

Emerging Privacy and Security Audit Standards for HIPAA/HITECH Compliance

A Presentation to
ISACA, Central Ohio Chapter
April 14, 2011

That was then...

“Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets.”

— *Oath of Hippocrates, 4th Century, B.C.E.*

This is now...

“Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds.”

John Perry Barlow

Key Definitions

Privacy: The right of individuals to control what information is collected about them, to know the purpose for its use, to learn who has access to it and how it is maintained.

Key Definitions

Confidentiality: The assurance that information about an individual that the individual perceives to be private, will not be disclosed without consent, except as allowed by law.

Fair Information Practices

Openness [Notice]

- * Existence and purpose of record-keeping systems must be publicly known.

Individual Participation [Access]

- * Individual right to see records and assure quality of information.
 - Accurate, complete, and timely.

Security

- * Reasonable safeguards for confidentiality, integrity, and availability of information.

Accountability [Enforcement]

- * Violations result in reasonable penalties and mitigation.

Limits on Collection, Use, and Disclosure [Choice]

- * Collected only with knowledge and permission of subject.
- * Used only in ways relevant to the purpose for which the data was collected.
- * Disclosed only with permission or overriding legal authority.

HIPAA

The **H**ealth **I**nsurance **P**ortability
and **A**ccountability **A**ct of 1996

One “P”

Two “A’s”

HIPPO

(from the ancient Greek for “river horse”)

Two “P’s”

One “O”



HIPAA

Passed by Congress in 1996, **HIPAA**:

Protects health insurance coverage for workers and their families when they change or lose their jobs;

Requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers;

Addresses the security and privacy of **some** health data.

HIPAA

Created to **protect individual privacy**, therefore, it limits the use and disclosure of records or other patient related information.

The prohibition on unauthorized disclosure applies whether or not the person seeking the information already has the information, has other means of obtaining it, has official status, has obtained a warrant or subpoena, or is authorized by state law.

HIPAA is a floor...

Congress: No one should get “less” privacy because of HIPAA.

- * State or federal laws that provide more privacy to individuals than HIPAA **remain in effect.**
- * This is the challenge for creating audit standards for HIPAA privacy compliance.
- * Security audit standards are easier because there are very few state or federal laws that afford individuals more security for their electronic health information.

Ohio Privacy Law: The Basics

Laws impacting the privacy of health information in Ohio come from several sources:

- Federal and State Court Opinions
- Ohio Revised Code
- Ohio Administrative Code
- Rules of Evidence
- Rules of Court

Ohio Privacy Law: The Basics

- Professional ethics standards codified as licensure or certification standards in the Ohio Revised and Administrative Codes (pharmacists, physicians, nurses, psychologists, etc.).

Ohio Privacy Law: The Basics

1956: Justice Brandeis: the right of privacy is “the right to be left alone.”

Ohio: recognizes the tort of “invasion of privacy.”

Ohio also recognizes an independent tort of “inducement” to violate privacy.

See Biddle v. Warren General Hospital (1999) 86 Ohio St. 3d 395.

Biddle v. Warren General Hospital

“We hold that in Ohio, an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship.”

Key concepts of HIPAA Privacy and Security

Provides a national uniform health information privacy and security **baseline**.

Does **not** regulate **all** health **information**.

Is **pre-empted by other laws** that give individuals greater privacy.

Privacy compliance requires a thorough knowledge of other state and federal privacy laws.

Who must comply with HIPAA?

Health Care Clearinghouses

Health Plans

Health Care Providers

HIPAA Term: **Covered Entity (CE)**

Who else is effected by HIPAA?

Any person or entity that performs a function, activity or service on behalf of a **Covered Entity** that **requires** the use of, or access to, **PHI**.

HIPAA Term: Business Associate (BA)



What does HIPAA protect?

Information, maintained or transmitted in **any format**, that:

is created or received by a health care provider, health plan, employer, or health care clearinghouse; that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; **AND**

What does HIPAA protect?

That identifies the individual; or

With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

HIPAA Term: **P**rotected **H**ealth **I**nformation
(PHI)

How does HIPAA protect PHI?



How does HIPAA protect PHI?

PHI?

Depends on why...

Focus is on the **purpose** for the disclosure

HIPAA: Disclosing PHI

TPO

EVERY OTHER
REASON *

* Permission required unless
exception applies

HIPAA: Disclosing PHI

Exceptions are **permissive**, not mandatory;

Exceptions must be specifically required under other state and federal laws;

Approximately twenty exceptions exist;

Disclosure is permitted under carefully circumscribed conditions;

Minimum necessary **always** applies.

Ohio Confidentiality Laws

**Confidential
Health
Information**



Can Always Be Released
With Permission of the
Individual

Ohio Confidentiality Laws

Confidential Health Information

May be released without permission

Situational:

- Who has the records?
- Who wants the records?

HIPAA



HITECH

The **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth Act

Title XIII of the American Recovery and Reinvestment Act of 2009
(ARRA), P.L. 111-5, (2/17/09):

Creates the Office of the National Coordinator for
Health Information Technology (ONCHIT);



HITECH

Creates grants (**‘free’ hardware!**) and incentives (**meaningful use**) to promote the adoption of electronic health records.

Changes certain aspects of the HIPAA Privacy, Security and Enforcement Rules (**big fines**).

Authorizes Breach Notification to be implemented and enforced through HHS and the Federal Trade Commission (FTC) (**bad publicity**).

What's in Effect Now?

Enforcement Rule (new and improved):

Plans and Providers effective April, 2003 (2004 for small plans)

BA's must comply effective February, 2010 (via HITECH at 42 USC §17931)

Key Changes in Enforcement

Applies to BA's as a matter of law, not contract.

Expands enforcement to each states' Attorney General.

- Limited to \$100/\$25,000 per violation

Government attorneys fees and costs may be awarded.

Harmed Individuals can get a percentage of penalties (**whistleblowers!**).


Key Changes in Enforcement

Civil Monetary Penalties (CMP):


No knowledge: \$100 (\$25,000)

Reasonable cause: \$1,000 (\$100,000)

Willful neglect/corrected: \$10,000 (\$250,000)

 Willful neglect/not corrected: \$50,000
(\$1,500,000)

Criminal penalties

 Providers and Plans (corporate and individual liability)

Business Associates

Non-employees

What's in Effect Now?

Security Rule:

Providers and Plans effective April, 2005
(2006 for small plans)

BA's must comply effective February,
2010 (via HITECH at 42 USC §17931)

Key Concepts in Security

Objective Standards for:

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

protecting against any reasonably anticipated threats or hazards to the security or integrity of such information;

Key Concepts in Security

Objective Standards for:

protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and

ensuring compliance with its security measures by its workforce.

What's in Effect Now?

Privacy Rule:

NPRM published July, 2010

Comment Period closed 9/13/10

NO FINAL RULE

BA's must comply effective February, 2010 (via HITECH at 42 USC §17931)

Key Changes in Privacy

1. Marketing:
2. Sale of PHI:
3. Minimum Necessary:
4. Fundraising:

Key Changes in Privacy

5. Right to Request Restrictions:
6. Right to Access:
7. BA contracting:

HITECH and Business Associates



Business Associate Concepts

Before HITECH:

- BA's were not bound by the HIPAA Privacy and Security Rules (and were not subject to civil monetary penalties); but
- Before allowing a BA to access, receive or use PHI, a CE was required to enter into a business associate agreement (BAA) with the BA whereby the BA made specific promises regarding the protection of PHI.

After HITECH:

- Effective February 18, 2010, BA's are legally bound by certain provisions of the Privacy and Security Rules (and subject to civil monetary penalties for failures with respect to violations); and
- A CE still must have a BAA with its BA's.

Business Associate Concepts

HITECH made BA's subject to the Privacy and Security Rules (HITECH §§13401 and 13404) effective as of February 18, 2010, but the scope of the application was not clear.

Proposed rule:

- * BA's will be subject to all of the Security Rule; and
- * BA's will be subject to all of the Privacy Rule except requirements related to the provision of Notices of Privacy Practices and the administration of individual rights.

Business Associate Concepts

Subcontractors

Current: A BAA must include the BA's agreement that it will obtain from its subcontractors agreement "to the same restrictions and conditions" that apply to the BA with respect to PHI.

Proposed:

- The definition of BA will be changed to include a "subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate."
- A BA (but not the CE) will be required to enter into BAA's with subcontractors that create or receive PHI for the BA.
- A BAA between a BA and its subcontractor will need to include the same elements as a BAA between the CE and the BA.

What's in Effect Now?

Breach Notification Rule:

Interim Final Rule published 8/23/09

Applicable to breaches occurring on
or after 9/23/09

Proposed Final Breach Notification
Rule withdrawn 7/28/10

Breach Notification Concepts

Before HITECH: A covered entity must mitigate to the extent practicable, any harmful effect from an improper use or disclosure of PHI.

After HITECH: Mitigation still required (same as old), *plus a* covered entity must notify individuals without unreasonable delay (and not later than 60 days) after the **discovery** of a breach of “**unsecured**” PHI.

Breach Notification Concepts

Breach: the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA privacy regulations which compromises the security or privacy of the PHI (**harm threshold exception**).

Discovered: the first day on which such breach is known to the CE or BA or **should reasonably have been known** to the CE or BA to have occurred.

Breach Notification Concepts

Breach notification **required** if “unsecured” PHI was breached.

Two acceptable ways to “secure” PHI:

- **Encryption** (to a standard that is revised on an annual basis); or
- **Destruction** (in accordance with a federally defined standard).

Breach Notification Concepts

Role of the BA

If the breach involved unsecured PHI maintained by the BA, the BA must (**promptly**) notify the CE of the breach and (**promptly**) identify all affected individuals.

Why Audit?

HIPAA requires Covered Entities (and HITECH extends this requirement to Business Associates) to create records sufficient to demonstrate compliance with the Privacy, Security and Breach provisions of HIPAA.

HIPAA Privacy Compliance

Develop and implement administrative, technical, and physical safeguards to **reasonably** safeguard the privacy of PHI.

This applies to PHI maintained in any format.

HIPAA Privacy Compliance

1. Assess
2. Develop Privacy Plan
3. Implement the Plan
4. Document Decisions
5. Re-assess and Modify Plan

HIPAA Privacy Compliance

45 C.F.R. Parts 160 and 164

Each rule contains a standard.

Each rule contains implementation specifications.

HIPAA Privacy Compliance

1. Uses and Disclosures of PHI
2. Individual Rights
3. Administrative Requirements
4. Business Associates

Emerging Privacy and Security Audit Standards for HIPAA/HITECH Compliance

**A Presentation by
Melissa J. Mitchell, Esq.
mjm@sentientlaw.com**