FOLEY HOAG LLP

Driving Business Advantage

Compliance Approaches in the Changing HIT Privacy and Security Landscape

How You Can Nurture a Culture of Health Information Security and Privacy

March 2, 2011

Colin J. Zick
Foley Hoag LLP
(617) 832-1275
czick@foleyhoag.com

FOLEY HOAG LLP
Driving Business Advantage

Laws Impacting Data Privacy and Security

- Federal and 50 State Laws Governing:
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
  - Requirements for responding to data breaches and data losses
  - Penalties for data breaches and data losses

- And there are the international laws . . .

FOLEY HOAG LLP
Driving Business Advantage

List of U.S. Laws Impacting Data Privacy and Security

- Administrative Procedure Act. (5 U.S.C. §§ 551, 554-558)
- Cable Communications Policy Act (47 U.S.C. § 551)
- Cable TV Privacy Act of 1984 (47 U.S.C. § 551)
- Census Confidentiality Statute (13 U.S.C. § 9)
- Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501, et seq., 16 C.F.R. § 312)
- Communications Assistance for Law Enforcement Act of 1994 (47 U.S.C. § 1001)
- Computer Fraud and Abuse Act, as amended by the USA PATRIOT Act (18 U.S.C. § 1030)
- Computer Security Act (40 U.S.C. § 1441)
- Consumer Financial Protection Act of 2010 (Pub. L. No. 111-203, 124 Stat. 1376)
- Criminal Justice Information Systems (42 U.S.C. § 3789g)
- Counterfeit Access Device and Computer Fraud Abuse Act of 1984 (18 U.S.C. § 1030)
- Customer Proprietary Network Information (47 U.S.C. § 222)
- Driver's Privacy Protection Ac (18 U.S.C. § 2721)
- Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3)
- Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.), aka Stored Communications Act
- Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m)
- Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.)
- Employee Retirement Income Security Act (29 U.S.C. § 1025)
- Equal Credit Opportunity Act (15 U.S.C. § 1691, et. seq.)
- Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.)
- Fair Credit Billing Act (15 U.S.C. § 1666)

List of U.S. Laws Impacting Data Privacy and Security (cont.)

- Fair and Accurate Credit Transactions Act of 2003
- Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.)
- Fair Debt Collection Practices Act (15 U.S.C. § 1692, et seq.)
- Fair Housing Statute (42 U.S.C. §§ 3604, 3605)
- Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)
- Freedom of Information Act (5 U.S.C. § 552) (FOIA)
- Genetic Information Nondiscrimination Act (P.L. 110-233, 122 Stat. 881)
- Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, et seq.)
- Health Insurance Portability and Accountability Act (Pub. Law No. 104-191 § §262,264: 45 C.F.R. § §160-164))
- Health Research Data Statute (42 U.S.C. § 242m)
- HITECH Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5)
- Mail Privacy Statute (39 U.S.C. § 3623)
- Paperwork Reduction Act of 1980 (44 U.S.C. §3501, et seq.)
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Privacy Protection Act (42 U.S.C. § 2000aa)
- Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.)
- Tax Reform Act (26 U.S.C. § §6103, 6108, 7609)
- Telecommunications Act of 1996 (47 U.S.C. § 222)
- Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227)
- U.S.A. Patriot Act (Pub. L. 107-56) (bill extending three anti-terrorism authorities signed 02/25/11)
- Video Privacy Protection Act of 1998 (18 U.S.C. § 2710)
- Wiretap Statutes (18 U.S.C. §2510, et seq.; 47 U.S.C. § 605)

FOLEY HOAG LLP
Driving Business Advantage

Things to look for in 2011:

- Increased federal regulation in array of “hot” areas
  - Consumer privacy
  - Cyber security
  - Comprehensive breach notice
- More security breaches
- Battle within government to see who regulates what
- Increased government focus on national security aspects of security and privacy
- Increased corporate focus on internal cyber-security programs

REGULATORY OVERVIEW: HITECH ACT

- In March 2010, fulfilling what Senator Edward Kennedy described as “the great unfinished business of our society,” comprehensive health reform was adopted in the Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act.
- But, a year before, HIT changed first, via the Health Information Technology for Economic and Clinical Health Act (the “HITECH” Act), part of the American Recovery and Reinvestment Act of 2009 (“ARRA”).
- ARRA was enacted on February 17, 2009; it marked the first significant modification/expansion of HIPAA since 2003.

Areas Addressed by the HITECH Act and Related Regulations

- Guidance on technology/methods to render PHI unusable in the event of a breach
- Dealing with data breach, particularly breach notification
- Extension of privacy and security provisions to business associates
- Enforcement

FOLEY HOAG LLP
Driving Business Advantage

HITECH ACT REGULATIONS

- Even thought the law passed in early 2009, we are still waiting on and wading through many new regulations.
- You may remember that although HIPAA passed in 1996, the privacy regulations did not go into effect until 2001:
  - This type of delay is normal when dealing with a complex set of issues.
  - Delay can be a good thing, as it creates time to adjust and adapt.

DEADLINES

- February 17, 2010: the provisions of the HITECH Act regarding HIPAA business associates went into effect (albeit without regulations, which we have been expected to be issued any day now for over a year). Many HIPAA covered entities have been revising their Business Associate Agreements in an effort to comply with what they think the regulations will say. Others are waiting until they see the regulations to amend those agreements.

- February 22, 2010: FTC rules regarding health information breaches went into effect. The FTC has provided a standard reporting form for such breaches. And the FTC is putting its money where its mouth is: in the Fiscal Year 2011 Congressional Budget Justification, the FTC is seeking two full-time employees for "data security enforcement and rulemakings."

- March 1, 2010: Last but not least, the Massachusetts Data Security regulations went into effect on March 1, although we have not received much information from the Massachusetts Attorney General as to how these regulations will be enforced.

Guidance on Technology/Methods to Render PHI Unusable in the Event of a Breach

- When issued: April 17, 2009
- What is it? Guidance specifying the technologies and methodologies acceptable to render PHI, which is stored on paper or in electronic format, unusable, unreadable, or indecipherable to unauthorized persons.
- What does it mean? If you follow these standards for encryption, then you are within safe harbor and they would not be required to give the prescribed notification in the event of a breach.
- What do you have to do: Render PHI "unusable, unreadable, or indecipherable" to unauthorized individuals, or make notice for all breaches.

Federal Breach Notification Rules

- **When issued?** The interim final regulations were published in the Federal Register on August 24, 2009
- **What is it?** Breach notification for breaches from September 23, 2009 onward. No sanctions until February 22, 2010.
- **What does it mean?** HITECH defines "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information 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."
- **What do you have to do?** HITECH requires a covered entity to notify each individual "whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed" due to the breach. Here's the form: http://transparency.cit.nih.gov/breach/index.cfm

Privacy Rules for Business Associates

- When issued? July 8, 2010
- What is it? Extending to business associates many of the requirements in the Privacy Rules:
  - Establishing new limitations on the use and disclosure of protected health information for marketing and fundraising purposes
  - Restricting the disclosure of PHI) to health plans; expanding individuals' rights to access their information
- What does it mean?
  - HHS's proposed rules confirm the extension of HIPAA privacy and security rules to BAs (essentially making "business associates" into "covered entities.")
  - The proposed rule would add an addition circumstance to the existing two circumstances in current regulations where such authorization is necessary. Currently, authorization is required for (1) most uses and disclosures of psychotherapy notes; and (2) uses and disclosures for marketing. The third circumstance added by the HITECH Act – the sale of PHI – would require a covered entity (or business associate) to obtain authorization for disclosure of PHI that is in exchange for director or indirect remuneration, unless a specified exception applies.
- What do you have to do? HHS intends to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with "most of the rule's provisions."

Security Rules for Business Associates

- When issued? July 8, 2010
- What is it? Extending to business associates many of the requirements in the Security Rules
- What does it mean? HHS proposes a number of changes to the Security Rule including technical modifications as well as modifications to references to business associates.
- **What do you have to do?** HHS intends to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with “most of the rule’s provisions.”

Increased Enforcement/Penalties

- **When issued?** Increased penalties went into effect immediately but OCR held off on enforcement for a while.
- **What is it?** Increased enforcement at the federal level, new state enforcement and bigger penalties.
- **What does it mean?**
  - HHS transfers the authority for enforcement of HIPAA's security rules to OCR
  - OCR has a field force of 275 investigators that have an annual budget of $40 million Business associates under HIPAA are now subject to almost the same regulations as HIPAA covered entities.
- **What do you have to do?** These provisions will be in effect and apply at the time the final rule becomes effective or as otherwise provided.

HIPAA/HITECH Penalties

- Tier A: Accidental / unknowing violations
  - $100 fine for each violation, and the total imposed for such violations cannot exceed $25,000 for the calendar year.
- Tier B: Not accidental but a "reasonable case," but not "willful neglect."
  - $1,000 fine for each violation, and the fines cannot exceed $100,000 for the calendar year.
- Tier C: Willful neglect that the organization ultimately corrected.
  - $10,000 fine for each violation, and the fines cannot exceed $250,000 for the calendar year.
- Tier D: Willful neglect that the organization did not correct.
  - $50,000 fine for each violation, and the fines cannot exceed $1,500,000 for the calendar year.

The Number and Size of Breaches Continue to Rise

- At the end of February, OCR posted on its website a list of HIPAA "covered entities" that have reported breaches of unsecured health information affecting more than 500 individuals. OCR's posting showed 35 health data breaches that impacted over 700,000 individuals (with individual breaches ranging in size from 359,000 individuals, due to the theft of a laptop to 501 individuals impacted by the theft of a portable USB device). It's now over 100 and they haven't updated the list since June.
- This posting by OCR was required by the August 2009 Interim Final Rule, which was issued pursuant to the HITECH Act. In particular, § 164.408 of this breach notification interim final rule implements § 13402(e)(3) of the HITECH Act. The rule became effective September 23, 2009.
- Under this rule, breaches that affected 500 or more individuals must be reported to OCR within 60 days, via an OCR online notification form. Training materials and related guidance on breach notification can be found on the OCR web site.

Health Net Settlement in Connecticut

- On July 6, 2010, the Connecticut Attorney General Announced Health Net Settlement. First state HIPAA enforcement action.
- Blumenthal sued after Health Net allegedly lost a computer disk drive in May 2009 containing protected health and other private information on more than 500,000 Connecticut citizens and 1.5 million consumers nationwide. The missing disk drive contained names, addresses, social security numbers, protected health information and financial information. Blumenthal learned that the company delayed notifying consumers and law enforcement authorities, and that an investigation by a Health Net consultant concluded the disk drive was likely stolen.
- Under this settlement, Health Net and its affiliates have agreed to:
  - A "Corrective Action Plan" in which Health Net is implementing several detailed measures to protect health information and other private data in compliance with HIPAA. This plan includes continued identity theft protection, improved systems controls, improved management and oversight structures, improved training and awareness for its employees, and improved incentives, monitoring, and reports.
  - A $250,000 payment to the state representing statutory damages. This payment is intended as a future deterrent to such conduct not only by Health Net, but by other insurers and health care entities that are entrusted with individuals' private information.
  - An additional contingent payment to the state of $500,000, should it be established that the lost disk drive was accessed and personal information used illegally, impacting plan members.

Federal HIPAA Settlements and Penalties

- Resolution Agreement with Providence Health & Services--July 16, 2008
  - $100,000
- Resolution Agreement with CVS Pharmacy, Inc.--January 16, 2009
  - $2.25 million
- Resolution Agreement with Rite Aid Corporation--July 27, 2010
  - $1 million
- Resolution Agreement with Management Services Organization Washington, Inc.--December 13, 2010
  - $35,000
- Civil Money Penalty issued to Cignet Health of Prince George's County, MD--February 4, 2011
  - $4.3 million
- Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc.--February 14, 2011
  - $1 million

Cignet and MGH

- The Cignet settlement reflects a unique set of circumstances:
  - OCR found that Cignet violated 41 patients' rights by denying them access to their medical records when requested between September 2008 and October 2009.
  - The patients individually filed complaints with OCR, initiating investigations of each complaint.
  - The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The CMP for these violations was $1.3 million.
  - During the investigations, Cignet refused to respond to OCR's demands to produce the records. Additionally, Cignet failed to cooperate with OCR's investigations of the complaints and produce the records in response to OCR's subpoena. Covered entities are required under law to cooperate with the Department's investigations. The CMP for these violations was $3 million.
- The MGH incident involved the PHI of 192 patients from MGH's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR said that its investigation indicated that MGH failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule.
  - OCR press release: "We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information."

FOLEY HOAG LLP
Driving Business Advantage

Security: Why Should It Be a Priority?

- **More federal and state laws, increased penalties**
- **Theft of consumer information increasing:**
  - **TJX/Heartland**
    - Attorney General settlement
    - Private consumer litigation
    - Harm to brand
- **Attacks on systems increasing:**
  - **North Korean attack in 2009**
    - Treasury Department and Federal Trade Commission Web sites were shut down by the software attack, which lasted for days over the holiday weekend, others such as the Pentagon and the White House were able to fend it off with little disruption.
  - **NYSE has suffered several recent incursions**
  - **Stuxnet Worm in Iran's nuclear program**
- **Wikileaks**

Massachusetts Data Security Law

- Most recent law in the Massachusetts in the area of data privacy and security – Mass. Gen. L. ch. 93H.
- Enacted after the TJX data breach was made public.
- Intended to protect Massachusetts residents from identity theft.
- Applies to any business entity that owns, licenses, maintains or stores the **"personal information"** of a Massachusetts resident.
- Regulations – 201 CMR 17.00 – most took effect on March 1, 2010, govern measures businesses must take to comply with new data security law.

What is “Personal Information”?

“Personal Information” is:

- A person’s first name and last name (or first initial and last name) **PLUS** any **one** of the following:
  - Social Security number
  - Driver’s license number (or other state issued ID card number)
  - A financial account number, or credit or debit card number, with or without any required security code, access code or PIN that would allow account access

Key Requirements in the Massachusetts Regulations

- Designate an individual who will be responsible for your information security program.
- Develop a written information security policy.
- Identify what personal information your business possesses, where it is kept and who has access to it.
- Place reasonable restrictions on access to personal information: physical restrictions for hard copy files; log-in and password protection for electronic files.
- Take steps to ensure that third party service providers have the capacity to protect personal information.
- Prevent terminated employees from accessing personal information.
- Regular monitoring and updating of security measures.
- Document responsive actions taken in connection with any incident involving a breach of security.

HIPAA Security Regulations

- Physical safeguards
- Administrative safeguards
- Technical safeguards

Questions to ask about Administrative Safeguards: Security Management

- Where are the risks and vulnerabilities to our ePHI?
- What can we do to manage those risks?
- How will we sanction those who do not follow our policies that protect ePHI?
- How do we review our security records (e.g., logs, video, incident reports, etc.)
- Who is our security point person?

Questions to ask about Administrative Safeguards: Workforce Security

- These are “addressable” and therefore can be adopted with flexibility to meet our unique needs:
  - What are our procedures for authorizing and supervising those with access to ePHI?
  - How do we approve people to access ePHI?
  - How do we terminate access to ePHI?

Questions to ask about Administrative Safeguards: Information Access Management

- How to we keep our health plan information away from other, unrelated functions?
- What are our protocols for accessing health plan information at the computer terminal and program level?
- How do we modify that access?

Questions to ask about Administrative Safeguards: Workforce Security

- These are “addressable” and therefore can be adopted with flexibility to meet your unique needs:
  - What are our procedures for authorizing and supervising those with access to ePHI?
  - How do we approve people to access ePHI?
  - How do we terminate access to ePHI?

Questions to ask about Administrative Safeguards: Information Access Management

- How to we keep our health plan information away from other, unrelated functions?
- What are our protocols for accessing health plan information at the computer terminal and program level?
- How do we modify that access?

FOLEY HOAG LLP
Driving Business Advantage

Questions to ask about Administrative Safeguards: Security Awareness and Training

- This is a very straightforward set of requirements:
  - What are our security reminders to personnel?
  - What do we have to protect our data against viruses, spyware, etc.?
  - How to we oversee who signs into the health plan computer systems?
  - How do we control and change computer passwords for systems with access to ePHI?

FOLEY HOAG LLP
Driving Business Advantage

More Administrative Safeguards

- Security incident policies and procedures
- Contingency plans (data backup, disaster recovery, emergency operation, testing and revision, criticality analysis for applications and data)
- Periodic evaluation of security policies and procedures
- Review business associate agreements

FOLEY HOAG LLP
Driving Business Advantage

Overview of Issues Regarding Physical Safeguards

- Facility access controls (contingency plans, facility security plans, access control and validation, maintenance records)
- Workstation use policies and procedures
- Building, room, record, and workstation security to restrict access to authorized users
- Control on receipt and removal of hardware and media (disposal, use and reuse, inventory, backup and storage)

FOLEY HOAG LLP
Driving Business Advantage

Questions to ask about Physical Safeguards: Facility Access

- What are your policies and procedures regarding allowing authorized and limiting unauthorized access to ePHI and the areas it is housed?
- How do these policies and procedures identify those who are authorized to have access (e.g., by title, job function, name, etc.)?
- What are the physical access controls (e.g., locks, alarms, monitoring)?

Questions to ask about Physical Safeguards: Contingency Operations

- What are the procedures in the event of a loss of power or other emergency?
- Do people with responsibility for the ePHI know about these procedures and how to implement them?

FOLEY HOAG LLP
Driving Business Advantage

Questions to ask about Physical Safeguards: Workstations, Device and Media Controls

- How do we specify what happens at workstations linked to ePHI?
- How do we dispose/reuse old computers and data sources (e.g., disks) that may have ePHI?
- Do people with responsibility for the ePHI know about these procedures and how to implement them?

FOLEY HOAG LLP
Driving Business Advantage

Physical Safeguards: Facility Security/Access Control

- Where is ePHI kept and who has access to those places/systems?
  - These questions have to be asked and answered.
- Access control is a continuing process, as employees come and go regularly.

FOLEY HOAG LLP
Driving Business Advantage

Technical Safeguards

- Access control (unique IDs, emergency access procedure, auto logoff, encryption)
- Audit controls
- Data integrity policies (authentication mechanisms)
- Person or entity authentication
- Transmission security (integrity and encryption)

Documentation Requirements

- Regulations require policies and procedures be documented (written record of any required actions).
- Retain documentation for 6 years.
- Make documentation available to those implementing procedures.
- Update documentation as necessary.

RESOURSES

- OCR: http://www.hhs.gov/ocr/privacy
- Cignet OCR materials: http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html
- MGH Resolution Agreement: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralra.pdf
- AHIMA: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_023082.html
- My blog: http://www.securityprivacyandthelaw.com