HIPAA RISKS & STRATEGIES
Health Insurance Portability and Accountability Act of 1996
REGULATORY BACKGROUND

- Health Information Portability and Accountability Act (HIPAA) was enacted on August 21, 1996
- **Title I: Healthcare Access, Portability & Renewability**
  - Limits preexisting condition exclusion
  - Special enrollment periods if loss of coverage/life event
  - Prohibits discrimination
  - Guarantees certain individuals access/renewal to individual health insurance policies
REGULATORY BACKGROUND

Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform
  • Privacy Rule (4/13/2003)
  • Transactions and Code Sets Rule (10/16/2004)
  • Security Rule (4/21/2005)
    o Administrative, Technical and Physical Safeguards
  • Unique Identifiers Rule (5/23/2007)
  • Enforcement Rule (3/16/2006)
REGULATORY BACKGROUND

Health Information Technology for Economic and Clinical Health Act (HITECH) (Title XIII of ARRA 2009)

- Subtitle A: Promotion of Health Information Technology
- Subtitle B: Testing of Health Information Technology
- Subtitle C: Grants and Loans Funding
- Subtitle D: Privacy
HR Areas of Privacy

- ADA
- FMLA
- Workers’ Compensation
- Employer Medical Exams
  - Drug Testing
  - Pre-employment Physicals
  - Fitness for Duty Examinations
- Employer Health Insurance
ADA & PRIVACY

○ Employment Entrance Exams
  • Pre-Employment Post-Offer
    ○ Required of all entering employees
    ○ Information obtained regarding medical condition/history is collected and maintained in separate forms and in separate medical files and is treated as a confidential medical record, except that –
      ○ Supervisors may be informed regarding necessary restrictions or accommodations
      ○ First aid and safety personnel may be informed if disability might require emergency treatment
      ○ Government officials investigating compliance
ADA & Privacy

- Disability related inquiries generally prohibited by ADA
- Employers allowed to ask for medical documentation of a disability if hidden impairment and requesting a reasonable accommodation
  - Scope of inquiry limited to documenting person has an ADA disability
  - Cannot ask for employee’s complete medical record
FMLA & Privacy

- **HIPAA**
  - Does not regulate the employer’s use and disclosure of this medical information
  - Does regulate the doctor’s ability to release the information
    - HR should give certification to employee who gives it to their doctor
    - If HR goes directly to doctor than request should be accompanied by a written authorization by the employee
WORKERS’ COMPENSATION & PRIVACY

- HIPAA does not apply to:
  - Workers’ compensation insurers
  - Workers’ compensation administrative agencies
  - Employers (unless otherwise covered)

- Privacy Rule permits disclosures of health information for workers’ compensation
Workers’ Compensation & Privacy

- Disclosures without individual authorization
  - As authorized by and to extent necessary to comply with laws relating to workers’ compensation
    - Also includes Black Lung Benefits Act, the Federal Employees’ Compensation Act, the Longshore and Harbor Workers’ Compensation Act and the Energy Employees’ Occupational Illness Compensation Program Act

- Disclosures with individual authorization
  - Individual provides authorization for release of information to entity

- Minimum necessary
  - Limit PHI to minimum necessary to accomplish workers compensation purpose
  - For payment purposes
WORKERS’ COMPENSATION & PRIVACY

- OSHA 300 Log of Work-Related Injuries & Illnesses
- “Privacy Concern Case”
  - Injury or illness to intimate body part or reproductive system
  - Resulting from sexual assault
  - Mental Illness
  - HIV infection, hepatitis or tuberculosis
  - Needle stick injuries & cuts from contaminated sharp objects
  - Other illnesses if employee voluntarily requests name not be entered on the log
WORKERS’ COMPENSATION & PRIVACY

- OSHA 300 – other privacy concerns
  - Identifiable without name
    - Enough information to identify cause of incident and general severity of injury/illness
    - No details of intimate or private nature
    - i.e. sexual assault = injury from assault
EMPLOYER MEDICAL EXAMS & PRIVACY

- PHI may disclosed to employer when:
  - Service at request of employer or as a member of employer’s workforce
  - Service must relate to medical surveillance of workplace
    - Determine whether individual has work-related illness or injury
  - Employer has a duty under OSHA to keep records on or act on such information
- Generally, this does not include pre-employment physicals, drug tests and fitness for duty exams
  - But, see ADA Privacy Rule
**Drug Testing & Privacy**

- State or Local Laws unless industry heavily regulated by federal government
  - i.e. transportation, nuclear energy, military contracting
  - California has many privacy rules affecting the workplace
- Not an exam under the ADA
- But, results are medical records
  - Privacy rule under ADA
EMPLOYER HEALTH INSURANCE & PRIVACY

- See HIPAA Privacy and Security Rules
HIPAA Overview

- Privacy Rule
  - “Standards for Privacy of Individually Identifiable Health Information”

- Security Rule
  - “Security Standards for Protection of Electronic Protected Health Information”
  - Operationalizes protections contained in Privacy Rule
Privacy Rule – Major Goal

Protect PHI  Quality Health Care
Privacy Rule – Who’s Covered?

- Health Plans
- Health Care Clearinghouses
- Health Care Providers (Transmitting Electronically)
Privacy Rule – Covered Health Plans

- Individual and group plans
  - Employer sponsored
  - Government and church sponsored
  - Multi-employer plans

- Health, dental, vision and prescription drug
- HMO’s
- Medicare
- Medicaid
- Medicare+Choice and Medicare Supplements
- Long-Term Care
Privacy Rule – Covered Health Plans

Exceptions

- Group health plan
  - Less than 50 participants
  - Administered solely by employer
  - Maintains plan is not a covered entity

- Government-funded programs
  - Principal purpose is not providing or paying cost of healthcare (i.e. food stamps)
  - Principal activity is directly providing health care
    - Community health center
    - Grants to fund direct provision of health care

- Other Insurance
  - Workers’ compensation
  - Automobile
  - Property and casualty
Privacy Rule – Covered Clearinghouse

- Entities that process nonstandard information they receive from another entity into a standard or vice versa
- If a business associate then only some provisions of Privacy Rule are applicable
“Person or organization, other than member of covered entity’s workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information”
Privacy Rule – Business Associates

- Business Associate Agreement (Contract)
  - Covered entity imposes specified written safeguards on PHI used or disclosed by business associates
  - Covered entity may not contractually authorize business associate to use or disclose PHI that would violate Privacy Rule
  - See Department of Health and Human Services Office of Civil Rights for sample contract language
Privacy Rule – Business Associates

- Functions
  - Claims processing
  - Data analysis
  - Utilization review
  - Billing

- Services
  - Legal
  - Actuarial
  - Accounting
  - Consulting
  - Data aggregation
  - Management
  - Administrative
  - Accreditation
  - Financial services
Privacy Rule – Business Associates

- Not a business associate –
  - Function or service does not involve use or disclosure of PHI or access to PHI would be incidental
- Covered entity can be the business associate of another covered entity
PRIVACY RULE – WHAT IS PHI

- PHI = Protected Health Information
- The Privacy Rule Protects:
  - Individually identifiable health information
  - Held or transmitted by a Covered Entity or its Business Associate
  - In any form or media
    - Electronic
    - Paper
    - Oral
PRIVACY RULE – WHAT IS PHI

Demographic data

- Individual’s past, present or future physical or mental health or condition,
- Provision of health care to the individual, or
- Past, present or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
Privacy Rule – What is PHI

Exclusions –
- Employment records
- Education records (as defined in FERPA)
Privacy Rule – What is PHI

- De-identified Health Information
  - No restrictions on use or disclosure
  - Neither identifies nor provides reasonable basis to identify an individual
  - Methods
    - Formal determination by qualified statistician
    - Removal of specified identifies of individual, of individual’s relatives, household members and employers is required
      - And if covered entity has no actual knowledge that remaining information could be used to identify the individual
PRIVACY RULE – USE AND DISCLOSURE

- Comply with the Privacy Rule
  - Use or disclose information as the patient authorizes
  - To the individual (or their personal representatives)
  - To the US Department of Health & Human Services (HHS) if undertaking a compliance investigation.

- It is appropriate to use or disclose patient health information for:
  - Treatment
  - Payment
  - Normal operations of health care

- Public Interest and Benefit Activities
PRIVACY RULE – USES AND DISCLOSURES

Permitted, but not required, to use and disclose PHI without individual’s authorization for following purposes:

- To individual (unless required)
- Treatment, Payment and Health Care Operations
- Opportunity to Agree or Object
- Incident to an otherwise permitted use and disclosure
- Public Interest and Benefit Activities
- Limited Data Set for purposes of research, public health or health care operations
Privacy Rule – Authorized Use

- When protected health information is used or disclosed outside of normal operations, for treatment or billing:
  - A patient must give written authorization in specific terms to the covered entity to do so
  - The principle of “Minimum Necessary” should apply
    - Circumstances which do not require “Minimum Necessary”:
      - The information is required by law
      - HHS would use the information in a complaint investigation
      - An entity will use the information internally
Minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure or request
Privacy Rule – Minimum Use

Not applicable when –

- Health care provider for treatment
- Patient being treated
- Pursuant to authorization
- HHS for complaint investigation, review or enforcement
- Required by law
- Required by other HIPAA rules
**Privacy Rule - Notice**

- Each covered entity must provide notice of its privacy practices
  - Acknowledgement of Notice Receipt
- Right to review and obtain a copy of PHI
- Disclosure Accounting
Privacy Rule – Administrative Requirements

- Privacy Policies and Procedures
- Privacy Personnel – designated privacy official
- Workforce Training and Management
- Mitigation
- Data Safeguards
- Complaints
- Retaliation and Waiver
- Documentation and Record Retention
Privacy Rule – Other

- Personal Representative – treat same as individual with respect to uses and disclosures of that individual’s PHI (and their rights)
- Minors: parents are usually the personal representative; if not refer to state law
PRIVACY RULE - MISCELLANEOUS

- **State Law Preemption**
  - Federal requirements apply when state laws are contrary

- **Enforcement**
  - Department of Health and Human Services Office of Civil Rights
SECURITY RULE

- Major Goal: protect privacy of individuals’ health information while allowing covered entities to adopt new technologies
- Designed to be flexible and scalable based on size, organizational structure and risks
Security Rule

Safeguards
- Administrative
- Technical
- Physical

Assurances
- Confidentiality
- Integrity
- Availability
SECURITY RULE – COVERED ENTITIES

Health Plans

Health Care Clearinghouses

Health Care Providers (Transmitting Electronically)
Security Rule – Protected Information

- Electronic Protected Health Information (e-PHI)
  - All individually identifiable health information a covered entity *creates, receives, maintains or transmits* in electronic form.
  - Security Rule does *not* apply to PHI transmitted orally or in writing
Security Rule – General Rules

- Maintain reasonable and appropriate administrative, technical and physical safeguards for protecting e-PHI
  1. Ensure confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit
  2. Identify and protect against reasonably anticipated threats to security or integrity of information
  3. Protect against reasonably anticipated, impermissible uses or disclosures; and
  4. Ensure compliance by their workforce
Security Rule – Confidentiality

- E-PHI is not available or disclosed to unauthorized persons
- Supports Privacy Rule prohibitions (improper uses and disclosure of PHI)
- Two additional goals
  - Maintaining integrity of e-PHI
    - Not altered or destroyed in an unauthorized manner
  - Maintaining availability of e-PHI
    - Accessible and useable on demand by an authorized person
SECURITY RULE – CONSIDERATIONS

- Size, complexity and capabilities of organization
- Technical hardware and software infrastructure
- Costs of security measures
- Likelihood and possible impact of potential risks to e-PHI

Covered entities must **review and modify** their security measures to continue protecting e-PHI
On-going Risk Analysis includes, but not limited to:

- Evaluate likelihood and impact of potential risks to e- PHI
- Implement appropriate security measures to address risks identified in risk analysis
- Document chosen security measures and the rationale for adopting those measures
- Maintain continuous, reasonable, and appropriate security provisions
Security Rule – Risk Analysis

- Regularly review records to
  - Track access to e-PHI
  - Detect security incidents
  - Evaluate effectiveness of security measures
  - Reevaluate potential risks to e-PHI
SECURITY RULE – ADMINISTRATIVE SAFEGUARDS

- Security Management Process
- Security Personnel
- Information Access Management
- Workforce Training and Management
- Evaluation
Security Rule – Physical Safeguards

- Facility Access and Control
- Workstation and Device Security
SECURITY RULE – TECHNICAL SAFEGUARDS

- Access Control
- Audit Controls
- Integrity Controls
- Transmission Security
SECURITY RULE

- Required and Addressable Implementation Specs
  - Required – must be implemented
  - Addressable – (doesn’t mean optional)
    - Permits covered entities to determine whether spec is reasonable and appropriate
    - If not, may adopt alternative measure to achieve purpose of standard (if reasonable and appropriate)
SECURITY RULE – ADDITIONAL REQUIREMENTS

- Covered Entity Responsibilities
  - Must take reasonable steps to cure material breach or violation of obligations

- Business Associate Contracts
  - See HITECH Act of 2009

- Policy and Procedures
  - Must adopt reasonable and appropriate P&P
  - Maintain records (6 years)
    - Policies and Procedures
    - Records of required actions, activities or assessments
  - Update and Review
SECURITY RULE - MISCELLANEOUS

- **State Law Preemption**
  - Federal requirements apply when state laws are contrary

- **Enforcement**
  - Department of Health and Human Services Office of Civil Rights
HITECH ACT OF 2009

Subtitle A—Promotion of Health Information Technology
  • PART 1—Improving Health Care Quality, Safety, And Efficiency
  • PART 2—Application and use of adopted health information technology standards; Reports

Subtitle B—Testing of Health Information Technology

Subtitle C—Grants and Loans Funding

Subtitle D—Privacy
  • PART 2—Relationship To Other Laws; Regulatory References; Effective Date; Reports
HITECH ACT OF 2009

- Health Information Technology for Economic and Clinical Health
  - Part of the American Recovery and Re-investment Act (ARRA)
  - Promote widespread adoption and standardization of electronic health records
  - Notification requirements for breaches of unsecured information
  - Increases potential civil monetary penalties for violations of HIPAA
  - Strengthens privacy rights
HITECH ACT OF 2009

- Penalties
  - $100 to $50,000 per violation
  - Calendar year cap for any identical violation raised to $1.5 million (from $25,000)

- Business Associates
  - Expanded Responsibilities of Business Associates
Sanctions & Liability

- See Penalties under HITECH
- No private right of action under HIPAA, but
- Other Potential Liability
  - Invasion of privacy, intentional infliction of emotional distress, defamation
- Private right of action available under employment laws
THANK YOU!

Questions?

Sandy Cooper, MS, JD, SPHR
Oklahoma State University in Tulsa
sandy.cooper@okstate.edu