Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Privacy Meets Security – Data Protection Statutes

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 2

Sarbanes-Oxley Act of 2002

- "To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes."
- In response to financial scandals
  - Enron, WorldCom, Tyco
  - Arthur Andersen

Organization

- 11 sections with requirements procedures; e.g.
  - Companies evaluate and disclose the effectiveness of their internal financial controls
  - CEO & CFO certify accuracy of reports
  - Fully independent audit committees and auditors
  - Increased insider trade reporting

SOX Provisions

- Established Public Company Accounting Oversight Board (PCAOB)
- Auditor Independence
- Corporate Responsibility
- Enhanced Financial Disclosures
- Analyze Conflicts of Interests
- SEC Resources and Authority

And More SOX?

- Studies and Reports
- Corporate and Criminal Fraud Accountability
- White Collar Crime Penalty Enhancements
- Corporate Tax Returns
- Corporate Fraud Accountability

Penalties Severe

Failure to comply or submission of an inaccurate certification	Fine up to $1 million and ten years in prison
A wrong certification submitted purposely	Fine up to $5 million and twenty years in prison.
Violate SEC regulations	May be ineligible to hold a director or officer position in any publicly traded company

404: Viable Internal Controls

- Creation and maintenance of internal controls
  - Separation of duties
  - Checks and balances
  - Documentation of events
  - Internal controls
- Internal controls include
  - Policies
  - Procedures
  - Training programs
  - Other processes (example: inventory control)

SOX Section 404 & IT

- SOX internal controls
  - Requires annual statement of the *"effectiveness of the company's internal control structure and procedures for financial reporting" and "must disclose any material weakness"*
  - IT controls underlie other process controls - thus section 404 requires good IT controls

HIPAA

- The Health Insurance Portability and Accountability Act (HIPAA) Healthcare providers must ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits
- Privacy Rule – any PHI
  - Mini-security rule
- Security Rule – ePHI

Covered Information

- Protected Health Information (PHI) includes patient identifiable data such as:
  - Names, addresses, dates, phone numbers, email addresses, SSN, license numbers, IP addresses, account numbers, etc.
  - Any patient information created or received relating to past, present, or future condition; provision of health care; past, present, or future payments for health care provision
- De-identified health information is not considered PHI

Privacy Rule

- Disclose policies for use and disclosure of information
- Privacy compliance program, including staff training

Enforcement

- Civil and criminal
- HHS
  - Office of Civil Rights (OCR) – Security and Privacy Rules
  - Inspector General (IG) - Audits
- DoJ – criminal referrals
- Doesn't preclude private actions based on tort

CIA

"Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits"

- A widely used benchmark for evaluation of information systems security
- A system possessing all three of these properties all of the time is secure
- A system not possessing one or more of these properties at any time isn't

Confidentiality

The concealment of information or resources

- A requirement that private or confidential information not be disclosed to unauthorized individuals.
- Also applies to the *existence* of private or confidential information

Integrity

The trustworthiness of information or resources

- A requirement that private or confidential information not be modified or deleted by unauthorized individuals.

Availability

The ability to use the information or resources when desired

- A requirement that a system be able to provide access to requested information whenever needed
- Attempts to block availability are called *denial of service* (DOS) attacks

The HIPAA Security Rule

- Requires covered entities to:
  - Ensure protection against any reasonably anticipated threats or hazards to the security or integrity of information
  - Protect against reasonably anticipated uses and disclosures
  - Ensure compliance by workforce
  - Review and modify security measures periodically to continue reasonable and appropriate protections

Policies, Procedures and Documentation

- Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the security rule
- Ensure that written or electronic records of policies and procedures implemented to comply with the security rule be maintained for a period of six years from the date of creation or the date when last in effect

Implementation Specifications

- Grouped into 5 Categories
  - Administrative
  - Physical
  - Technical
  - Organizational
  - Policies, Procedures and Documentation
- Identified as “Required” or “Addressable”
  - Required
  - Addressable - based on sound, documented reasoning from risk analysis

Administrative Safeguards

- Designate an individual responsible for HIPAA compliance for the organization
- Analyze security risks and implement policies and procedures that prevent, detect, and correct security issues
- Define sanctions for security violations
- Ensure members of the work force have access to information appropriate for their jobs
- Implement termination procedures
- Implement procedures authorizing access

Administrative Safeguards (Cont.)

- Implement
  - a security awareness and training program
  - policies and procedures for reporting and responding to security incidents and other emergencies
- Periodically monitor adherence to security policies and procedures, document results, and make appropriate improvements
- Establish contracts between a covered entity and business associates to ensure appropriate safeguards are in place to protect ePHI

Physical Safeguards

- Limit physical access to equipment and locations that contain or use ePHI
- Specify workstation and work area roles and assignments where workstations with access to ePHI are located
- Specify how workstations permitting access to ePHI are protected from unauthorized use, including laptops, PDAs, etc.
- Address the receipt and removal of hardware and electronic media that contain ePHI.

Technical Safeguards

- Implement policies and procedures limiting access to ePHI to persons or software programs requiring the ePHI to do their jobs
- Install hardware, software, or manual mechanisms to examine activity in systems containing ePHI
- Ensure policies and procedures that protect ePHI from being altered or destroyed
- Implement mechanisms to protect ePHI that is being transmitted electronically from one organization to another

Organizational Requirements

- Document that business associate contracts or other arrangements comply with the security measures when handling ePHI
- Ensure that business associates have plans that document appropriate safeguards for ePHI

FCRA/FACTA

- Fair Credit Reporting Act/Fair and Accurate Credit Transactions Act of 2003
- 15 USC 1681 et seq
- Prescreen opt-out notice
  - 16 CFR 642

Major FACTA Provisions

- Free report - Annualcreditreport.com
- Prescreen opt-out notice
- Disclose credit scores to mortgage applicants
- Credit report fraud alert
- ID Theft database
- Eased employee notification requirements when records checked in wrongdoing investigation
- Red Flag rules

FACTA/FCRA

- Credit reports on file with credit bureaus
- Other files of information collected and maintained on consumers, depending on their content and use.
  - Medical information
  - Information used to prevent and detect fraud
- Disclosure for authorized purposes
- Amount of info varies with purpose

Red Flag Rules

- To detect and stop identity thieves from using someone else's identifying information to commit fraud
- To address identity theft problems
- Identify and address problematic information
- Six enforcing agencies

Red Flag Rule Requirements

- Financial institutions and creditors with covered accounts must implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with:
  - the opening of a covered account, or
  - any existing covered account
- Program must be appropriate to the size and complexity of entity and nature and scope of activities.

Red Flag Rule Elements

- Must include reasonable policies and procedures to:
  - Identify relevant Red Flags and incorporate them into the Program
  - Detect Red Flags that are part of the Program
  - Respond appropriately to any Red Flags that are detected
  - Ensure the Program is updated periodically to address changing risks

Gramm-Leach-Bliley

- To protect consumers' personal financial information held by financial institutions
  - Non-Public Personal Information
- Broad definition of FIs
- Authority given to eight federal agencies and to states
- For FIs but good model for others

NPI

- **NPI Includes:**
- Nonpublic personally identifiable financial information; and
- Any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.

PII Definition - AICPA/CICA

- Information related to identified or identifiable individual
  - Name, Address, Telephone, SS # or Other Govt ID Numbers
  - Employer, Employment History
  - Credit Card Numbers, Credit History, Purchase History
  - Personal or Family Financial or Medical Information

Usual State PII Definition

- First and last name OR last name and first initial - plus
  - Social Security Number OR
  - Drivers' License Number OR
  - State Identification Number OR
  - Debit or Credit Card Number OR +
  - Financial Account Number OR
  - Medical Information OR
  - Health Insurance Information
- Most state notification laws require PIN or access code be disclosed to include account numbers in definition

Sensitive Consumer Information

- In Interagency Guidance GLBA document issued by OCC, Federal Reserve, OTS, FDIC
- PII or combination of customer information that would allow someone to log onto or access the customer's account; *e.g.*, user name and password or password and account number.

GLB Overall Requirements

- Administrative, technical, and physical protections
- Ensure confidentiality and security
- Protect against anticipated threats or hazards
- Protect against unauthorized access
- Comprehensive written information security program

GLB – Privacy Rule

- Governs the collection and disclosure of customers' personal financial information by financial institutions
- Also applies to companies, whether or not they are financial institutions, who receive such information

GLB – Safeguards Rule

- Requires all financial institutions to design, implement, and maintain safeguards to protect customer information. Reasonable policies
- Applies to
  - financial institutions that collect information from their own customers,
  - financial institutions such as credit reporting agencies that receive customer information from other financial institutions.

Safeguards Rule Objectives

- Ensure the security and confidentiality of customer records and information – in paper, electronic or other form
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of any records or information which could result in substantial harm or inconvenience to any customer

Safeguards Specifics

- Designate coordinator
- Identify reasonably foreseeable risks
- Design and implement safeguards for risks
- Oversee service providers

Security Program

- Comprehensive process oriented approach
  - Identify assets
  - Conduct periodic risk assessments
  - Develop and implement program that addresses specific requirements
  - Monitor and test program
  - Continually review and adjust
  - Oversee third party provider arrangements and practices
- Check relevant external standards

Security Factors

- Representations
- Practices to protect and detect
- Reasonableness
- Reaction
- Demonstrable harm
- Orders require remedies, provisions, and audits

FTC Act Section 5

- “Any unfair or deceptive act or practice in or affecting commerce” is unlawful
- Basis for security investigations that do not fall under GLBA jurisdiction

HITECH Act of 2009

- Part of American Recovery and Reinvestment Act (ARRA) of 2009
- HITECH Act
  - Incentive programs for developing electronic health records systems
  - EHR – Electronic Health Records
  - PHR – Personal Health Records

HITECH Act Breach Provisions

- Also included first clear federal affirmative requirements for private sector breach disclosure notification
- Breach enforcement responsibilities split between HHS and FTC
  - HHS – traditional HIPAA "covered entities"
  - FTC – non-covered entities
    - Personal health records systems

HITECH Act Breach Regulations

- HHS and FTC issued own regs
- Differences
  - Statute limited HHS discretion
  - Historical attitude and activity

HHS

- Document procedures to prevent and react
- Provide affected individuals with timely notice (i.e., no later than 60 days) upon the discovery of a breach of *unsecured* PHI if
  - breach poses significant risk of financial, reputational or other harm to the individual.
- HHS "secured" definitions
  - E-data - unusable, unreadable, or indecipherable to unauthorized individuals
  - Paper - destroyed

HHS Notice Requirements

- Include brief description of the event that led to the breach, specific PHI involved, and steps affected individuals should take to protect themselves from further harm.
- If breach involves more than 500 individuals, notify the media and HHS Secretary.
- Breaches involving fewer than 500 individuals must be reported to the HHS Secretary on annual basis.

HHS Third Parties

- Business Associate agreements must require contractors to follow HIPAA and HITECH
- Business associates of covered entities (e.g., third-party administrators, pharmacy benefit managers) must notify related covered entity upon the discovery of a breach of unsecured PHI.
- The covered entity then must provide the affected persons with notice.

FTC

- Covers PHR vendors and “PHR-related entities”
- Approach similar to HHS and adopts HHS definitions of items such as “secured.”

PHR-Related Entities

- "PHR-related entities"
  - (1) offer products or services through PHR vendor's website,
  - (2) offers products or services through the web sites of HIPAA-covered entities that offer individuals' PHRs, or
  - (3) access information in PHR or send information to a PHR.
- Similar to BA concept in HIPAA

Critical HHS/FTC Difference

- No risk of harm threshold in FTC rule
  - Must notify even where PHR vendor might reasonably conclude that presents small risk of harm to a consumer
  - Can rebut presumption of harmful acquisition of PHR.

Pending Legislation

- HR 2221 – Data Accountability and Trust Act (DATA)
- S 1490 - Personal Data Privacy and Security Act of 2009

HR 2221 – Passed House 12/8/09

- FTC must promulgate regulations that owners or possessors of electronic personal information establish security policies and procedures
- Authorizes FTC to set standards for destroying obsolete non-electronic data
- Security breach notification to FTC and individuals
- Preempts state information security laws

S. 1490 Broad Data Security

- Establishes standards for developing and implementing safeguards to protect the security of PII
- Civil penalties for violations of such standards.
- Notify: (1) individual whose information has been accessed or acquired; (2) nationwide CRAs over 5,000 involved; and (3) the U.S. Secret Service if over 10,000
- State AG can enforce

S. 1490 Other

- intentionally accessing a computer without authorization added to definition of racketeering activity
- Criminal penalties for concealing breach
- Special provisions for data brokers