

Legally-Defensible Security:

What new legal requirements and government enforcement mean for your organization's information security initiatives

Elizabeth Johnson
Of Counsel
Poyner Spruill LLP
(919) 783-2971
ejohnson@poyners.com



Poyner Spruill^{LLP}

ATTORNEYS AT LAW

These materials have been prepared by Poyner Spruill LLP for informational purposes only and are not legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship.



Poyner Spruill

- 117 attorneys
- 4 offices – Raleigh, Charlotte, Rocky Mount, Southern Pines
- 35 practice areas
- 28 attorneys in Best Lawyers in America®
- Interdisciplinary Privacy and Information Security practice area – 10 attorneys

Why would you need to defend your information security program?

- Multiple sources of information security requirements invite allegations of noncompliance
 - Government agency enforcement
 - Private lawsuits
- Breach notification may bring scrutiny on your program
 - Notify affected individuals, multiple regulators, clients, CRAs, media
- Your program becomes Exhibit A in resultant government agency enforcement action and client or individual lawsuits

Roadmap

- Sources of information security requirements
 - Federal laws and regulations
 - State laws and regulations
 - Contracts
 - Government agency enforcement
 - Private lawsuits
- What you should do first to address the situation
 - Create and implement a documented information security program
 - Mitigate biggest risk areas (and what are those?)

Federal Laws



HIPAA

- Applies to:
 - “Covered Entities” – health care providers, health care clearinghouses, and **HEALTH PLANS**
 - “Protected Health Information” – individually identifiable health information held or transmitted by a covered entity or its business associate that:
 - Identifies the individual or for which there is a reasonable basis to believe it could be used to identify the individual; and
 - Relates to past, present or future physical or mental health or condition; provision of health care to the individual, or past, present, or future payment for care
 - Business Associates
 - Subcontractors

HIPAA Security Rule

- Only applies to Electronic PHI
- Requires implementation of administrative, physical and technical safeguards to protect ePHI
- Employee assigned with responsibility for program
- Physical and technical access management
 - Authorization
 - Establishment
 - Modification
 - Termination

HIPAA Security Rule (2)

- Person or entity authentication
- Security awareness and training
- Security incident response procedures
- Contingency and disaster recovery planning
- Emergency mode operation plan
- Data back-up
- Device and media controls
- System logging and monitoring

HIPAA Security Rule (3)

- Data integrity controls
- Encryption of PHI in storage
- Encryption of PHI in transmission
- Facility access plan
- Workstation security
- Employee sanctions
- Periodic risk analysis and management
- Periodic compliance evaluations

HIPAA Security Rule (4)

- Vendor management
 - Covered entities fully liable for business associates, so diligence and ongoing oversight warranted
 - Security contract (business associate agreement) legally required
 - Several mandatory provisions must be included
 - Business Associates must fully comply with Security Rule (new requirement) (and parts of Privacy Rule)
 - Business Associates must downstream all requirements to subcontractors
- **Program must be fully documented**

Gramm-Leach-Bliley Act

- Applies to “financial institutions”
 - Defined broadly to include banks, mortgage lenders, financial advisors, brokers, pay day lenders, money order providers, check cashing services, auto dealers who provide financing or leasing, insurance companies, etc.
 - “Nonpublic personal information” – generally speaking, any non-publicly available information about an individual consumer of a financial institution, including the fact that the individual is a customer (but only if individual did business in a personal capacity)
- Federal financial regulators issue rules to implement
- States regulate insurance industry (based on domicile)

GLBA Safeguards Rule

- Administrative, technical, and physical safeguards
 - Appropriate to size and complexity, nature and scope of activities, and sensitivity of customer information
- Employee(s) designated to coordinate program
- Identify reasonably foreseeable internal and external risks to security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information

GLBA Safeguards Rule (2)

- Assess the sufficiency of any safeguards in place to control risks, which must consider:
 - Employee training and management;
 - Information systems, including network and software design, as well as information processing, storage, transmission and disposal;
 - Detecting, preventing and responding to attacks, intrusions, or other systems failures
- Design and implement information safeguards to control the risks identified
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures

GLBA Safeguards Rule (3)

- **Oversee service providers with access to NPI by**
 - Taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for NPI
 - Requiring your service providers by contract to implement and maintain such safeguards
- **Evaluate and adjust program in light of:**
 - Results of required testing and monitoring
 - Material changes to operations or business arrangements
 - Any other circumstances that may have a material impact on information security program
- **Program must be fully documented**



State Laws



Massachusetts Regulations

- Applies to all persons who own, license, store or maintain personal information about a Massachusetts resident
- Requires a comprehensive information security program with administrative, technical and physical safeguards
- Designating one or more employees to maintain program
- Risk assessment and management
- Ongoing monitoring/evaluations of program effectiveness as well as an annual review of scope of safeguards
- Policies related to storing, accessing and transporting records off business premises

Massachusetts Regulations (2)

- Training
- Sanctions
- Restricting physical access to records containing PI
- Security incident response procedure
- Secure access controls and user authentication protocols
- Encryption of PI transmitted wirelessly or across public networks
- Encryption of PI on laptops and other portable devices
- System logging and monitoring

Massachusetts Regulations (3)

- Up-to-date firewalls, security patches and malware protection
- Oversight of service providers with access to PI
 - “Reasonable steps” to retain service providers “capable of” maintaining security measures “consistent with” these regulations and federal requirements
 - Requiring service providers to implement such security measures by contract (existing contracts grandfathered until March 2012)
- **Program must be fully documented**

Nevada Statute

- Applies to organizations doing business in the state
- Requires compliance with PCI DSS for any business that accepts payment cards
- For everyone else, requires encryption of
 - Portable devices containing personal information and transported outside the “logical or physical controls” of the business (electronic or optical media, including smart phones)
 - Personal information transmitted electronically, other than by fax, “outside the secure system of the business
- Encryption = NIST standards

Other States

- General Security Requirements
 - Implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure
 - Service provider contracts must require same
- Topic-Specific Requirements
 - Disposal
 - Particular methods, written disposal policy, certain types of diligence regarding disposal vendors
 - SSNs
 - Transmission security, requiring to access website, embedding in cards, written policies



Contracts



Contractual Obligations

- Provisions required by law
 - See above (HIPAA, GLBA, Massachusetts, Nevada, California, North Carolina, etc.)
- Additional obligations
 - Breach reporting and mitigation
 - Audit rights
 - Encryption
 - Cost shifting
- International

Payment Card Industry Data Security Standard

- Applies to merchants processing payment card data
- Typically applies via contract
 - But some states have incorporated in statutes or provided for merchant liability in event of violation
- Requirements
 - Firewalls and malware protection
 - Physical and technical access controls
 - Encrypt transmitted card holder data
 - Test systems and monitor access
 - Larger volume merchants must obtain a third party compliance assessment; smaller volume merchants can do a self-assessment
 - **Documented Security Program**

Government Enforcement



How Does Enforcement Happen?

- Follows from an individual's complaint
- Follows a reported information security breach
 - 46 states, Puerto Rico, Virgin Islands, D.C.
 - Federal financial regulators
 - HHS (HIPAA covered entities and business associates)
 - FTC (vendors of personal health records)

What's the Pattern?

1. Incident is notified to individuals and regulators (or an individual complains privacy rights were violated)
2. Agency files complaint:
 - Alleges legal violations (HIPAA, state law, etc.)
 - Unfair and deceptive trade practices rationale
3. Settlement is reached in which:
 - Agreement to implement a comprehensive security program
 - Agency retains oversight authority
 - Periodic assessments required over a long period

FTC Enforcement

- Agency identifies a security breach
- Alleges violation of section 5 of the FTC Act – “unfair and deceptive trade practices”
- Advances one or both of the following theories:
 - Circumstances demonstrate lax security that is “unfair”
 - Circumstances render privacy notice “deceptive”
- Settlement includes
 - Requirement to implement a “comprehensive, written information security program”
 - Audits every other year for 10 or 20 years with agency oversight
 - Various other equitable remedies

FTC Enforcement – Specific Security Allegations

- DSW
 - Stored information in multiple files when it no longer had a business need to keep the information
 - Stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password
- TJX
 - Stored and transmitted personal information in clear text
 - Did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks

FTC Enforcement – Specific Security Allegations (2)

- Reed Elsevier Inc. and Seisint, Inc.
 - Failed to establish or enforce rules sufficient to make user credentials hard to guess; allowed customers to use the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password
 - Failed to require periodic changes of user credentials, such as every 90 days, for customers with access to sensitive nonpublic information
 - Failed to suspend user credentials after a certain number of unsuccessful log-in attempts
 - Allowed customers to store their user credentials in a vulnerable format in cookies on their computers



FTC Enforcement – Specific Security Allegations (3)

- Twitter
 - Failure to use strong passwords
 - Failure to maintain separate site for administrator log on
 - Employees storing passwords in email accounts
- Dave & Buster's
 - Failure to employ sufficient measures to detect and prevent unauthorized access, such as an intrusion detection system and monitoring system logs
 - Failure to monitor and filter outbound traffic from networks to identify and block export of information without authorization

Evolution FTC Enforcement

- Becoming increasingly granular in allegations
- “Unfair” trade practice and “reasonable” security are subjective standards that evolve with:
 - Technology
 - Types of attacks and risks
 - Best practices
- Security flaws typically do not otherwise constitute a legal violation (no underlying HIPAA or state law violation alleged by FTC)
 - Meeting your statutory/regulatory obligations may not be enough

HHS Enforcement

- Penalties
 - \$100 - \$50,000 per violation, depending on level of culpability
 - \$1.5 million maximum cap on violations of an identical HIPAA provision in calendar year
- Business associates can now be held directly liable for violations (proposed rule, not yet final)
- OCR has stated it will conduct compliance reviews of all entities reporting a breach affecting 500 or more and will contract with third parties to conduct audits
- Reportedly intends to use settlement monies to fund future enforcement actions

Piedmont Hospital

- March 2007 – HHS Office of Inspector General conducts audit of Piedmont Hospital in Atlanta
- 42 questions requiring written response within 10 days (not business days)
- Audit ultimately lasted several months

[www.computerworld.com/s/article/9025253/
HIPAA audit The 42 questions HHS might ask](http://www.computerworld.com/s/article/9025253/HIPAA_audit_The_42_questions_HHS_might_ask)

Providence Health

- Series of security incidents:
 - Four incidents of stolen, unencrypted laptops in late 2005 and early 2006
 - Unencrypted backup tapes and optical disks stolen from an employee's car in late 2005
- HHS receives about 30 complaints
- July 2008, becomes public that HHS pursued an enforcement action
 - Parties enter into a resolution agreement
 - Providence does not concede HIPAA liability
 - HHS does not concede that Providence is not liable

Providence Health (2)

- Features of the enforcement action:
 - Implies that encryption is a required technical safeguard, although Rule lists as “addressable”
 - Providence pays \$100,000
 - Equitable remedy – “Corrective Action Plan” filed with resolution agreement
 - Details policies and procedures
 - HHS retains final approval authority
 - Implementation report detailing training, etc. due within 120 days of HHS’s approval of policies and procedures.
 - Entity must monitor own compliance quarterly
 - Entity must file a compliance report with HHS annually for duration of agreement (3 years)

Joint HHS-FTC Enforcement

- CVS Caremark
 - First joint FTC and HHS enforcement to HHS
 - \$2.25 million
 - Corrective action plan / comprehensive info security program
 - Assessments and compliance reports (HHS – annually for 3 years, FTC – biennially for 20 years)
- Rite Aid
 - \$1 million, same as above
- Walgreens under investigation
- All alleged violations occurred prior to notification requirement and increase in maximum penalties
- HIPAA-related allegations limited to Privacy Rule

State Agency Enforcement

- What are they enforcing?
 - Little FTC Acts
 - State breach notification laws
 - State disposal laws
 - State attorneys general now can enforce HIPAA



State Agency HIPAA Enforcement

- CT Attorney General
 - Health Net settlement of \$250,000 (plus cost of 2 years of credit monitoring), additional payment of \$500,000 if any ID theft results
 - Corrective action plan
 - First ever state AG HIPAA enforcement action
 - 1.5 million affected, 500,000 in CT
 - Occurred pre-HHS Breach Notice Rule
- Investigating BCBS, Griffin Hospital, ECMC (student loan data), and Yale Medical School
- The “elected official effect”

State Agency Breach Enforcement

- Multi-State Actions
 - Choice Point (also the FTC)
 - TJX (also the FTC)
- Oregon Attorney General
 - Providence Health System (also HHS)
- CA Dept Public Health
 - \$1.8 million in fines against 143 hospitals for failure to report “adverse events” (including breaches)
 - \$1.12 million in fines against 8 hospitals (as of June) for experiencing breaches

State Agency Breach Enforcement (2)

- NY Attorney General
 - Barnes & Noble (website security flaw)
 - Datran Media (improper use of personal information)
 - CS Stars LLC (lost laptop)

State Agency Disposal Enforcement

- NC Attorney General
 - Prompt Med (\$50,000)
- Massachusetts (U.S. Attorney)
 - Plastilam (\$25,000)
- TX Attorney General
 - About two dozen entities (generally 10s of thousands)
- Ensure that you have a documented disposal policy (not specifically required by HIPAA, but required by state laws)

Private Lawsuits



Private Lawsuits

- Lawsuits by individuals affected by security breach
 - Theories of liability
 - Fail for lack of damages
 - Settle where identity theft has occurred
- Lawsuits by clients enforcing contracts
 - *Experi-Metal, Inc. v. Comerica Bank*
 - Phishing email used to “lure” EMI into providing authentication credentials that facilitated fraudulent wire transfers
 - EMI’s argument fails due to its earlier execution of a contract, under which it agreed that all of Comerica’s existing and future security was “commercially reasonable” as a matter of law

What Should You Do Next?

- Create/Enhance a Documented Information Security Program
- Mitigate Risks



Documented Information Security Program

- Needs to incorporate all specific features required by laws, regulations, or agency guidance documents that apply to your organization
- Needs to address issues targeted by public and private enforcement actions (e.g., passwords stored in email)
- **MUST BE FULLY DOCUMENTED**
- Worry about the scope of your policies and procedures
- Consider legal review of program and/or legal involvement in audits and assessments
- Incorporate periodic review (legal, organizational and technological changes)

Mitigating Risks – Actual Breaches

- Common Causes of Breach
 - Portable media
 - Portable records (hard copies)
 - Vendors
 - Hackers and malicious insiders
 - Natural disasters?

Portable Media

- Account for 35% of breaches (Ponemon) (45% HHS list)
- Example
 - Univ. of Utah Hospitals & Clinics – computer tapes stolen from vendor's car contained 1.5M patient billing records (some 30 yrs old)
 - \$3.4M in costs (so far) without factoring in reputational damage and lost productivity (reportedly fielded 11,000 calls from worried patients and spent 6,632 personnel hours on response)
- Mitigation
 - Encryption
 - Data loss prevention
 - Policies and training
 - Records management (get rid of data no longer needed for compliance or business purposes)

Portable Records (Hard Copies)

- Account for 22% of breaches (HHS list)
- Examples
 - Boston Globe – Printed credit card numbers on reverse side of distribution sheets bound to stacks of newspapers for circulation
 - BCBS Association – Mailhouse vendor's mis-mailing resulted in PHI of 15,000 individuals sent to incorrect recipients
- Mitigation
 - Handling policy and training
 - Disposal policy and training
 - Diligence/contracts with records management/disposal (and other) providers
 - Mailing failsafe

Service Providers/Vendors

- Cause 44% of breaches and increase cost about 25% (Ponemon)
- Examples
 - South Shore Hospital – Lost shipment of backup tapes containing PHI and PI of 800,000 people; Iron Mountain Data Products, now called Archive Data Solutions, was hired to dispose of records; job was subcontracted “without South Shore Hospital’s prior knowledge” to Graham Magnetics, which attempted to ship the tapes to a Texas facility for destruction
 - Lincoln Medical and Mental Health Center – Lost CDs containing PHI and financial information of 130,000 persons; CDs handled and shipped by Siemens Medical Solutions USA, Lincoln’s billing and claims processor
 - See also prior two slides (University of Utah and BCBS Assoc.)

Service Providers/Vendors (2)

- Mitigation
 - Diligence, diligence, diligence
 - Contracts, contract, contracts (indemnification)
 - Control of subs
 - Insurance?
 - Enforcement
- Remember that not all vendors are business associates (so need contracts other than BAAs)
- Remember that business associates may handle PI that is not PHI (so scope of BAA might not cover all issues)

Hackers and Malicious Insiders

- Cause 12% of breaches (Ponemon) (28% - Privacy Rights Clearinghouse)
- Examples
 - DSW – Hackers accessed payment card and check details of 1.5 million customers (including a VIP customer)
 - UNC-CH – Hackers accessed data on 236,000 women enrolled in UNC study (part of the Carolina Mammography Registry)
 - Countrywide – Insider steals and sells information on unknown number of customers; highest reported estimate is 17 million
- Mitigation
 - Penetration testing, firewalls, intrusion detection, etc.
 - Systems activity review – logging **and** monitoring
 - Insurance (but beware of carve-outs)

p.s.

Poyner Spruill^{LLP}
ATTORNEYS AT LAW

www.poynerspruill.com

Natural Disasters

- Unclear how many breaches are caused by natural disasters (probably very few), but highlights the unpredictable and inevitable nature of breaches
- Example
 - Cornerstone in Nashville, TN reports that unprecedented flooding broke office windows and hard copy records “may have been removed from the building by flood waters.”
- Mitigation
 - Back-up copies
 - Insurance (but beware of carve-outs)

Questions?

Elizabeth Johnson
Of Counsel
Poyner Spruill LLP
(919) 783-2971
ejohnson@poyners.com