HIPAA, HITECH and The Final Rule

Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA

Preferred Quality Consulting Services

~

Kelly Stewart, MS, RHIA

Indian Health Service

Objectives:

HIPAA Privacy and Security

- Understand the 2009 and 2013 Modifications
- Conduct security risk analysis to identify threats and risks.
- Document and monitor security measures
- Develop a risk mitigation plan

Best Practices in Breach Prevention

- Develop appropriate security measures
- Monitor compliance with required measures
- Comply with reporting requirements

Session One Overview:

- Introductions
- HIPAA 1996
- HITECH 2009
- Final Rule 2013
- Privacy Standards Refresher and Modifications
- Breach Notifications
- Compliance and Enforcement Overview after HITECH
- Penalties

HIPAA 1996

Health Insurance Portability and Accountability Act

- The Purpose of HIPAA
  - Portability
  - Fraud and Abuse
  - Efficiency and Effectiveness
  - Protection and Security
  - Statistics
  - Patients Right

- Major Sections
  - Privacy Rule
  - Security Rule
  - Enforcement
  - Transactions and Codes Sets
  - Unique Identifiers – providers and employers

HITECH 2009

Health Information Technology For Economic and Clinical Health

- ARRA
  - Economic stimulus for the entire economy
- HITECH under ARRA
  - Economic Stimulation and Improving Health Care
  - CMS EHR Incentive Program
    - Meaningful Use
    - Certified EHR
  - Modifications to Privacy and Security Laws

HITECH 2009

Health Information Technology For Economic and Clinical Health

Revisions Implemented in 2009

- Breach Notifications
- FTC Breach Notifications PHR Vendors
- Technology/Methodology PHI - U, U and I
- Enforcement Rules Tiered Approach & Higher Penalties

Revisions Included but NOT Implemented in 2009
hence, the Omnibus Final Rule of 2013

Omnibus Final Rule 2013

- Guidance on how and when to implement privacy requirements from HITECH
- Effective March 26, 2013
- Compliance in 180 days following
- Modifications:
  - Privacy
  - Security
  - Breach Notification
  - Enforcement
  - Genetic Information Nondiscrimination Act

Privacy Overview with Modifications

- Applicability △ 2013
- Definitions
  - Health Care Operations △ 2013
  - Marketing △ 2013
  - Payment △ 2013

164.500 & 164.501

General Rules for Uses and Disclosures of PHI

- Uses and Disc for Treatment, Payment and Health Care Operations △ 2013
- Minimum Necessary △ 2013
- Uses and Disc of PHI Subject to an Agreed Upon Restriction
- Creation of De-identified Information
- Disclosures to Business Associates △ 2013
- Deceased Individuals △ 2013
- Personal Representatives
- Confidential Communications
- Uses and Disc Consistent with Notice
- Disclosures by Whistleblowers and Workforce Member Crime Victims

164.502

Uses and Disclosures: Organizational Requirements

- Business Associated Contracts △ 2013
- Requirements for Group Health Plans △ 2013
- Requirements for Covered Entities with Multiple Covered Functions

164.504

Uses and Disclosures: Treatment, Payment & Health Care Operations

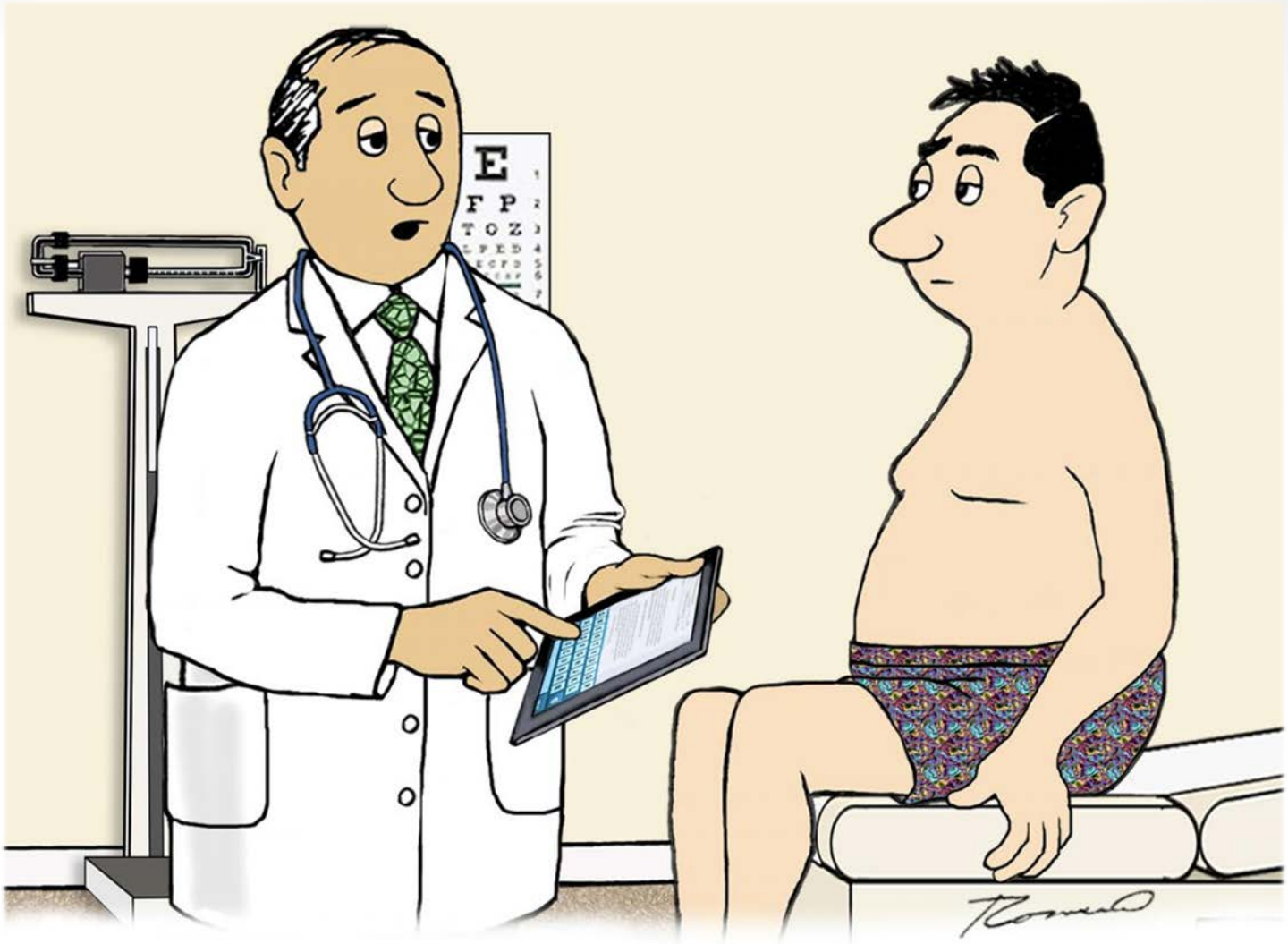
- Permitted Uses and Disc △ 2013
  - Consent for Uses and Disc Permitted
- Treatment, Payment and Health Care Operations △ 2013

164.506

Uses and Disclosures: Authorization is Required

- Authorizations for Uses and Disc △ 2013
- General Requirements △ 2013
- Core Elements and Requirements △ 2013

164.508


"According to your HIPAA release form
I can't share anything with you."

Uses and Disclosures: Opportunity for Individual to Agree/Object

- Use and Disc for Facility Directory △ 2013
- Uses and Disc for Involvement in the Individuals Care and Notification Purposes △ 2013

164.510

Uses and Disclosures: Authorization or Opportunity to Agree/Object is NOT Required

- Uses and Disclosures Required by Law
- Uses and Disc for Public Health Activities △ 2013
- Disclosures About Victims of Abuse, Neglect and Domestic Violence
- Uses and Disc for Health Oversight Activities
- Disclosures for Judicial and Administrative Proceedings △ 2013
- Disclosure for Law Enforcement Purposes
- Uses and Disc about Decedents
- Uses and Disc for Cadaveric Organ, Eye, Tissue Donation
- Uses and Disc for Research Purposes △ 2013
- Uses and Disc to Avert a Serious Threat to Health or Safety
- Uses and Disc for Specialized Government Functions △ 2013
- Disclosures for Workers' Compensation

Other Requirements

- De-Identification of PHI
- Requirements for De-Identification of PHI
- Re-Identification
- Minimum Necessary Requirements
- Limited Data Set △ 2013
- Fundraising △ 2013
- Underwriting △ 2013
- Verification Requirements

164.514

Patient Rights:
Notice of Privacy Practices for PHI

- Right to Notice of Privacy Practices
- Content of Notice of Privacy Practices △ 2013
- Provision of Notice of Privacy Practices △ 2013
- Joint Notice by Separate Covered Entities
- Documentation of Notice

164.520

Patient Rights:
Right to Request Privacy Protection for PHI

- Right of an Individual to Request Restriction of Uses and Disc
  △ 2013
- Confidential Communications Requirements

164.522

Patient Rights:
Access to Individuals to PHI

- Access to PHI
- Requests for Access and Timely Action △ 2013
- Provision of Access △ 2013
- Denial of Access
- Documentation

164.524

Patient Rights: Amendment of PHI

- Right to Amend
- Requests for Amendment and Timely Action
- Accepting the Amendment
- Denying the Amendment
- Actions on Notice of Amendment
- Documentation

164.526

Patient Rights: Accounting of Disclosures of PHI

- Right to an Accounting
- Content of the Accounting
- Provision of the Accounting
- Documentation

164.528

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

The Administrative Requirements

- Personal Designations
- Training
- Safeguards
- Complaints to the Covered Entity
- Sanctions
- Mitigation
- Refraining from Intimidating or Retaliatory Acts
- Waiver of Rights
- Policies and Procedures
- Documentation
- Group Health Plans

Transition Provisions △ 2013

Compliance

Breach Notification Overview with Modifications

Effective September 2009

Notification in the Case of Breach of Unsecured Protected Health Information

- 164.400 Applicability
- 164.402 Definitions 2013

  Breach Means

  - Exclusions to Breach
    - Unintentional
    - Inadvertent disclosure
    - Non-retention
  - Assumption of Breach
  - Risk assessment factors

  Unsecure PHI Means

Breach Notification Overview with Modifications

Effective September 2009

164.404 Notification to Individuals: General Rule

Timeliness of Notification

Content of Notification

Methods of Individual Notification

- Substitute Notification
- Urgent Notification

Notification to the Media 2013

Breach Notification Overview with Modifications

Effective September 2009

- 164.406 Notification to the Media 2013
- 164.408 Notification to the Secretary of HHS 2013
  - Immediate
  - Yearly
- 164.410 Notification by Business Associates 2013
  - Report unsecure PHI
  - Notify the CE without unreasonable delay -no later than 60 days
- 164.412 Law Enforcement Delay
- 164.414 Administrative Requirements and Burden of Proof

Compliance and Enforcement after HITECH

- Applicability △ 2013
- Section 160. 302 removed △ 2013
- Principles for Achieving Compliance △ 2013
- Complaints to the Secretary △ 2013
- Compliance Reviews △ 2013
- Responsibilities of Covered Entities △ 2013

160.300 - 160.310

Secretarial Action Regarding Complaints and Compliance Reviews △ 2013

- OCR Oversight
  - Accepts complaints
  - Investigates
  - Conducts Audits
  - Issue penalties
  - Guidance and educational material

Investigational Subpoenas and Inquiries △ 2013

Refraining from Intimidation or Retaliation

Enforcement…the past, the future. It's going to get ugly!

Trends in Enforcement

HITECH Changes

- Willful Neglect
  - Mandatory Investigations and penalties (monetary)
- Periodic Audits
- Fines and Penalties go to OCR
- Harmed Individuals will receive portion of fines
- Individuals subject to criminal provisions with CE and BA
- State Attorney General can bring action on behalf of states

Penalties

- Effective 2009
- Penalty for non-compliance even when no individual involved
- Penalty for violations of wrongful disclosure
- Four Tiers of penalty
  - A-Didn't Know (100-25K)
  - B-Reasonable Cause (1K-100K)
  - C-Willful Neglect but corrected (10K-250K)
  - D-Willful Neglect no corrected (50K-1.5M)
- Maximum Penalties for one year

Penalties

TABLE 1—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE		
Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

IHS Policies & Procedures

Scenario:

IMPERMISSABLE USES AND DISCLOSURE

Session One Conclusion

- HIPAA 1996
- HITECH 2009
- Final Rule 2013
- Privacy Standards Refresher and Modifications
- Breach Notification
- Compliance and Enforcement Overview after HITECH
- Penalties
- Hand Outs

Questions?