

Data Security

Protection and Compliance Basics

John L. Culhane, Jr., Consumer Financial Services

Mark J. Furletti, Consumer Financial Services

Jean C. Hemphill, Health Care

Beth Moskow-Schnoll, Corporate/Government Investigations, Health Care

Amy Underwood, Health Care

Focus of Today's Program

- I. Overview of applicable federal, state and local laws
- II. Assessment, risk management and prevention
- III. Handling breaches and other unauthorized disclosures
- IV. Dealing with government investigations and lawsuits

Data Security – What are we talking about?

- Protecting the security and integrity of data in your information systems
 - Proprietary business information
- Protecting the privacy of your customer/patient personal information (individually identifiable information)
 - Identity theft for financial fraud
 - Commercial use of information
- Primarily electronic information but some laws and regulations apply to information in ANY medium (including paper records)

Our Focus: Data Security for Lawyers

- Contractual negotiations
- Compliance
- Risk Management
- Litigation management

I. Federal Laws & Self Regulation Applicable to Financial Data

- Gramm-Leach-Bliley Act
 - Data Safeguards Rule, 12 CFR Pts. 30 (OCC), 208 (FRB), 364 (FDIC), 570 (OTS) & 16 CFR Pt. 314 (FTC)
 - Unauthorized Access Guidance, 70 Fed. Reg. 15,736 (3/29/05)
- Fair Credit Reporting Act / Fair & Accurate Credit Transactions Act
 - Data Disposal Rule, 12 CFR Pts. 30 (OCC), 208 (FRB), 334 & 364 (FDIC), 571 (OTS) & 16 CFR Pt. 682 (FTC)
 - Red Flags Rule, 12 CFR Pts. 41 (OCC), 222 (FRB), 334 (FDIC), 571 (OTS) & 16 CFR Pt. 681 (FTC)
- Federal Trade Commission Act
- PCI Data Security Standard

Federal Laws Applicable to Health Data

- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
 - Covered entities (health care providers, plans and clearinghouses)
- Health Information Technology for Economic and Clinical Health Act of 2009 (part of ARRA (the economic stimulus bill)) (“HITECH”)
 - HHS security standards for covered entities
 - FTC security standards for electronic medical records

Federal Laws Applicable to Federal Government

- Federal Information Security Management Act of 2002 (part of E-Government Act of 2002) (“FISMA”)
 - Comprehensive framework for ensuring effectiveness of information security controls over Federal data
- Homeland Security Presidential Directives (“HSPD -7”)
 - Identification standards for government employees and contractors

State Data Security Laws Applicable to Private Entities

- Pennsylvania
 - 73 PA. CONS. STAT. ANN. §2303(b)
- New Jersey
 - N.J. STAT. ANN. §56:8-163
- Delaware
 - DEL. CODE ANN. tit. 6, § 12B-101-104

Gramm-Leach-Bliley Act & Data Safeguards Rule

- Applies to “nonpublic personal information” in the possession of “financial institutions”
- Requires institutions to develop an information security program that is appropriate to:
 - the institution’s size and complexity
 - the nature and scope of its activities
 - and the sensitivity of the information it obtains
- Program must address administrative, technical and physical safeguards

Gramm-Leach-Bliley Act & Unauthorized Access Guidance

- Applies to federally-regulated financial institutions
- Requires institutions to develop and implement a “response program” to address unauthorized access to or use of “sensitive customer information” that could result in substantial harm or inconvenience
- Program should be “risk-based” (i.e., based on the institution’s size and complexity and the nature and scope of its activities)
- Institutions must have a procedure for containing unauthorized access and notify bank regulators, law enforcement and/or customers when there is a breach

Fair Credit Reporting Act / Fair & Accurate Credit Transactions Act & Red Flags Rule

- Applies to “creditors” and “financial institutions” that offer “covered accounts”
- Requires creditors and FI’s to develop their own “identity theft prevention programs” designed to detect, prevent and mitigate identity theft
- Program must be appropriate to the size and complexity of the institution and the nature and scope of its activities
- FTC’s Rule remains in limbo

Federal Trade Commission Act

- Section 5(a) gives FTC broad authority to pursue non-banks engaged in “unfair or deceptive acts or practices in or affecting commerce”
- “Unfair or deceptive” not defined, but FTC can rely on statute to pursue data-security-related violations that are not otherwise covered by its other rules, such as misrepresentations regarding:
 - the extent to which data is private
 - how a company uses data
 - data that a company collects

PCI Data Security Standard

- Developed by Visa, MasterCard, Amex, Discover & JCB
- Generally applies to merchants that accept credit, debit and/or prepaid cards
- Sets a data security “floor” that individual card networks can build upon
- Generally requires:
 - annual self-assessment
 - quarterly “vulnerability scans”
 - “attestation of compliance”

HIPAA pre- HITECH: An Overview

- Aimed to promote use of electronic media for medical information
- Addressed privacy and security of PHI
- Regulations included
 - Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”)
 - Security and Electronic Signature Standards (“Security Rule”)
- Applied to Covered Entities (“CE”)
- Not employers (at least not directly)
- Not business associates (at least not directly)

Health Information Technology for Economic and Clinical Health (HITECH)

- HHS security standards for covered entities
- FTC security standards for electronic personal health records
- Part of the February, 2009 economic stimulus bill
- Amends certain HIPAA standards
- Effective - September 2009
- Enforcement/civil penalties associated with compliance – February 2010

HIPAA post-HITECH

- Major expansion of the scope and applicability of the Privacy Rule
- Expansion of HIPAA regulation of “business associate”
 - Directly subject to certain aspects of HIPAA, including breach notification (rather than contractual obligation by CE)
- New and increased penalties and enforcement provisions
 - Per violation cap raised to potential \$1.5M (previous cap of \$25,000)
- First federal law mandating breach notification

FTC Personal Health Record Security Rule

- FTC requirements similar to HHS
- Applies to
 - vendors of personal health records
 - PHR-related entities
 - and their third-party service providers
- Includes notification requirement --does not overlap with HHS requirements in order to avoid consumers receiving multiple notifications of the same breach of electronic PHI

De-Identified Health Data

- No reasonable basis to believe the information can be re-identified
- Two Ways to De-Identify:
 1. Formal determination by a qualified statistician certifying that information meets this standard or
 2. Removal of 18 specific identifiers of the data such that the remaining information could not be used to identify the individual
- Once De-Identified, it is no longer PHI
- No legislative requirement to obtain consent from patients and the other stipulations of privacy laws would not apply

Information Stripped of Customer Identifier

- Nonpublic personal information does not include:
 - “Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.” 16 CFR 313.3(o)(2)(ii)(B)
- Allows businesses to provide information for surveys, financial modeling, or for other types of demographic studies

What is Unsecured PHI?

- Not protected by “technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals”
- Basically information that is not **encrypted** or **destroyed** (per National Institute of Standards and Technology Standards)

Unsecured PHI

- Data comprising PHI can be vulnerable to breach in any of these commonly recognized data states:
 - “data in motion” – data that is moving through a network, including wireless transmission
 - “data at rest” – data that resides in databases, file systems, and other structured storage methods
 - “data in use” – data in the process of being created, received, updated or deleted
 - “data disposed” – discarded paper records or recycled electronic media

Encrypting PHI

- Guidance requires use of a NIST approved algorithm and procedure to be considered unreadable
- Electronic PHI is encrypted when (1) “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304) and (2) key to decrypt the PHI has not been breached
- Entities should retain encryption keys on separate device from the one housing the encrypted data

Destruction

- Destruction is also considered an acceptable method of rendering PHI unreadable and/or unusable
- Acceptable methods for destroying PHI at this time:
 - Paper, film, or other hard copy media be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed; and
 - Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88 Guidelines for Media Sanitization, such that the PHI cannot be retrieved. (Guidance at 17).
 - Redaction of paper records is not an alternative to destruction (but may create a Limited Data Set)

Fair Credit Reporting Act / Fair & Accurate Credit Transactions Act & Data Disposal Rule

- Applies to “any person” that maintains or otherwise possesses “consumer information”
- Requires “proper disposal” of consumer information
 - Must burn, pulverize or shred paper
 - Must destroy or erase electronic files/media
 - Conduct due diligence of any document destruction contractors
- Must incorporate data disposal procedures into data safeguards program

II. Assessment, Risk Management & Prevention

- Informatics: the sciences concerned with gathering, manipulating, storing, retrieving, and classifying recorded information
- Data security is an art as much as a science
 - The level of data security controls will depend on the size and nature of the information and the organization
 - Judgment must be exercised: Compliance tolerance level, enterprise risk assessment and available resources (manpower and financial)

The Science: It's All About Standards and Controls

- Fundamentals of a Data Security Program
 - Administrative Standards
 - Technical Standards
 - Physical Standards
- Understanding the required standards versus the addressable standards
- How you meet a standard is scalable depending on the nature, size and resources of your organization
 - E.g. encryption

The HIPAA Security Rule: General Overview

- Protects “e-PHI”
- Three types of safeguards: administrative, physical and technical
- Ensure the confidentiality, integrity and availability of e-PHI
- Protect against any reasonably anticipated threats or hazards to security or integrity
- Protects against any reasonably anticipated uses and disclosures of e-PHI not permitted or required under the Privacy Rule

Elements of an Information Security Program Under the Safeguards Rule

A Safeguards-Rule-compliant program must:

- Designate an employee to coordinate the program
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information
- Implement information safeguards to control identified risks
- Provide for the oversight of service providers
- Provide for the evaluation and adjustment of the program based on changes in business operations or other circumstances

Standardization of Security Control Concepts

- Security control structure, organization, baselines and assurances applicable to all government agencies are well articulated in NIST publications
 - NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations
 - NIST 200 Minimum Security Requirements for Federal Information and Information Systems
- Same standards are incorporated into Federal regulations
 - E.g., HIPAA Security Standards

The Bottom Line

- Important compliance responsibility – initially and on-going responsibility
- Documentation of your assessment process and decisions is key
- Annual assessment reviews

Your Data In the Control of Others

- Assuring data security practices of your vendors
- Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 ("SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes.
- Contractual assurances

Contractual Assurances

- Business Associate Agreements
- Data Use Agreements
- Key terms:
 - Ownership of data
 - Contractual obligation to maintain security controls to protect the security and integrity of your data
 - Restrict use of your data to performance of services and disclosures required by law
 - Use of de-identified data
 - Notice in the event of an unauthorized disclosure or suspected breach

Insurance and Indemnification Considerations

- Available insurance coverage depends on nature of the claim
 - Third party property loss v. personal injury
 - Remediation costs
 - Government investigations
- Indemnification
 - Unauthorized use and disclosures
 - Failure to de-identify properly

III. When the #*!* hits the fan

- Investigate the breach
- Mitigate the harm
- Protect against further breaches
- Notification?

FTC Breach Notification Rule

- FTC defines PHR identifiable health information as “individually identifiable health information” (as defined in HIPAA)
- Does not include “de-identified” information as defined in HIPAA; definition of “unsecured” references HHS Interim Final Rule
- An unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless vendor or entity that experienced the breach has reasonable evidence showing there has not been, or could not have been, any unauthorized access of information
 - Rebuttable presumption
 - Stolen laptop- demonstrate that files were never opened

HHS - Breach Notification for Unsecured Protected Health Information

- Breach: unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, *except* where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information
 - Occurs if four requirements met
 - Unauthorized
 - Unsecure
 - Significant risk of harm
 - No exception

Breach and Harm Threshold

- HHS defines “compromises the security or privacy” of such information as:
 - Poses a significant risk of
 - Financial
 - Reputational or
 - Other harm to the individual
 - Creates a harm threshold that is not in statute
 - Conforms federal breach notification law to most state law requirements
 - Must Perform a risk assessment to determine if there is significant risk of harm to individual as a result of the impermissible use or disclosure

Breach & Harm Threshold

- Requires fact-specific analysis
- De-identified information (not PHI) does not pose risk of harm
- Exceptions:
 - Unauthorized individual would not reasonably have been able to obtain the PHI
 - Good Faith or inadvertent access by or disclosures to workforce in same covered entity/business associate and does not result in further inappropriate use or disclosure

Notification In Case of Breach

- Notification to affected individuals
 - Written Notice
 - Electronic Notice if agreed to by the individual
 - Substitute Notice
- Notification to HHS
 - Contemporaneously with individual notice (for breach >500)
 - Log
- Notification to Media
 - If more than 500 residents in a State or jurisdiction affected
- Notification by business associate to covered entity

Content of Notification

- What happened
- Types of unsecured PHI involved
- Steps individuals should take to protect themselves
- What the covered entity is doing to:
 - Investigate the Breach
 - Mitigate Harm
 - Protect Against further Breaches
- Contact Procedures for questions/information

Timing

- Notification without unreasonable delay but not later than 60 days after “discovery”
- Breach is discovered on the first day it is known to covered entity or business associate
 - Known to any employee, officer, or other agent of such entity or associate, other than the person who committed the breach
- Subject to law enforcement delay if notice will “impede a criminal investigation or cause damage to national security”
- Burden on organization to prove compliance
- Need a plan to respond

Pennsylvania Breach Notification Law

- Breach of Personal Information Notification Act (BPINA)
73 Pa. Cons. Stat. Ann. § 2303
 - Notice to any resident of the Commonwealth whose “personal information” is obtained by unauthorized access to a computer system or database containing personal information in an unencrypted or un-redacted format
 - Notice must be provided if encrypted information is
 - Accessed and acquired in unencrypted form
 - Security key is accessed
 - AG may sue violators under the Unfair Trade Practices and Consumer Protection Law

New Jersey Breach Notification Law

- Identity Theft Prevention Act- N.J. STAT. ANN. §56:8-163
 - Requires notice of breach of security of unencrypted computerized personal information held by a business or public entity if the personal information “was, or is reasonably believed to have been, accessed by an unauthorized person”
 - No notice if a thorough investigation finds misuse of the information is not reasonably possible

Delaware Breach Notification Law

- Computer Security Breaches - DEL. CODE ANN. tit. 6, § 12B-101-104
 - Requires notice to consumers of breach in the security of “unencrypted computerized data” that compromises personal information if the investigation determines that misuse of information about a Delaware resident has occurred or is reasonably likely to occur
 - Notice must be in the most expedient time possible and without reasonable delay
 - Deemed in compliance if entity notifies affected residents in accordance with the maintained procedures when a breach occurs
 - AG may bring an action to address violations under Consumer Protection Division of the DOJ

IV. Increased HIPAA Enforcement & Penalties

- Compliance Audits & Investigations
- Enforcement of HIPAA by State Attorneys General
- Harmed Individuals Right to Receive Portion of Penalties Collected
- Increased Civil Penalties

Resolution Agreements

- Settlement agreement between HHS and CE that incorporates a corrective action plan (CAP)
 - Usually three years
 - Policies and procedures subject to HHS approval
 - Improved training
 - Monitoring of implementation and compliance
 - Includes payment of resolution amount
 - Examples: CVS and Providence

Criminal Penalties

HIPPA's Criminal Penalties Unchanged But Scope of Liability Broadened

Knowingly obtaining PHI in violation of law	1 year imprisonment \$50,000 fine
Committed under "false pretenses"	5 years' imprisonment \$100,000 fine
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	10 years' imprisonment \$250,000 fine

State AG Enforcement

- State AGs authorized to bring civil actions in federal court on behalf of its citizens harmed by HIPAA violations and may seek
 - Injunctive relief
 - Damages
 - Costs and attorneys fees
- AG must notify HHS of action and HHS has right to intervene
 - State may not bring action if there is pending federal action against same individual

(Section 13410(e))

Consequences of Violations by Financial Institutions/Merchants

- Cease and desist order issued by FTC/federal banking regulator and/or enforcement action by state AG (FCRA/FACTA)
- Civil penalties for violations of law can be assessed by banking regulators in administrative actions and civil penalties for violations of final cease and desist orders can likewise be assessed by FTC and banking regulators in administrative actions
- Civil penalties under FTCA and FCRA for knowing violations (up to \$3,500 per violation in enforcement action by FTC)
- Agency- or court-ordered restitution
- Remedies and statutory penalties in private actions available under FCRA/FACTA and/or applicable state statutes

Consequences of Violations by Financial Institutions/Merchants (continued)

- Loss of card-acceptance privileges under card network rules
- Potential exposure under state unfair or deceptive acts or practices statutes (e.g., Cal. Bus. & Prof. Code 17200)
- Potential breach of contract liability
- Potential tort liability (e.g., negligent enablement of imposter fraud)
- Reputational damage

Audits

- HHS required to perform periodic audits to ensure that covered entities and business associates meet the privacy and security provisions
- HHS required to conduct investigations of alleged violations of HIPAA due to “willful neglect”

Post-Breach Actions

- Re-assess technology systems, physical and administrative security
 - Determine causes and review access controls and procedures to ensure weaknesses are addressed and resolved
 - Determine necessary revisions to data collection, retention, storage and processing policies and procedures
- Evaluate Your Response
 - Implement changes to improve your effectiveness in preventing and responding to breaches

Prepare Now!

- Develop a Post- Breach Response Plan and Test before a Breach Happens
 - Identifying key management (CIO, Legal) and what role they will have when a breach happens
 - Communications plans, written policies and procedures in place regarding breaches
 - Periodically audit policies and procedures to ensure compliance
- Buy-In of Upper Management; Training of All Employees
- Know what regulations, statutes and contracts cover post-breach obligations
- Draft notices that are ready to be customized with specific facts
- Update response plan periodically

Sometimes even the best of plans can go awry

- Tales of trash and other hypotheticals
- Questions