Privacy & Security Matters: Protecting Personal Data

Privacy & Security Project

UNIVERSITY OF MINNESOTA

HIPAA: What it is

- Health Insurance Portability and Accountability Act of 1996
  - Also known as Kennedy-Kassebaum Act
- Legislation had wide regulatory impact
  - Medicare Fraud to Medical Savings Accounts.
- Department of Health and Human Services
  - Responsible for creating regulations
  - Office of Civil Rights responsible for enforcement

What HIPAA Does

1. Creates standards for protecting the privacy of health information
2. Creates standards for the security of health information
3. Creates standards for electronic exchange of health information
4. Requires action as single entity
5. Privacy rule mandates training 25,000 workforce members on standards and policies

Deadlines for Compliance

- Privacy — **April 14, 2003!**
- Security — **Fall 2004**
- Transactions & Code Sets — **October 16, 2003**
- Identifiers — **Fall 2004**

Key Definitions

- Individually Identifiable Health Information
  - Related to an individual; the provision of health care to an individual; or payment for health care
  - and that identifies the individual
  - or a reasonable basis to believe the information can be used to identify the individual
- Protected Health Information (PHI)
  - Individually Identifiable Health Information
  - Electronic, paper, oral
  - Created or received by a health care provider, public health authority, employer, school or university

Definitions

- Covered Entity
  - Health care provider who transmits any health information in electronic form in connection with HIPAA regulations
    - “Health care provider” means a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Impact on the University System

- Significant financial implications
- High level of risk to individuals and to institution
  - civil monetary penalties
  - criminal sanctions
- Requires a change in the way we do business
  - New U-wide policies & procedures
  - Limits access to information

Scope of Impact

- **University-wide**

  -Athletics
  -Auxiliary Services
  -Carlson SOM
  -General Counsel
  -MMF
  -U Health Plan
  -Student Health Services
  -Environmental Health
  -Ed and Human Devel.
  -College of Liberal Arts
  -School of Music
  -Food Science & Nutrition
  -University Foundation
  -General College
  -Disability Services
  -OIT

- **All Coordinate Campuses**
- **Business partners: UMP, FUMC, affiliated sites**
- **“business associates”**

Operations Impact

- Education
  - ensure students competencies in privacy & technology.
    - Record keeping
    - curriculum
- Research
    - Major change to process
    - IRB processes and function
- Health Care
    - Culture change

University Policies and Procedures Needed

- Regents policy on privacy, compliance and enforcement
- Policies for use and disclosures of PHI
- Privacy policy for patients
- Administrative forms permitting disclosure
- Policies for sanctions, mitigation, and monitoring
- Policies for data security
- Policies for education and training

Key Components of Compliance with Privacy Rule

- Policies and procedures
- Privacy Officer
- Training Program
- Complaint Process
- Internal compliance audit program
- Sanctions
- Incident response and corrective action procedures

Privacy and Security Project Organization

Education & Training Task Force

Privacy and Confidentiality

Curriculum for Tech Competencies

Curriculum for Policy, Legal, Ethics, and Health Systems Issues

Privacy Environment

Implementation

Competency Assessment

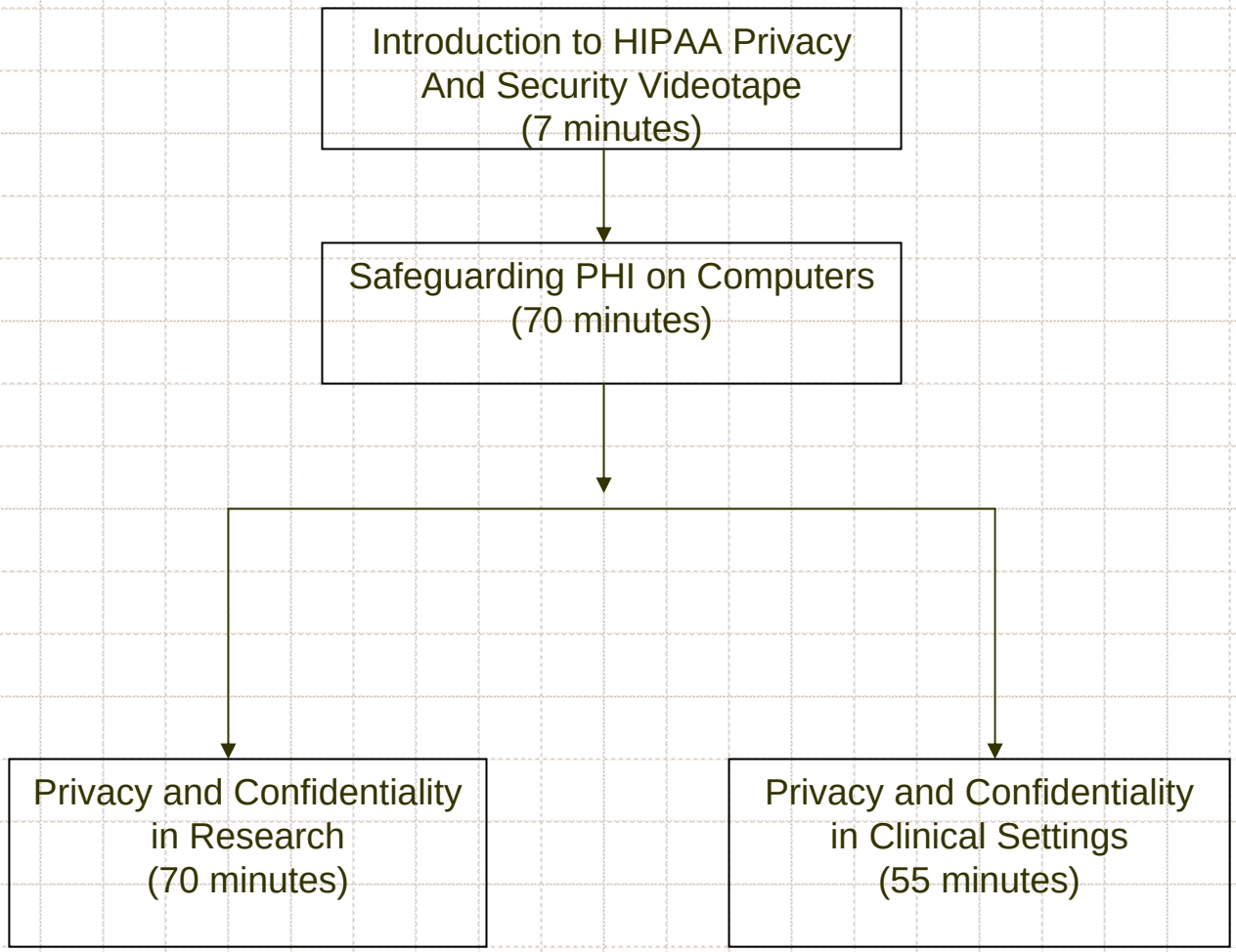
Technology Task Force

Clinical issues

Technical & Security Audit

Research Issues

Privacy and Security Project Education Program Model



Privacy and Security Project Organization

Example of Training Material

Security and the Privacy Rule

- Must implement appropriate technical safeguards to protect privacy of PHI.
- Must be able to reasonably safeguard against any intentional or unintentional use or disclosure that is a privacy violation.
- Should work in conjunction with “minimum necessary” rule
- Coordinated with HIPAA security regulations.

HIPAA Security Rule: Implications for University IT

- Security Rule applies to individually identifiable information that is in electronic form.
- All health care providers, health plans, or clearinghouses must comply!

Goal of Security Rule

- To ensure reasonable and appropriate administrative, technical, and physical safeguards that insure the integrity, availability and confidentiality of health care information, and protect against reasonably foreseeable threats to the security or integrity of the information.

Focus of Security Rule

- Both external and internal threats
- Prevention of denial of service
- Theft of private information
- Integrity of information

Rule has 4 categories

1. Administrative Procedures
2. Physical Safeguards
3. Technical data security services
4. Technical security mechanisms

Administrative Procedures: 12 Requirements

1. Certification
2. Chain of Trust Agreements
3. Contingency Plan
4. Mechanism for processing records
5. Information Access Control
6. Internal Audit
7. Personnel Security
8. Security Configuration Management
9. Security Incident Procedures
10. Security Management Process
11. Termination Procedures
12. Training

Physical Safegaurds: 6 Requirements

1. Assigned Security Responsibility
2. Media Controls
3. Physical Access Controls
4. Policy on Workstation Use
5. Secure Workstation Location
6. Security Awareness Training

Technical Data Security Services: 5 Requirements

1. Access Control
2. Audit Controls
3. Authorization Control
4. Data Authentication
5. Entity Authentication

Technical Security Mechanism: 1 Requirement

1. Protections for health information transmitted over open networks via:
   - Integrity controls, and
   - Message authentication, and
   - Access controls OR encryption

Dash Board For Evaluation

- # staff - # volunteers - % trained
- # of clients
- # of security incidents
- Have list of systems containing PHI and know location of system and who is data steward -# of items on list
- Confidence that unit has good physical security

Dash Board For Evaluation

- Have list of data interfaces -# of data interfaces
- Have list of contracts/business associates - # of contracts/business associates
- Allow PHI to be put on personal PCs or in Email or loaded to WEB site

Dash Board For Evaluation

- Have to do list for securing computer systems - # of items on list
- Have process to receive/communicate HIPAA compliant risk - # of items on list