



## 2010 Minnesota e-Health Summit

### Break out Session # 4

#### Explore Evolving Policy in HIT Privacy and Security

June 17, 2010

**Laurie Beyer-Kropuenske, JD, Session Moderator**  
Director, Information Policy Analysis Division  
MN Department of Administration  
MN e-Health Advisory Committee Member  
Minnesota e-Health Initiative



## Session Goals & Objectives

- Learn about the Minnesota e-Health Initiative and the Minnesota Privacy and Security Program
- Discuss potential implications of the new HITECH privacy & security requirements
- Understand the new HITECH privacy & security requirements through case studies



## Session Speakers

- **Patricia Carter, JD**  
Senior Counsel  
HealthPartners  
Minnesota e-Health Workgroup Member
- **Lois Dahl, MBA, RHIA, CHPS**  
Director, Information Privacy  
Fairview Health Services  
Minnesota e-Health Workgroup Member
- **David P. Lawton, RN, PhD**  
Project Officer – Midwest States  
ONC/Office of State and Community Programs



## The Minnesota e-Health Initiative

### A public-private collaboration established in 2004

- Legislatively chartered
- Coordinates and recommends statewide policy on e-Health
- Develops and acts on statewide e-health priorities
- Reflects the health community's strong commitment to act in a coordinated, systematic and focused way



“**Vision:** ... accelerate the adoption and effective use of **Health Information Technology** to improve healthcare quality, increase patient safety, reduce healthcare costs, and enable individuals and communities to make the best possible health decisions.”

Source: e-Health Initiative Report to the MN Legislature, January 2004



## Minnesota Privacy and Security Program

- Established as part of the Minnesota e-Health Initiative and the e-Health Advisory Committee
- Engages in and monitors state and national privacy & security policy development
- Addresses privacy & security topics and issues raised by interested parties and in workgroups of the e-Health Advisory Committee
- Beginning 2010-2011, will be renamed the Privacy, Legal and Policy Workgroup



## Patricia Carter, JD

Senior Counsel, HealthPartners  
Minnesota e-Health Workgroup Member



## Overview

- The Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Part of the American Recovery and Reinvestment Act (ARRA or Stimulus Bill)
  - Signed by President on February 17, 2009
- HITECH contains numerous changes to privacy & security requirements that impact HIPAA
- Focus today on
  - Business Associate Agreements
  - Analysis of Breach Situations
  - Regulatory Updates



## HITECH Business Associate Issues

- HITECH provisions regarding BAs were effective February 17, 2010
- BAs must comply with the key provisions of the HIPAA Privacy Rule & Security Rule
- BAs become directly liable under HIPAA and subject to HIPAA civil and criminal penalties



## Business Associate Agreements

- HITECH BA Requirements “shall be incorporated into” business associate agreements
  - Incorporated by operation of law?
  - Requires BAAs to be amended to incorporate new HITECH obligations?
- To amend or not to amend, that is the question



## To Amend or Not to Amend?

- Possible approaches
  - Not amend, because it's a lot work and not required by the statute
  - Amend, even though it is a lot a work, because it is required by the statute
  - Wait for clarifying regulations, then decide
  - Amend because you want to clearly set expectations and allocate accountabilities
    - Amend all BAAs, or
    - Amend key BAAs, and take a wait-and-see approach on the others
- Get legal advice



## Thoughts on Drafting an Amendment

*Dear, we need to talk about our relationship . . .*

- Significant changes in the relationship between a Covered Entity and a Business Associate
- What needs to be said (or made part of a BAA amendment)?



## Thoughts on Drafting an Amendment

*Breaking the Ice - there's something we need to discuss*

- Preliminaries
  - Introduce the topic: Explain what the HITECH Act is and that it imposes new requirements on Business Associates with regard to privacy & security
  - Be clear about applicable Effective Dates:
    - February 17, 2010 for key HITECH provisions
    - May be later or earlier for certain other provisions



### Thoughts on Drafting an Amendment

*Things have to change or we can't keep seeing each other*

- Echo the language of the Statute

Security Regulations. Effective on and after February 17, 2010:  
(a) 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 apply to Business Associate in the same manner that such sections apply to Covered Entity, and  
(b) The additional requirements of Section 13401 of the HITECH Act that relate to security and that are made applicable with respect to covered entities shall also be applicable to Business Associate as a business associate of Covered Entity.

Privacy Regulations. Effective on and after February 17, 2010:  
(a) Business Associate may use and disclose Protected Health Information only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 C.F.R. § 164.504(e), and  
(b) The additional requirements of Section 13404 of the HITECH Act that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to Business Associate as a business associate of Covered Entity.

- Go into detail on some or all of these “additional HITECH requirements”



### Thoughts on Drafting an Amendment

*Because I said so, that's why*

- Minimum necessary determinations – eff. 2/17/10
  - New standards for making minimum necessary determinations

- Under the interim standards in HITECH – Limited Data Set approach
  - Under subsequent guidance from DHHS
- The disclosing party makes the minimum necessary determination, whether it's the BA or the Covered Entity (CE)



### Thoughts on Drafting an Amendment

*Are you hiding something?*

- Encryption – Secured PHI

- Under the new breach notification standards, whether notices are required depend in part on whether the PHI was encrypted according to certain standards (is not “unsecured PHI”)
  - Does the CE impose encryption obligations on BA?
- Variations in approach
  - Encrypt all PHI (at rest, in motion, disposed of)
  - Encrypt PHI transmitted by BA to a third party or Covered Entity
  - Rely on the BA now being subject to HIPAA Security Rules (which address but do not mandate encryption)



### Thoughts on Drafting an Amendment

*Tell me who you've been with*

- Accounting of Disclosures

- HITECH specifically permits a CE to either:
    - Respond to an individual's request for an accounting with an accounting of its own disclosures plus those of its BAs, or
    - Provide an accounting of its own disclosures and a list of BAs, who then must respond directly to individual
- Address the expansion of the accounting requirement to TPO?



**Thoughts on Drafting an Amendment**

*Just tell me what really happened*

- BA Reporting Breaches to a CE
  - Timing of reporting by BA to CE
    - HITECH requires BA to report within 60 days, but this may run concurrently with CE's obligation to provide individual notification within 60 days
    - CE may want to ask for much shorter period
  - Prior to HITECH, BA agreements imposed a requirement for the BA to report unauthorized uses and disclosures and security incidents to CE
    - Coordinate these provisions with Breach notice provisions



**Thoughts on Drafting an Amendment**

*We need to communicate*

- BA Reporting Breaches (*continued*)
  - What information does the BA need to provide?
    - Cross-reference to regulations for details or spell out?
  - Details about reporting process – e.g., to privacy officer of CE?
- Breach Investigation
  - Specify that the parties agree to cooperate in any reasonable investigation of a Breach?



**Thoughts on Drafting an Amendment**

*This is gonna cost you*

- Costs Related to a Breach by BA
  - Not addressed in HITECH or Breach Regs
  - Should BA reimburse CE for the reasonable costs CE incurs in
    - Notifying individuals of a breach by BA?
    - Investigating the incident?
    - Mitigating harm?



**Lois Dahl, MBA, RHIA, CHPS**

Information Privacy Director

Fairview Health Services

Minnesota e-Health Workgroup Member



## Breach

- A *privacy breach* is defined as unauthorized acquisition, access, use or disclosure of unsecured protected health information (PHI) that compromises the security or privacy of PHI.
- If a breach constitutes a violation of the HIPAA privacy rule, a risk assessment must be performed and documented.



## Breach Notification for Unsecured Protected Health Information

Effective September 23, 2009, HIPAA covered entities and their business associates are required to comply with mandatory patient notification of any unauthorized acquisition, access, use, or disclosure of their "unsecured PHI" that compromises the privacy or security of such information.



## Risk Assessment

- Elements needed to perform assessment:
  - Date of the breach
  - What was disclosed
  - To whom
  - Steps taken to eliminate or reduce the risk of harm
- Does the breach meet one of the exceptions?



## Exceptions

- Good faith belief that unauthorized person was not able to retain the information
- Unintentional access or acquisition by a workforce member or BA and no further impermissible use or disclosure
- Inadvertent disclosure to others similarly authorized to access PHI at a BA, another covered entity or within OHCA



## Breach Notification

- Notification must include:
  - Brief description of what happened including the date of the breach;
  - Steps the individual should take to protect themselves from potential harm;
  - Description of what the CE is doing to investigate, mitigate and prevent reoccurrence;
  - Contact information for questions.



## Breach Notification

- Large or single, patient must be notified in writing within 60 days
- Breaches of more than 500 patients must be reported to DHHS immediately and DHHS will post the name of the offending entity on its website
- Annual report to DHHS for small breaches



## Other Breach Notification Requirements

- Breaches of 500 or more patients within the same area must be reported to prominent media outlets.
- If sufficient contact info is not available for 10 or more individuals, conspicuous notice must be placed on the homepage of the CE's website (must remain there for 90 days) or put in major print or broadcast media.



## Scenarios

- See Handout
- Each situation is different

*Questions?*



**David P. Lawton, RN, PhD**  
Project Officer – Midwest States  
Office of the National Coordinator for Health IT  
Office of State and Community Programs



## HITECH Regulatory Updates Since the Last Minnesota e-Health Summit

- Delegation of Security Rule enforcement to OCR – Aug. 2009
- Breach Notification – Interim Final Rule – Aug. 2009  
*<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>*
- Enforcement Rule Interim Final Rule – Oct. 2009  
*<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfiifr.pdf>*
- Draft Guidance on Risk Analysis – May 2010  
*<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf>*
- Accounting of Disclosures RFI – May 2010  
*<http://edocket.access.gpo.gov/2010/pdf/2010-10054.pdf>*



## Previews of Coming Attractions HITECH Regulatory Agenda

- HHS Spring Regulatory Agenda
  - Final Breach Notification Rule – April 2010
  - Omnibus Privacy NPRM – May 2010
  - Final Enforcement Rule – Aug. 2010
  - Accounting of Disclosures NPRM – June 2010
  - Final GINA/HIPAA Rule – Aug. 2010
- Some Other HITECH Dates
  - Minimum Necessary Guidance – Aug. 2010
  - Sale of PHI NPRM – Aug. 2010
  - Guidance re de-identification of PHI – Feb. 2010



# Minnesota e-Health Summit 2010

## Breakout Session 4: Privacy and Security Issues

### HITECH Breach Notification Analysis Case Studies

**Scenario 1:** Lab results are being faxed to the patient's primary care physician. The wrong fax number is used and the recipient is (a) a dentist office, or (b) a drycleaners. Recipient calls and notifies you right away, and says they are shredding the fax (or mailing it back to you). Does it matter if it was the dentist or the drycleaners? Does it matter what type of test?

**Scenario 2:** A business associate sends your PHI to the wrong recipient. The BA notifies you and states that the envelope was returned unopened. Is this a breach? What factors would need to be considered if the envelope was returned, but had been opened? If it is a breach, do you report it or does the BA since HIPAA now applies to BAs?

**Scenario 3:** A patient is discharged from the facility and the next patient in the room finds the previous patient's order for a 72 hour hold for chemical dependency. It appears that the previous patient was responsible for placing the document out of sight inside a folder that stays in the patient room. Since we didn't put it there, is this a breach?



**Scenario 4:** An automated insurance verification program assigns another patient's insurance to a patient's account. The insured, with the same name and date of birth, receives an explanation of benefits from his insurer and contacts the insurer to investigate. The error is traced to your organization. Is this a breach?

**Scenario 5:** A periodic audit reveals that an employee accessed the record of a family member. Upon investigation, the employee adamantly denies accessing the record. Is this a breach?

**Scenario 6:** An employee's user ID and password is discovered to have been used to log into their email account without their knowledge or consent. Logs show that the email account was used to send several thousand spam-type messages periodically over a period of 6 hours in the middle of the night on a weekend. The issue is discovered on Monday. The employee has multiple patient schedules in the sent mailbox - each containing patient name, diagnosis, phone numbers, insurance company name and type of services scheduled. What steps should be taken to analyze this type of potential breach and determine if patient notification is required?

