HITECH Requirements

Health Plan and Provider Perspective
Proposed Rules

- Modifications to the HIPAA Privacy, Security and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule
- Interim Final Rule on Breach Notification
  - Still in place
  - Final rule was withdrawn from OMB
Proposed Rule

- Effective Dates
  - Date of enactment – February 18, 2009
  - One year from date of enactment – February 18, 2010
Definitions moved around for the sake of consistency
Business Associate definition was substantively changed to add new entities
Definitions were changed to add “business associates” to applicability
Added HITECH to statutory authority
Subjects in Proposed Rule - Enforcement

- Changes apply to business associates
- Secretary *will* investigate any complaint when a preliminary investigation indicates willful neglect
- Secretary *will* conduct compliance reviews when a preliminary review indicates possible willful neglect
- Permits Secretary to disclose PHI to other authorities *such as state Attorneys General* and the Federal Trade Commission
- Allows the Secretary to go to a formal finding without informal resolution where there is willful neglect
Subjects in Proposed Rule - Enforcement

- Complement the Enforcement Rules
  - “Reasonable Cause”
  - Knowledge and Reasonable Diligence
  - Willful Neglect
  - Correction of Willful Neglect
  - Basis for civil money penalty
  - Factors to consider in imposing civil money penalty
  - Affirmative Defenses
  - Waiver
Mainly addition of business associates to different sections
Addressed business associate as part of hybrid entity
Specifically apply 164.306 to business associates
Subjects in Proposed Rule - Privacy

- Business Associates
- Health Care Operations
- Marketing
- Decedents
- Immunizations
- Minimum Necessary

- Fundraising
- Notice of Privacy Practices
- Right to request restrictions
- Access to Individual’s PHI
HITECH explicitly requires that its new provisions be incorporated into existing Business Associate Agreements (BAAs).

Due to these new privacy and security requirements, current agreements must be updated and amended in order to incorporate them.
HCMC’s Activities for Patients

- Patients may notify that they do not want their treatment encounter to be disclosed to the payer.
  - Worked with our E H R vendor to set up a process that electronically protects that information from being reported

- Updating Notice of Privacy Practices
  - Pending final privacy rules, adding information regarding breach process, PHI sale protections, marketing changes, and the right to control information to payers paid out of pocket
HCMC’s Activities for Patient cont.

- Break the Glass
  - Employees
  - Physicians
  - By patient request

- Privacy audits
  - Patient Complaints
  - Random quarterly + Persons of Interest
  - Management request
  - ID theft
The HITECH Act narrows the exceptions to the definition of "marketing communications."
- A communication is marketing unless it meets one of the three existing exceptions and there is no direct or indirect payment for making such communication.
- If payment is involved, not marketing if
  - for treatment purposes, or
  - about a drug or biologic that has been previously prescribed to that individual

Need to revisit all activities that were considered TPO before
Medica’s Processes

- Survey to business departments to identify
  - Communications that are sent to members
  - Benefits available only to Medica members
- Identify if any third party was involved in the communication
  - Did any remuneration exchange hands
- Identify all areas where third parties are making communications on behalf of Medica and making changes to business associate agreements
Requires covered entities to initially limit the use, disclosure or request of PHI, to the extent practicable, to a \textit{limited data set}.

Disclosure must be the \textit{minimum necessary to accomplish the intended purpose} of such use, disclosure, or request.

The entity disclosing the PHI is responsible for making the minimum necessary determination.

Proposed rule asked for comments without giving any guidance.
Medica’s Process

- **Culture Change**
- **Create the appropriate documentation**
  - What is the purpose of the disclosure?
  - Can a limited data set be used?
  - If not, why?
  - Why is each element of PHI that is being requested *necessary* to achieve the purpose?
  - What alternatives were considered?
- **Review Routine Uses and Disclosures**
  - Disclosures to other entities need to be re-examined
  - Some exceptions still apply
HCMC Security Reviews

Review each IT System for the following:

- The risk management, security policy, asset management, organizational security, human resource security, physical and environmental security, communications and operational environment, access control, system acquisition and development, Information Security incident management & business continuity of finalist vendor.

- Specific interview based on the type of system/application and it’s hosting of data the following are examined:
  - Remote Access availability
  - Ability to do role-based access
  - Account Management
  - Password/log on capabilities
  - Auditing/monitoring capabilities
  - Encryption capabilities in transit, storage, etc
  - Assessment of third party tools
Breach Notification

- Covered entities are required to notify the affected individuals of any unauthorized acquisition, access, use, or disclosure of unsecured PHI without unreasonable delay but not later than 60 calendar days after discovery.
- BAs who have access to PHI are required to notify the covered entity of any such breach, including the name of any individual whose unsecured PHI has been released.
- While HHS has indicated that the parties to BA agreements have flexibility in this regard, it has encouraged the parties to ensure that individuals do not receive notification from both the BA and the covered entity, as this could be confusing.
Breach Notification

- **What is a Breach?**
  - Acquisition, access, use, or disclosure of *unsecured PHI* which is not permitted by the HIPAA Privacy Rules and compromises the security or privacy of the PHI.
  - There is a significant risk of financial, reputational, or other harm to the affected individual(s).

- **What is Unsecured PHI?**
  - PHI that is not secured through a technology or methodology, specified by HHS, that renders the PHI unusable
  - Encryption and destruction are deemed as the technologies and methods for securing PHI. The encryption must be an algorithmic process with a confidential process or encryption key, and the decryption tools are stored at a location separate from the encrypted data.
## Breach Notification

### Exceptions

- **Any unintentional acquisition** by an authorized individual or business associate (BA), who acquired, accessed, or used the PHI in good faith and within the normal scope of his/her authority, and if that PHI is not further used or disclosed.

- **Any inadvertent disclosure** by an authorized person or BA to another authorized person at the same covered entity, BA, or organized health care arrangement, and the PHI is not further used or disclosed in violation of the HIPAA Privacy Rules;

- A disclosure of PHI where a covered entity or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- Law enforcement determines that notification would impede a criminal investigation or cause damage to national security, *for up to 30 days as orally directed by the law enforcement agency, or for such longer period as the law enforcement agency specifies in writing*.
Breach Notification

- **Discovery of Breaches**
  - Breaches are treated as discovered as of the first day on which the breach is known or should have been known to the covered entity.

- **How to Provide Notice**
  - Covered entities should send written notification via first class mail to each affected individual (or if deceased, the individual’s next of kin) at the last known address, unless the individual has indicated a preference for e-mail.
  - If the address is unknown for fewer than 10 individuals, then a substitute notice must be provided by other means reasonably calculated to reach the affected individual.
  - If the address is unknown for 10 or more individuals, then a substitute notice must be provided by either a conspicuous posting on the entity’s web homepage for a specified period of time (period of time proposed by HHS is 90 days) or a conspicuous publication in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside.
Breach Notification

**Notice to 500+ Affected Individuals**
- If the breach of unsecured PHI affects 500 or more individuals, then the notice must also be provided to major media outlets serving the relevant State or jurisdiction. The notice to the media must contain the same information as the written notice to individuals, and must similarly be provided without unreasonable delay, but in no case later than 60 calendar days after discovery of the breach.

**Notice to HHS**
- Additionally, the covered entity must notify HHS, in the manner specified on the HHS website, contemporaneously with the notice sent to the individuals.
- The HHS website will have a list that identifies the covered entities involved in a breach in which 500 or more individuals are affected.
- If less than 500 individuals are affected then the covered entity may maintain a log of the breaches and must submit this log annually to HHS (within 60 days after the end of each calendar year).
Breach Notification

Contents of the Written Notice

- Notification must be written in plain language;
- A brief description of what happened, including the date of the breach and the date of the discovery of the breach;
- A description of the types of unsecured PHI that were disclosed;
- Steps that individuals should take to protect themselves from potential harm resulting from the breach of unsecured PHI (such as contacting their credit card companies);
- A brief description of the actions taken by the covered entity to investigate the breach, mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free number, an e-mail address, website, or postal address.
Breach Notification

**Compliance with Federal and State Laws on Breach Notifications**

- The new HIPAA breach notification requirements override any conflicting state laws.
- However, covered entities must comply with both federal and state breach notification laws if the state law does not conflict with these new HIPAA breach notification requirements.
- These requirements similarly do not override obligations imposed by other federal laws, such as requirements imposed by Title VI of the Civil Rights Act to take reasonable steps to ensure meaningful access to the notice by those with Limited English Proficiency, and requirements imposed by the Americans with Disabilities Act to ensure effective communication of the notice to individuals with disabilities.
Other Requirements

**Additional Requirements**

In addition to the breach notification requirements, the federal regulations impose additional compliance obligations on covered entity practices consistent with those imposed by other HIPAA obligations, including the requirement to:

- Revise policies and procedures and Notice of Privacy Practices to reflect the HIPAA Breach Notification Rule;
- Train workforce members on the policies and procedures with respect to the notification requirements;
- Allow individuals to complain about those policies and procedures, or whether the notification requirements have been violated;
- Sanction workforce members who violate the notification requirements; and
- Refrain from retaliating against those who exercise their rights.
HCMC’s Process for Notification

- Defined
  - Breach,
  - Encryption,
  - Protected Health Information
    - Individually Identifiable information
  - ARRA/HIPAA
HCMC’s Process for Notification

- Require any one discovering a potential breach of protected health information to report as soon as it’s discovered.
- Established a Breach Response Team with representation from Information Security & Privacy, Compliance, Public Relations, Legal, and Patient Safety.
- The Breach Response Team conducts a thorough review of the breach event, contacts appropriate involved persons, identifies level of risk, reviews the breach exception criteria, and creates an action plan that meets regulatory requirements and documents the event.
- Affected patients receive a letter with all required information regarding the breach.
- Based on severity, breaches are communicated to HHS/Media as required per event and/or annually.
- Breach contributing factors are addressed to prevent reoccurrence.
Published July 14, 2010

First steps in risk analysis
- Identify the e-PHI within your organization
- Identify the external sources of e-PHI
- Identify the human, natural and environmental threats to information systems

The risk analysis helps
- Design appropriate personnel screening processes
- Identify what to backup and how
- Decide whether and how to use encryption
- Address what must be authenticated in particular situations to protect data integrity
- Determine the appropriate manner of protecting health information transmissions
Elements of Risk Analysis

- Define scope of analysis
- Data collection
- Identify and document potential threats and vulnerabilities
- Assess current security measures
- Determine the likelihood of threat
- Determine potential impact of threat
- Determine level of risk
- Finalize Documentation
- Conduct continuous risk analysis
HCMC’s process regarding risk

- Completed preliminary ePHI review focusing on external communication
- Interfaces secured ePHI in transit
- In process of creating a secure file transfer capability hospital wide for ePHI
- Incorporated level of ePHI risk as part of our Hazard Vulnerability Analysis
- Perform annual risk assessments based on National Institute of Standards and Technology referenced in HIPAA
Presenter Contact Information

- **Billie Zippel, Associate General Counsel Medica Health Plans**
  - wilma.zippel@medica.com
  - 952-992-3670

- **Reidun Hanson, HCMC Information Security & Privacy Officer**
  - reidun.hanson@hcmed.org
  - 612-873-6324