

**2009 Minnesota e-Health Summit**

**Break out Session # 8**  
**Explore Evolving Policy in HIT Privacy and Security**

June 25, 2009

**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
- **Eric Klavetter, JD**  
 Administrator, Information Security  
 Privacy and Compliance Officer  
 Mayo Clinic  
 Minnesota e-Health Workgroup Member



**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

- An ongoing program 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 sponsored by the e-Health Advisory Committee



## Overview

- The Health Information Technology for Economic and Clinical Health (HITECH) Act is part of the American Recovery and Reinvestment Act (ARRA or Stimulus Bill) signed by the President on February 17, 2009
- HITECH contains numerous changes to privacy & security requirements that impact HIPAA



## Business Associate (BA) Issues

- Effective February 17, 2010
- HIPAA Security – BAs must comply with the key provisions of the Security Rule
- HIPAA Privacy – BAs must comply with BA Agreement requirements



## Business Associate (BA) Issues, Continued

- Direct Liability – Business Associates become directly liable under HIPAA and subject to HIPAA civil and criminal penalties
- HITECH BA Requirements – “shall be incorporated into” business associate agreements



## Breach Notification

- Effective – approximately September 2009
  - Regulations to be issued by August
- Federal Breach Notification Requirements
  - Must be read together with existing State breach notification requirements
  - Frequency and manner of breach notifications will expand



## Breach Notification, Continued

- Applies to breaches of “unsecured PHI” –
  - Unsecured means NOT *encrypted* or *destroyed* according to specific standards
- Detailed requirements regarding –
  - Timing of notice
  - Manner
  - Content



## Breach Notification, Continued

- If there is insufficient or out-of-date contact information for 10+ individuals, covered entity must put a conspicuous notice on its website home page or put notice in major print or broadcast media
- If the breach involves 500+ individuals, notice must be provided through prominent local media outlets
- All breaches of unsecured PHI must be reported to DHHS
  - Immediately, if 500+ individuals involved
  - Others submitted in an annual log/report
  - DHHS will post lists of covered entities & breaches on website



## Requests for Restrictions

- Effective February 17, 2010
- Covered entity must comply if a patient requests that their PHI not be disclosed:
  - To their health plan
  - For payment or health care operations
  - If the PHI pertains solely to a health care item or service for which the provider has been paid out-of-pocket in full



## Minimum Necessary

- Effective February 17, 2010
- Interim rule – A covered entity will be in compliance with “minimum necessary” rule ONLY if:
  - The PHI is limited, to the extent practicable, to a limited data set, or
  - If needed by covered entity, the minimum necessary to accomplish the intended purpose
  - The disclosing covered entity or business associate must make the minimum necessary determination



## Accounting of Disclosures

- Effective Date depends on date of EHR implementation (2011 - 2014)
- Major expansion of Accounting requirements
- HITECH eliminates the exception for tracking & reporting of disclosures for Treatment, Payment and Healthcare Operations – if a covered entity uses an EHR and the disclosure is made through the EHR



## Prohibition on Sale of PHI

- Effective approximately February 2011
- Covered entity or business associate may not directly or indirectly receive remuneration in exchange for any PHI, unless the covered entity obtains the individual's Authorization, which includes certain disclosures about the remuneration



## Marketing Communications Using PHI

- Effective February 17, 2010
- Certain activities are currently permitted as healthcare operations outside the HIPAA marketing rules, e.g. communications:
  - About a CE's own products or services
  - For case management/care coordination
  - For treatment of an individual
- These exceptions will be “marketing” (and will require individual authorization), IF the CE receives any direct or indirect payment in exchange for making such communications



## Access to PHI in Electronic Form

- Effective February 17, 2010
- If the covered entity uses or maintains an EHR, individual has the right to obtain a copy of his or her PHI in an “electronic format”
- Individual may choose to direct that the electronic copy be transmitted to a third party
- Fee may not exceed labor costs in responding to the request



## Enforcement

- Effective dates vary – February 17, 2009 & after
- Criminal penalties can be applied to non-covered entities (e.g., employees)
- Increased monetary amounts for civil penalties
  - Tiered based on level of intent
  - Increased from \$100 per violation to maximum level of \$50,000 per violation
    - maximum \$1.5M for identical violations in one year



## Enforcement, Continued

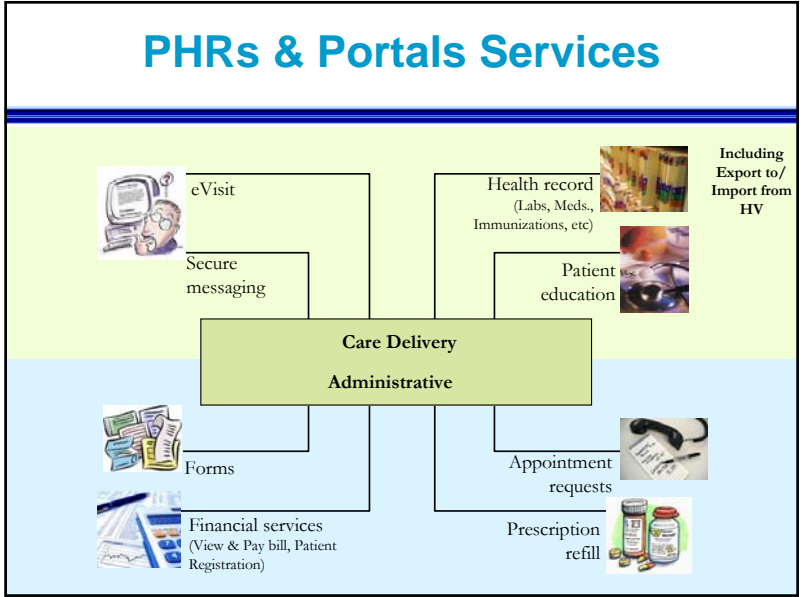
- State Attorneys General have enforcement power
- Civil penalties collected go to OCR for additional privacy enforcement
- There will be a methodology to share civil penalties collected with an individual who is harmed



## Personal Health Record (PHR)

- Initiated and maintained by an individual
  - Consumerism
- Companies that provide a PHR are not considering themselves Business Associates
- New Data Set to establish medical necessity or plan of care







### Breach Notification Case

Lotta Badluck is a nurse, working as a case manager at All-American Insurance Company. All-American is trying to leverage technology to improve efficiency and has provided its case managers with laptop computers with software to help them manage the care of health plan members with complex medical conditions. Data about these members is downloaded to the laptops from All-American's claims system.


Usually Lotta only uses the laptop at the office, but today she decides to take the laptop home to catch up on work after dinner. After stopping for takeout on her way home, Lotta returns to her car and finds it has been broken into! The laptop, which she had left on the back seat, is gone! Lotta calls the police and reports the damage and theft of the laptop. The next morning, Lotta tells her supervisor that the laptop was stolen.



- ### Breach Notification Case
- Breach Notification Summary
- 1) Do you have a Reportable Breach? Some threshold considerations:
    - Look at State and Federal Law – definition of breach
    - Which laws apply under the circumstances?
    - What information was involved?
    - How many people's information?
    - Was the information secured?
  - 2) It's a Breach, now what?
    - The most detailed requirements tend to be under HITECH
    - Timing & content of notification varies with applicable law
    - Individual notices
    - Public notices
    - Disclosure to DHHS
    - Notice to covered entity (if a BA)
    - Consumer reporting agencies
- 

### Mini-Case: Business Associates

All-American Insurance Company has an accounting & auditing firm (Addup & Associates) under contract.



### Mini-Case: Restrictions

Patient Trisha Trusting goes to her doctor for a physical. Miss Trusting decides to pay cash for the services and asks the clinic not to submit the bill to or share any information about today's visit with her insurance company, All American.



### Mini-Cases

- Patient Education & Marketing:
  - Pregnant women with Long QT Syndrome
- Point of Care Provider Education:
  - Know latest and greatest on:
    - Rare or complex medical topics
    - Routine care with rapid changes to care models
    - Pandemic Response



### Changes to Privacy & Security Requirements

QUESTIONS?



### Resources Available Through the Minnesota e-Health HITECH Web Page

[www.health.state.mn.us/e-health/hitech.html](http://www.health.state.mn.us/e-health/hitech.html)

#### Handouts / Resources

- Agenda
- Factsheets
  - Medicare – Hospital
  - Medicare-Professionals
  - Medicaid incentives
- Resource list
- Timeline
- Figure 1: Key Program, Distribution, Use and Recipients for the HITECH Act
- Slides from Public Meetings
- Minnesota Statewide Plan - 2008



## For More Information

[www.health.state.mn.us/e-health](http://www.health.state.mn.us/e-health)

Mick Hawton  
Center for Health Informatics  
[michael.hawton@state.mn.us](mailto:michael.hawton@state.mn.us)  
651-201-3598

