breach, conduct an investigation, complete a risk assessment, and determine necessary actions including involvement of enterprise, local, and legal counsel resources
- Coordinate communications with all involved in the investigation, including patients, licensing and accrediting organizations, state and federal governmental agencies, etc.

# Risk Assessment – Best Practice?

- If unable to determine "harm" based on type of information disclosed, consider contacting the patient to discuss the situation and ascertain their perception of "harm"
  - Examples: Collection agency inadvertently notifies John A. Smith, Sr. of balance due for son (John A. Smith, Jr.); eye appointment reminder made to wrong John A. Smith; home health supplies delivered to wrong John A. Smith patient, etc.). In these cases, information disclosed is minimal and may be perceived by the patient as not harmful.

*The unauthorized access, use, or disclosure of certain data elements should always be considered "harmful." Examples include diagnoses, procedures, Social Security number, DOB, etc.*

AHIMA

# Sanctions – Workforce Members

- Considerations
  - Factors to Consider
- Level of Occurrence
  - Categorize
- Recommended Action
  - Cumulative Factor
- Whistleblower / Retaliation

# Sanctions – Business Associates

- **Expectations Defined in Business Associate Agreement**
- **Ultimate Sanction – Termination of Relationship**

# Lessons Learned

- Totally Underestimated Impact on Daily Job Responsibilities
  - 2008: 38 Internal Privacy Investigations
  - 2009: 98 Internal Privacy Investigations (48 Last Q)
  - 2010: 200+ Internal Privacy Investigations
- Initial Approach to Addressing "Harm" Was Probably Too Conservative
- Partner with Collection Agency to Address Processes, Policies, Etc.

AHIMA

# Lessons Learned

- **Reach Out to Peers for Brain-Storming Best Practices**
- **Be Open to New Directives / Interpretations**
  - **Contacting Patients to Determine "Harm"**
  - **Employee Breach Attestation**

# Lessons Learned

- Mitigation
  - Patient Requests
  - Organizational Offerings
- Bookmark/Print Examples from Published Breaches
  - Notices
  - Press Releases
  - Website Communications
  - External Resources (Credit Card Agencies)

AHIMA

# Ongoing Challenges

- **Patient Billing Errors Resulting in Disclosures**
  - **Jrs/Srs**
  - **Adult Children**
  - **Same Name**
- **Identification and Reporting**
- **Access Audits**

# Model Data Breach Response Resources

**NCHICA Breach Notification Risk Assessment Tool**

http://www.nchica.org/

**HIPAA Collaborative of Wisconsin – "HIPAA-COW"**

www.hipaacow.org

**AHIMA – "Data Breach Investigation and Mitigation Checklist."**

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_036245.pdf

# 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
  - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1233&parentname=CommunityPage&parentid=3&mode=2&in_hi_userid=10741&cached=true

# Contact information

**Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA**

**Director Practice Leadership**

**harry.rhodes@ahima.org**

# Questions