
ARRA and HITECH Panel

February 23, 2010

- Kathryn Roe, Principal, The Health Law Consultancy
- Sharon Anolik, Director, Chief Privacy Official, Director of Corporate Compliance & Ethics, Blue Shield of California
- Jeannette Frey, Privacy Officer, Fallon Community Health Plan

1

The Program

- HITECH Overview
- HITECH Privacy & Security
 - Breach Notice Requirements
 - Business Associate Requirements
- Q&A

2

HITECH Overview

Kathryn Roe
Founding Principal
The Health Law Consultancy

The Start

- 1996—HIPAA-AS

Health Insurance Portability & Accountability Act of 1996, includes Administrative Simplification

- Directs Dep't of Health & Human Services (HHS) to adopt national health system standards to:
 - Conduct electronic administrative and financial transactions
 - Protect health information privacy and security
- Goal: Encourage development of electronic health information system

The Step Forward

- 2004—Executive Order 13335 establishes Office of the National Coordinator for Health Information Technology (ONC) in HHS
 - Charter: Lead development and implementation of nationwide interoperable HIT infrastructure
- Goal: *Majority* of Americans to have access to electronic health record (EHR) by 2014

The Journey Accelerates

- 2009—ARRA includes HITECH

Health Information Technology for Economic & Clinical Health Act, part of American Recovery and Reinvestment Act of 2009
 - ONC authorized and assigned leadership to implement HITECH
- Goal: *All* Americans to have access to EHR by 2014

HITECH Roadmap

- HIT promotion through standards
- HIT testing for certification
- HIT funding through grants and loans
- HIT incentives through Medicare and Medicaid
- HIT privacy and security enhancement

ONC Job 1: Support EHR Adoption

- Fund infrastructure that supports provider EHR adoption and implementation
 - \$634,000,000 for Regional HIT extension centers (RECs)
 - Nationwide network of 70 RECs
 - Technical assistance for PCPs and other providers
 - \$118,000,000 for HIT workforce training
 - Curriculum development, training, competency examinations
 - 45,000 new qualified HIT workers

ONC Job 2: Support HIE

- Establish infrastructure for secure health data flow to point of care
 - \$564,000,000 for state health information exchanges (HIEs)
 - Develop intra- and inter-state HIE capabilities
 - Backbone for nationwide electronic health information highway
 - Enhanced federal privacy and security protections
 - Strengthened HIPAA-AS—added terms, broadened reach, toughened enforcement, authorized more regulations
 - Included in EHR meaningful use definition

ONC Job 3: Support EHR Meaningful Use

- Define and incent provider EHR use to full potential
 - Medicare incentives
 - Extra provider reimbursement for EHR meaningful use starting 2011
 - Reduced provider reimbursement for no EHR meaningful use starting 2015
 - Medicaid incentives
 - Separate “carrot” program (no “stick”)
 - Combined federal/state effort

Overarching Federal Goal

- HIPAA-AS, EO 13335, HITECH advance overarching federal goal:
 - Effective health system that uses HIT to produce better national health at lower national cost
 - Improved individual and population health outcomes
 - Increased transparency and care efficiency
 - Enhanced ability to study, improve care delivery
- **Not** goal simply to have high-tech health system

HITECH's Message for You

- Understand HITECH's "why's" to inform HITECH compliance
- Health information privacy and security critical to achieving effective health system
 - Confidence in health information privacy and security essential to patient and provider HIT acceptance
 - No confidence spells resistance to more effective, efficient, coordinated health system

HITECH Breach Notice Requirements

Sharon A. Anolik, Esq., CIPP
Chief Privacy Officer, Director of
Corporate Compliance & Ethics
Blue Shield of California

Breach Notice Requirement

- Breach occurs in the event of unauthorized PHI acquisition, access, use or disclosure that “compromises the security or privacy” of the data [sec. 13400(1)(A)]
 - Excludes unintentional acquisition, access or use by employee or agent under the CE/BA’s authority (in good faith and within scope of relationship)
 - Excludes inadvertent disclosure between authorized individuals at the same facility
 - For both exclusions: PHI can’t have been further acquired, accessed, used or disclosed
- Applies to Covered Entities (CE) and Business Associates (BA) that hold, use or disclose unsecured PHI
 - Unsecured means not secured per an HHS-specified technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals
 - Not limited to electronic PHI; this covers paper and other media

Exceptions

HHS Guidance clarified the exceptions as follows:

- An unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition was in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the privacy rule.
- An inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of the privacy rule.
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom disclosure was made would not reasonably have been able to attain such information.

Risk of Harm Analysis

“Compromises the security or privacy of the PHI” means that the breach poses a “significant risk of financial, reputational, or other harm to the individual”

- Therefore notification is necessary only if the breach poses a significant risk of harm to the individual
- CEs and BAs must conduct and document their risk of harm (ROH) analysis to support their determination of whether or not notification is required
- Considerations
 - Documentation is time consuming
 - No calibration across the industry
 - Size/type of the disclosure is irrelevant; documented ROH analysis is required for all
 - Will ROH documentation be litigation fodder later? Should it be done under Attorney Client Privilege? Who should conduct these analyses?

Examples of differing/important facts when conducting an ROH analysis

- PHI is impermissibly disclosed by one CE to another
- A CE takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining satisfactory assurances from the recipient (e.g. a confidentiality agreement that the information will not be further used or disclosed or will be destroyed)
- A laptop is lost/stolen and then recovered, and forensic analysis shows that it was not opened, altered, transferred or otherwise compromised
- Type of information may also reduce risk, e.g. name and the fact that individual received services from a hospital is different from the type of services, or specialized facility, or other more sensitive elements (like SSN)

Timeframe for Notification to Individuals

“Without unreasonable delay” and in no case later than 60 calendar days after discovery of breach (unless law enforcement requires delay)

- CE must notify individuals and BA must notify CE within this time
- Breach is deemed discovered when CE or BA knows or should reasonably have known of breach
- Clock starts ticking when 1st workforce member or agent knew, or by exercising reasonable diligence should have known
- CE or BA has knowledge when employee, officer, or other agent knows or should reasonably have known of breach (does not include breach perpetrator)
- Considerations:
 - Add contract language stating time frame in which BA must notify CE
 - Training workforce to notify your Privacy/Compliance/Legal department immediately upon learning of a breach is more important than ever

Notice Content for Individuals

- Description of breach
- Date(s) of breach/discovery
- Description of “breached” PHI
- Protective steps for affected individuals
- Description of CE’s response
- Contact procedures in order to get more information

- Considerations
 - What are protective steps for disclosed PHI?
 - Credit monitoring may not be helpful unless social security number is include in the breach

Reporting Requirements

- Notify impacted individuals in writing

- Notify the Department of Health and Human Services (HHS)
 - Annually, or immediately if 500+ individuals are affected

- Notify the media if 500+ individuals in one state are affected

- Place a notice on the company website in some situations

Note: These are in addition to the standard HIPAA accounting of disclosure requirements, and any other contractual or state-required notifications

What can we do to prepare?

- Train, Train, Train! Not just on security and privacy, but specifics about security breach—examples of what constitutes a breach, how to report it, and the importance of immediate action
- Prepare or revise your Incident Response Plan to include the new security breach provisions
- Distinguish procedures for PHI breach with and without SSN
- Craft template notification letter that meets the highest standard

What can we do to prepare? (cont.)

- Consider alerting state AGs when a breach includes a significant number of residents, or when a significant number of SSNs are involved
- Evaluate statutory and contractual obligations beyond HITECH
- Don't forget: even if you make a determination that there is no risk of harm under HIPAA breach rules, you might still need to notify under state laws
- Address security breach in all future contracts and those up for renewal
- Consider amending existing contracts

HITECH Business Associate Requirements

Jeannette Frey, JD
Privacy Officer
Fallon Community Health Plan

New Requirements for Business Associates: Security

- BAs must comply with the administrative, physical, and technical safeguards of the security regulations.
- BAs must have policies and procedures in place as required by the security regulations.

New Requirements for Business Associates: Privacy

- BAs may only use or disclose PHI as permitted by the business associate agreement
- BAs are required to have business associate agreements in place with covered entities in the same way covered entities are required to have business associate agreements in place with BAs
- BA must take steps to cure a breach of the business associate agreement by the covered entity. If unsuccessful, the business associate must either terminate the contract or report the covered entity to HHS

New Requirements for Business Associates: Liability

- Any violations of the new requirements are considered direct violations of the privacy and/or security regulations
- Business associates are subject to direct enforcement and civil and criminal penalties for violations
- No longer simply a contractual obligation

New Requirements for Business Associates: Impact to Covered Entities

- Any new privacy and security requirements within HITECH that apply to covered entities will also apply to business associates and must be incorporated into the business associate agreements.
- What does this mean? What are the new privacy and security requirements that apply to covered entities?
 - BA's new requirements
 - Breach notification/Reporting requirements
 - Minimum Necessary
 - Marketing
 - Accounting of Disclosures
- HHS has stated they will be issuing guidance on what must be incorporated into the business associate agreement

What can we do to prepare?

- Prepare for a significant effort
- Work with counsel to determine whether agreements need to be updated, with what provisions, and when:
 - What exactly is required by the law to be incorporated into business associate agreements?
 - Do you want to wait for HHS guidance?
 - What do you want to include that might not be required by law, e.g. indemnification, insurance, specific security requirements, breach notification?
 - Do your current agreements have a provision that automatically incorporates new regulatory changes?
- Expect business associates to be savvy and proactive

What can we do to prepare?

- Update business associate agreement template
- Inventory business associates
 - Identify what version business associate agreement they have in place and the structure of that agreement (e.g. stand alone, appendix, incorporate into a service agreement)
- Work with business areas prior to communicating with business associates to determine the appropriate approach, identify high risk business associates, and prioritize
- Mail updates, negotiate contracts, track

Q & A

Contact Information

- Kathryn Roe - kroe@hlconsultancy.com
- Sharon Anolik - sharon.anolik@blueshieldca.com
- Jeannette Frey - jeannette.frey@fchp.org