Grant Thornton
An instinct for growth™

Foundations of HIPAA Compliance

Providing clarity on complex security and privacy regulations

Thursday, August 20, 2015

San Francisco ISACA August Educational Event

JOHANNA TERRONEZ, BAS SR. MANAGER

Today's Presenter

Johanna Terronez
Grant Thornton
Senior Manager, Business Advisory Services
San Francisco, CA
T: 415.318.2228
E: Johanna.Terronez@us.gt.com

AGENDA

About HIPAA

HIPAA Rules

- Privacy
- Security
- Breach Notification

Current Regulatory Environment

Delivery of HIPAA Service Offerings

Learning objectives

- Define current HIPAA security, privacy and breach notification regulatory requirements
- Mechanisms to address HIPAA requests from clients and regulators

What is HIPAA?

The "Health Insurance Portability and Accountability Act"

Abbreviated HIPAA, not HIPPA

A federal law originally passed in 1996

Two components:

- **Title I :** Protects health insurance coverage for workers and their families when they change or lose their jobs - COBRA

- **Title II :** Known as the Administrative Simplification (AS) provisions

Title II: Administrative Simplification provisions

Required the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers

This section of the HIPAA was **aimed at improving the efficiency and effectiveness of the health care system**

The key components:

- Standardized electronic transmission of common administrative and financial transactions (such as billing and payments)
- Unique health identifiers for individuals, employers, health plans, and heath care providers
- Privacy and security standards to protect the confidentiality and integrity of individually identifiable health information that was being transmitted over the Internet

The 4 main Administrative Simplification rules

- **Privacy Rule**
  Establishes standards to protect individuals' medical records and other personal health information.

- **Security Rule**
  Establishes standards to protect individuals' electronic personal health information.

- **Enforcement Rule**
  Contains provisions relating to compliance and investigations, the imposition of civil and criminal penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

- **Breach Notification Rule**
  Requires notification following a breach of unsecured protected health information.

What is the purpose of HIPAA?

- Provide health care coverage for all people, regardless of preexisting health conditions or layoff
- Protect medical records and other protected health information (PHI) and give patients new rights regarding the management of their PHI
- Establish precise and uniform standards for electronic transfer and storage of electronic PHI ("ePHI")
- Reduce the cost and improve the process of filing insurance claims and coordination of care

Before we move on, some definitions

Covered Entity ("CE")

(1) A health plan (2) A health care clearinghouse (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA

Business Associate ("BA")

Generally, a person or organization who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of PHI

Sub-Business Associate ("Sub-BA")

Generally, a person or organization who performs functions or activities on behalf of, or certain services for, a BA that involve the use or disclosure of PHI

Activities commonly performed by BA's for CE's

Claims processing or administration	Utilization review	Quality assurance
Billing	Benefit management	Practice management
Repricing	Legal	Actuarial
Management	Administrative	Accreditation
Accounting	Consulting	Data aggregation
Financial services	**Any other function or activity covered by the Rule**	

Definition of "Protected Health Information"

Individually identifiable health information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition
- the provision of health care to the individual
- the past, present, or future payment for the provision of health care to the individual

- Individually identifiable means that it identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual

- PHI in electronic form is referred to as "ePHI:

PHI identifiers (per HIPAA)

Names	Full Face Photos	Biometric Info
Health Plan Beneficiary #'s	Any geographical subdivisions smaller than a state (e.g., street, city)	Dates related to the individual (e.g., DOB)
Phone #'s	Fax #'s	Email Addresses
SSN's	Medical Record #'s	IP Addresses
Vehicle Identifiers	License #'s	Account #'s
Device Identifiers	Web URL's	**… or any other unique identifying number, characteristic, or code**

Who is covered by HIPAA?

- Almost every organization that **provides or pays for health services**, or exchanges health data of any kind, is covered by HIPAA
- Health care **providers** (physicians, nurses, allied health practitioners); health care **facilities** (hospitals, clinics); **health plans** (HMOs, insurers); and health information **clearinghouses** are what HIPAA calls "**covered entities**"
- HIPAA extends rights to every patient whose healthcare information is collected, used, or disclosed by such covered entities
- It imposes duties on covered entities -- and, by extension, on all persons who work in or for covered entities -- in order to protect those rights
- HIPAA reaches even to the business associates of health institutions; companies that handle health data on a covered entity's behalf

HIPAA is not new, but it was recently updated

- **1996:** HIPAA signed into law
- **2000:** Privacy rule published
- **2001:** Compliance with privacy rule required for covered entities
- **2003:** Security rule published
- **2005:** Compliance with security rule required for CE's
- **2006:** Enforcement rule published in final form
- **2007:** First security rule audit performed by regulators (Piedmont Hospital)
- **Feb. 2009:** HITECH act signed into law
- **June 2009:** OCR becomes responsible for enforcing security rule
- **Feb. 2009:** HITECH compliance required for CE's
- **2011:** OCR begins pilot audits
- **Jan. 2013:** Omnibus rule published
- **Sept. 2013:** Omnibus rule compliance required

The 2014 Omnibus Rule: Changes

Modifies the HIPAA privacy, security, and enforcement regulations in the following ways:

a. Makes BA's and subcontractors of BA's directly liable for compliance with certain of the HIPAA Privacy and Security Rule requirements

b. Strengthens the limitations on the use and disclosure of PHI for marketing and fundraising purposes, and prohibits the sale of PHI without individual authorization

c. Expands an individual's rights to receive electronic copies of his or her health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out-of-pocket in full

d. Requires modifications to a covered entity's Notice of Privacy Practices

e. Adopts additional enhancements to the Enforcement Rule, particularly regarding privacy breaches and penalties

AGENDA

About HIPAA

HIPAA Rules

- Privacy
- Security
- Breach

Current Regulatory Environment

Addressing HIPAA

Composition of the Privacy Rule

PART 164—SECURITY AND PRIVACY

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.501 Definitions.
§ 164.502 Uses and disclosures of protected health information: general rules.
§ 164.504 Uses and disclosures: Organizational requirements.
§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
§ 164.508 Uses and disclosures for which an authorization is required.
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.
§ 164.514 Other requirements relating to uses and disclosures of protected health information.
§ 164.520 Notice of privacy practices for protected health information.
§ 164.528 **Accounting of disclosures** of protected health information.
§ 164.522—Rights to Request Privacy Protection for Protected Health Information
§ 164.524—Access of Individuals to Protected Health Information
§ 164.526—Amendment of Protected Health Information
§ 164.528—Accounting for Disclosures of Protected Health Information
§ 164.530—Administrative Requirements

Privacy Rule key concepts

- Administrative safeguards
- Patient rights
- Uses and disclosures of PHI
- The "Minimum Necessary" standard

Administrative Safeguards of the Privacy Rule

- Personnel Designations—Privacy Officer
- Training
- Complaints to the Covered Entity
- Sanctions for non-compliance
- Mitigation
- Refraining From Intimidating or Retaliatory Acts
- Waiver of Rights
- Policies and Procedures
- Changes to Policies or Procedures
- Change in Law
- Documentation Requirements
- Group Health Plans Requirements

Summary of patient rights afforded by the HIPAA Privacy Rule

- The right to request restrictions on certain uses and disclosures of PHI
- The right to receive confidential communications of PHI
- The right to inspect and copy PHI
- The right to amend PHI
- The right to receive an accounting of disclosures of PHI
- The right of the individual, including an individual who has agreed to receive the notice electronically…to obtain a paper copy of the Notice from the covered entity upon request
- The right to complain to the covered entity and to the Secretary if they believe their privacy rights have been violated

Patient rights afforded by the HIPAA Privacy Rule *(continued)*

Notice of Privacy Practices for Protected Health Information:
- Right of an Individual to Request Restriction of Uses and Disclosures of PHI
- Confidential Communication Requirements

Access of Individuals to Protected Health Information
- Right of Access

Amendment of Protected Health Information
- Right to Amend

Accounting of Disclosures of Protected Health Information
- Right to an Accounting of Disclosures of PHI

Patient rights afforded by the HIPAA Privacy Rule *(continued)*

Rights to Request Privacy Protection for Protected Health Information:

- Right of an Individual to Request Restriction of Uses and Disclosures of PHI
  - The individual has the right to request that the covered entity restrict how PHI is used or disclosed to carry out treatment, payment, or healthcare operations;
    - The covered entity is not required to agree to requested restrictions; and
    - If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity.
- Confidential Communication Requirements
  - A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the covered health care provider by alternative means or at alternative locations."

The Minimum Necessary standard

- When using or disclosing PHI or when requesting PHI from another CE, a CE must make reasonable efforts to limit PHI to the **minimum necessary** to accomplish the intended purpose of the use, disclosure, or request.

- Minimum Necessary does not apply to:

  - Disclosures made to or a request by a healthcare provider for treatment purposes

  - Uses or disclosures made to or by the individual

  - Disclosures made in response to a request from the Secretary to investigate or determine the covered entity's compliance

  - Uses or disclosures that are required by law

The Minimum Necessary standard *(continued)*

- Covered entities also must implement reasonable minimum necessary **policies and procedures** that limit how much protected health information is used, disclosed, and requested for certain purposes.

- These policies and procedures also reasonably must limit **who** within the entity has access to protected health information, **and under what conditions**, based on job responsibilities and the nature of the business

Uses and Disclosures of De-Identified Protected Health Information

Standard: Uses and Disclosures to Create De-Identified Information

» The Rule states “a covered entity may use PHI to create information that is not individually identifiable health information or disclose PHI only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.”

» Health information that meets the standard and implementation specifications for de-identification is considered not to be individually identifiable health information.

Elements of PHI that must be scrubbed to create de-identified data

Names of the individual, and relatives, employers or household members of the individual	Geographic identifiers of the individual, et. al. including: Subdivisions smaller than a state Street addresses City County Precinct	Zip code—at any level less than the initial three digits. However, if the initial digits cover a geographical area of 20,000 or less people, then it has to be reported as 000	All elements of dates (except year) or dates directly related to an individual: • Birth date, • Admission date • Discharge date • Date of death, and • All ages over 89 and all elements of dates (including year) indicative of such age
Telephone numbers	Fax numbers	Electronic mail addresses	Social security numbers
Medical record numbers	Health plan beneficiary numbers	Account numbers	Certificate/license numbers
Vehicle identifiers and serials numbers, including license plate numbers	Device identifiers and serial numbers	Internet Protocol (IP) address numbers	Biometric identifiers, including finger and voice prints
Full-face photographic images and any comparable images	Web Universal Resource Locators (URLs)	**… or any other unique identifying number, characteristic, or code**	

A "limited data set" (LDS)

- A LDS may contain dates and certain geographic information associated with an individual that are absent from de-identified information

- A LDS may contain, for example:

DOB	City	State	Zip	Service Dates

- A covered entity may use or disclose a LDS **only** for the purposes of research, public health, or health care operations

Consent and Treatment, Payment and Operations (TPO)

- "A covered health care provider must obtain the individual's consent, in accordance with this [Rule], prior to using or disclosing PHI to carry out treatment, payment, or health care operations," with these exceptions:
  - A covered healthcare provider may, without consent, use or disclose PHI to carry out treatment, payment, or healthcare operations, if:
    - It has an indirect treatment relationship (§164.501) with the individual; or
    - It created or received the PHI in the course of providing healthcare to an individual who is an inmate
    - In emergency treatment situations, if the CE attempts to obtain the consent ASAP after the delivery of such treatment;
    - If the covered healthcare provider is required by law to treat the individual, and the covered healthcare provider attempts to obtain such consent, but is unable to obtain such consent; or
    - If a covered healthcare provider attempts to obtain such consent from the individual, but is unable to obtain such consent due to substantial barriers to communication with the individual

Uses and Disclosures of PHI

Uses and Disclosures for Which an Authorization Is Required:

- a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes except to carry out TPO
- The Rule spells out specifics for what constitutes a valid authorization

Other Use and Disclosure aspects:

- Individuals have the opportunity to agree to or prohibit or restrict the disclosure
- Use and Disclosure for Facility Directories
- Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes
- Use and Disclosure for Disaster Relief Purposes

Uses and Disclosures of PHI (continued)

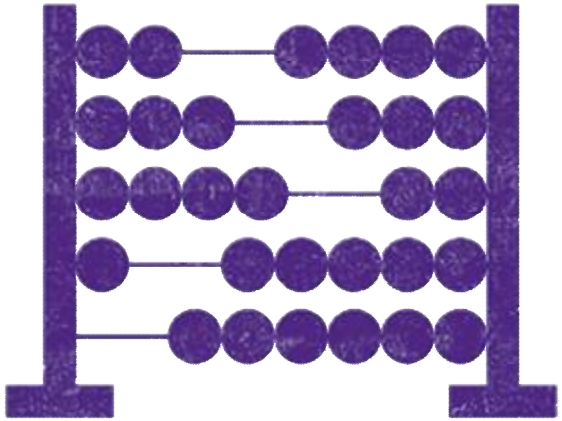
Use and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required:

- Uses and Disclosure Required by Law
- Uses and Disclosure for Public Health Activities
- Disclosure About Victims of Abuse, Neglect or Domestic Violence
- Uses and Disclosures for Health Oversight Activities
- Disclosures for Judicial and Administrative Proceedings
- Disclosure for Law Enforcement Purposes
- Uses and Disclosures About Decedents
- Uses and Disclosures for Research Purposes
- Uses and Disclosures to Avert a Serious Threat to Health or Safety
- Uses and Disclosure for Specialized Government Functions
- Correctional Institutions and Other Law Enforcement Custodial Situations
- Disclosure for Workers' Compensation
- Presidential Executive Order: To Protect the Privacy of Protected Health Information in
- Oversight Investigations

Uses and Disclosures of PHI (continued)

Other Requirements Relating to Uses and Disclosures of Protected Health Information:

- Uses and Disclosures of PHI for Marketing
- Uses and Disclosures for Fundraising
- Uses and Disclosures for Underwriting and Related Purposes
- Verification Requirement



AGENDA

About HIPAA

HIPAA Rules

- Privacy
- Security
- Breach Notification

Current Regulatory Environment

Addressing HIPAA

Purpose of the HIPAA Security Rule

- §164.530(c)(1) of the Privacy Rule requires that:

  A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information

- The Security Rule complements the Privacy Rule by providing guidance for the interpretation of these three safeguards

- The Security Rule applies only to ePHI; unlike the Privacy Rule, it does not cover paper documents or oral information

Purpose of the HIPAA Security Rule *(continued)*

Generally, the Security Rule requires a covered entity to:

- Ensure the **confidentiality, integrity,** and **availability** of all ePHI the covered entity creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule
- Ensure compliance by its workforce

Composition of the HIPAA Security Rule

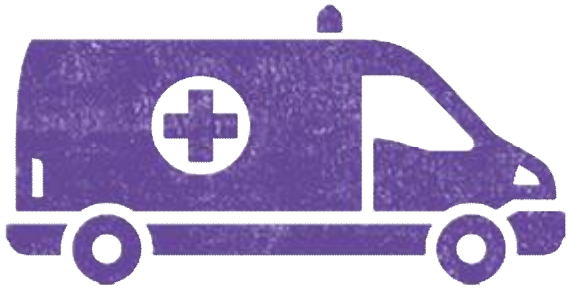
PART 164—SECURITY AND PRIVACY

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 Applicability
§ 164.304 Definitions
§ 164.306 Security standards: General rules
§ 164.308 Administrative safeguards
§ 164.310 Physical safeguards
§ 164.312 Technical safeguards
§ 164.314 Organizational requirements
§ 164.316 Policies and procedures and documentation requirements
§ 164.318 Compliance dates for the initial implementation of the security standards

Composition of the HIPAA Security Rule *(cont'd)*

- The Security Rule sections (known as safeguards) contain:
  - **Standards,** which are all required
  - **Implementation Specifications**, which can either be "required" or "addressable"



The Security Rule's **Administrative Safeguards (164.308)**

> *"**Administrative actions, and policies and procedures**, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."*

- The Administrative Safeguards comprise over half of the HIPAA Security requirements.
- Requires a thorough risk analysis, an evaluation of the security controls already in place, and a series of documented solutions derived from a number of factors unique to each covered entity.

The Security Rule's
Administrative Safeguards (164.308) *(Continued)*

Implementation Specification or Standard		
No.	Title	R / A
(a)(1)(ii)(A)	Risk Analysis	(R) Required
(a)(1)(ii)(B)	Risk Management	(R) Required
(a)(1)(ii)(C)	Sanction Policy	(R) Required
(a)(1)(ii)(D)	Information System Activity Review	(R) Required
(a)(2)	Assigned Security Responsibility	(R) Required
(a)(3)(ii)(A)	Authorize and/or Supervision	(A) Addressable
(a)(3)(ii)(B)	Workforce Clearance Procedure	(A) Addressable
(a)(3)(ii)(C)	Termination Procedures	(A) Addressable
(a)(4)(ii)(A)	Isolate Healthcare Clearinghouse Functions	(R) Required
(a)(4)(ii)(B)	Access Authorization	(A) Addressable
(a)(4)(ii)(C)	Access Establishment and Modification	(A) Addressable
(a)(5)(i)	Security awareness and training	(R) Required
(a)(5)(ii)(A)	Security Reminders	(A) Addressable
(a)(5)(ii)(B)	Protection from Malicious Software	(A) Addressable

The Security Rule's
Administrative Safeguards (164.308) *(Continued)*

Implementation Specification or Standard		
No.	Title	R / A
(a)(5)(ii)(C)	Login Monitoring	(A) Addressable
(a)(5)(ii)(D)	Password Management	(A) Addressable
(a)(6)(i)	Security Incident Procedures	(R) Required
(a)(6)(ii)	Security Incident Response	(R) Required
(a)(7)(ii)(A)	Data Backup Plan	(R) Required
(a)(7)(ii)(B)	Disaster Recovery Plan	(R) Required
(a)(7)(ii)(C)	Emergency Mode Operation Plan	(R) Required
(a)(7)(ii)(D)	Testing and Revision Procedure	(A) Addressable
(a)(7)(ii)(E)	Applications and Data Criticality Analysis	(A) Addressable
(a)(8)	Evaluation	(R) Required
(b)(1)	Written Contract or Other Arrangement	(R) Required

The Security Rule's **Administrative Safeguards (164.308)** *(Continued)*

Some examples:

164.308(a)(3)(ii)(a) Authorize and/or Supervision: Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.

164.308(a)(4)(2)(c) Access Establishment and Modification: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

164.308(a)(5)(i) Security and Awareness Training: Implement a security awareness and training program for all members of its workforce (including management).

The Security Rule's **Physical Safeguards (164.310)**

> *"Physical measures, policies, and procedures to protect a covered entity's electronic information systems and* ***related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion****."*

- Primarily applies to all locations in which ePHI is accessed, maintained, stored, or transmitted during the normal course of business

- When evaluating and implementing these standards, a covered entity must consider all physical access to ePHI. This may extend outside of an actual office, and could include workforce members' homes or other physical locations where they access ePHI.

The Security Rule's
Physical Safeguards (164.310) *(continued)*

Implementation Specification or Standard		
No.	Title	R / A
(a)(2)(i)	Contingency Operations	(A) Addressable
(a)(2)(ii)	Facility Security Plan	(A) Addressable
(a)(2)(iii)	Access Control and Validation Procedures	(A) Addressable
(a)(2)(iv)	Maintenance Records	(A) Addressable
(b)	Workstation Use	(R) Required
(c)	Workstation Security	(R) Required
(d)(1)	Device and Media Controls	(R) Required
(d)(2)(i)	Disposal	(R) Required
(d)(2)(ii)	Media Re-use	(R) Required
(d)(2)(iii)	Accountability	(A) Addressable
(d)(2)(iv)	Data Backup and Storage	(A) Addressable

The Security Rule's **Physical Safeguards (164.310)** *(continued)*

Some examples:

164.310(a)(2)(iii) Access Control and Validation: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision

164.310(d)(1) Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

The Security Rule's **Technical Safeguards (164.312)**

*"The **technology and the policy and procedures** for its use that protect electronic protected health information and control access to it."*

- Based on the fundamental concepts of flexibility, scalability and technology neutrality. So, no specific requirements for types of technology to implement are identified.
- Allows a covered entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications.
- A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.

The Security Rule's
Technical Safeguards (164.312) *(continued)*

Implementation Specification or Standard		
No.	Title	R / A
(a)(2)(i)	Unique User Identification	(R) Required
(a)(2)(ii)	Emergency Access Procedure	(R) Required
(a)(2)(iii)	Automatic Logoff	(A) Addressable
(a)(2)(iv)	Encryption and Decryption	(A) Addressable
(b)	Audit Controls	(R) Required
(c)(1)	Integrity	(A) Addressable
(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	(A) Addressable
(d)	Person or Entity Authentication	(R) Required
(e)(2)(i)	Integrity Controls	(A) Addressable
(e)(2)(ii)	Encryption (of Transmitted Data)	(A) Addressable

The Security Rule's **Technical Safeguards (164.312)** *(continued)*

Some examples:

164.312(a)(2)(iii) Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

164.312(e)(2)(ii) Encryption: Implement a mechanism to encrypt ePHI whenever deemed appropriate.

164.312(a)(2)(i) Unique User ID: Implement procedures to assign a unique name and/or number for identifying and tracking user identity

The Security Rule's **Organizational Safeguards (164.314)**

- Requires a covered entity to have **contracts or other arrangements with business associates** that will have access to the covered entity's electronic protected health information (ePHI)

- Also ***provides the specific criteria required for written contracts*** or other arrangements between a covered entity and its business associates

Implementation Specification or Standard		
No.	Title	R / A
(a)(2)(i)	Business Associate Contracts	(R) Required
(b)(2)	Requirements for group health plans	(R) Required

The Security Rule's **Documentation Requirements (164.316)**

- Sets forth ***specific requirements for all policies, procedures and documentation*** required by the Rule
- Requires covered entities to implement policies and procedures, but does not define either “policy” or “procedure”
  - Generally, **policies** define an organization’s approach. For example, most business policies establish measurable objectives and expectations for the workforce, assign responsibility for decision-making, and define enforcement and consequences for violations.
  - **Procedures** describe how the organization carries out that approach, setting forth explicit, step-by-step instructions that implement the organization’s policies.

The Security Rule's
Documentation Requirements (164.316) *(Cont'd)*

Implementation Specification or Standard		
No.	Title	R / A
(b)(1)(i)	Policies and procedures	(R) Required
(b)(2)(i)	Time Limit	(R) Required
(b)(2)(ii)	Audit Trails	(R) Required
(b)(2)(ii)	Availability	(R) Required
(b)(2)(iii)	Updates	(R) Required

An example:

164.316(b)(2)(iii) Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

AGENDA

About HIPAA

HIPAA Rules

- Privacy
- Security
- Breach Notification

Current Regulatory Environment

Addressing HIPAA

Purpose of the Breach Notification Rule

Requires CE's and BA's to track and provide notification of all breaches of unsecured PHI

- Notice must be provided without ***unreasonable delay*** (60 days)
- Specific content and procedure requirements for providing ***notices*** of breach
- Specific notification paths based on who is responsible for the breach (e.g., CE's, BA's, sub-BA's)

Audience of notification depends on breach size

- If breach involves more than 500 residents of a State or jurisdiction, provide notice to prominent media outlets in that State or Jurisdiction
- Same content requirements as notice to individual
- If breach involves 500 or more individuals, notify HHS Secretary simultaneously with notice to individuals
- If less than 500 individuals, maintain log and provide log to HHS Secretary within 60 days of the end of the calendar year

Breach tracking by OCR

Location of Breached PHI	Count	% of Total
Desktop Computer	174	13%
Electronic Medical Record	53	4%
Email	95	7%
Laptop	257	20%
Network Server	158	12%
Other	142	11%
Portable Electronic Device	121	9%
Paper/Films	296	23%
Grand Total	***1296***	***Breaches***

143,568,209 records breached!

21% of breaches caused by Business Associates

Type of Breach	Count	% of Total
Hacking/IT Incident	132	10%
Improper Disposal	52	4%
Loss	120	9%
Other	105	8%
Theft	639	49%
Unauthorized Access/Disclosure	233	18%
Unknown	15	1%

Data as of 8/15/2015

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

Securing PHI

- Notice requirements apply only to breaches of **unsecured PHI**
- "**Secured**" means unusable, unreadable or indecipherable to unauthorized individuals in accordance with methods and technologies specified by HHS
- Technology and methodology to render PHI secure: **destruction** and encryption
- If all of your PHI is “secured”, the breach notification obligations do not affect you

Securing PHI *(continued)*

The "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals":

- NIST SP 800-52: Guidelines for the Selection and Use of TLS Implementations
- NIST SP 800-77: Guide to IPsec VPNs
- NIST SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-113: Guide to SSL VPNs
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules
- NIST SP 800-88: Guidelines for Media Sanitization

Implementing these technologies provides "safe harbor" from breach notification requirements.

Extension of privacy protections to vendors of Personal Health Records (PHRs)

- Vendors of personal health records will have to report breaches of identifiable health information in much the same way that covered entities are required.

- This also extends to a third party service provider who provides services to a vendor (similar to what a business associate is to a covered entity). This section will be enforced by the Federal Trade Commission and will be considered an "unfair and deceptive act" under the Federal Trade Commission Act.

- PHR vendors, such as Google Health, etc. are not covered entities under HIPAA. This has been concerning to many privacy advocates and this change will provide at least some of the protections and accountability of HIPAA.

HIPAA – Breach Notification Rule

Enforcement by State Attorney Generals:

- Allows state Attorney Generals to bring civil actions on behalf of residents, up to an amount of $25,000 per year for identical violations (violation x$100 for each individual) and attorneys fees.
- This is new and is one more avenue that patients can use to have breaches addressed.

Harmed Individuals May Share in Civil Monetary Penalties:

- Within three years there will be a mechanism established by which individuals who were harmed by a disclosure will be able to share in civil monetary penalties collected by HHS.
- Previously HIPAA did not provide for a private cause of action or injured persons getting any compensation for data breaches (outside of possible state law claims for common law causes of action).

Fines associated with HIPAA Violations and Breaches

Violation Category – Section 1176(a)(1)	Each violation	All such violations of an Identical Provision in a Calendar Year
(A) Did Not Know	$100	$ 25,000
(B) Reasonable Cause	$1,000	$ 100,000
(C)(i) Willful Neglect – Corrected	$10,000	$ 250,000
(C)(ii) Willful Neglect - Not Corrected	$50,000	$1,500,000

Criminal penalties for a person who obtains or discloses PHI in violation of HIPAA

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to 1 year
Under false pretenses	Up to 5 years
For personal gain or malicious reasons *(i.e., intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm)*	Up to 10 years

Example PHI breaches

- **Examples of paper breaches include:**
  - Misdirected paper faxes with PHI to incorrect recipient
  - Loss or theft of paper documents containing PHI
  - Mailings with PHI to incorrect recipient

- **Examples of electronic breaches include all of the following if they contain PHI:**
  - Stolen unencrypted laptops, hard drives, or PCs
  - Stolen unencrypted thumb drives
  - FTP software allowing anonymous logins
  - Printer hard-drives leased to other organizations without first being wiped

Example OCR breach enforcement action #1

Who: Concentra Health Services **When:** April 22, 2014

What: OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

Result: $1,725,220 in fines

Example OCR breach enforcement action #2

Who: Wellpoint, Inc. **When:** July 11, 2013

What: The OCR began its investigation following a breach report submitted by WellPoint. The report indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.

The investigation indicated WellPoint did not:

- perform an appropriate technical evaluation in response to a software upgrade to its information systems
- have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

Result: $1.7 million in fines

AGENDA

About HIPAA

HIPAA Rules

- Privacy
- Security
- Breach Notification

Current Regulatory Environment

Addressing HIPAA

Healthcare Industry Regulators

Healthcare Industry Regulators (Continued)

Authority	Description	Related IT Security Regulation
HHS	The Department of Health and Human Services (HHS) is the United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves	HIPAA and HITECH
ONC	ONC is the principal Federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information. The position of National Coordinator was created in 2004, through an Executive Order, and legislatively mandated in the Health Information Technology for Economic and Clinical Health Act [HITECH Act] of 2009.	HITECH HITECH Policy and Standards Committees
OCR	OCR helps to protect you from discrimination in certain healthcare and social service programs. OCR is responsible for enforcing the HIPAA Privacy and Security rules	HIPAA Privacy and Security
CMS	To ensure effective, up-to-date health care coverage and to promote quality care for beneficiaries	CMS Computer Security Requirements for contactors
FTC	Oversees issues related to consumer privacy, credit reporting, identity theft, and information security	FTC Red Flags Rule HITECH (personal health records)
States	Protect the privacy and security of information related to state residents	HITECH Various state requirements for breach notification, security and privacy (e.g., California)

Healthcare Industry Frameworks & Standards

Authority	Description	Areas Affected	Cross-Referenced
HITRUST	The Health Information Trust Alliance (HITRUST) exists to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges.	All organizations from all segments of the healthcare industry	ISO 27001/2, NIST 800-53, CMS, PCI HIPAA, HITECH COBIT, FTC Red Flags Rule, State Requirements
HRAC	Healthcare Resource Access Control	Distributed enterprise systems, healthcare information systems, distributed object technology, Object Management Architecture (OMA), Common Object Request Broker Architecture (CORBA)	Role-based Access Control, NIST, distributed object technology standard OMA/CORBA
SOC 1	Statement on Auditing Standards No. 70: Service Organizations. This is a statement by an auditor on the internal controls of a service organization.	Internal controls and computer controls. However, there are no pre-established control objectives or criteria.	SOC 3
SOC 3	SysTrust provides professional guidance and best practices for system reliability. Other areas covered include: Availability, Security, Integrity, and Maintainability. SysTrust was developed by the AICPA and CICA (Canadian Institute of Chartered Accountants).	Internal controls and computer controls. However, there are pre-established control objectives or criteria.	SOC 1
PCI DSS	Payment Card Industry Data Security Standards. These standards were created by the major credit card corporations to define how payment cardholder and card authentication data must be stored, managed and processed to keep it secure.	Systems that accept, handle, and/or store payment card information and data.	

Healthcare Industry Frameworks & Standards (Continued)

Authority	Description	Areas Affected	Cross-Referenced
URAC	Utilization Review Accreditation Commission. This is a nonprofit unit that establishes accreditation standards for managed care organizations. URAC's programs include HIPAA Security and HIPAA Privacy.	Claims processing, HIPAA areas, Health websites.	HIPAA
CCHIT	Certification Commission for Healthcare Information Technology. This entity serves as the recognized US certification authority for electronic health records (EHR) and their networks.	Patient record privacy, criteria and inspection processes for electronic health records.	
ONCHIT	Office for the National Coordinator for Health Information Technology. This Office provides counsel to the Secretary of HHS and Departmental leadership for the development and nationwide implementation of an interoperable health information technology infrastructure.	The mission of this office is to achieve widespread adoption of interoperable electronic health records in the US within 10 years.	US Dept of Health and Human Services, American Health Information Community
ISO	ISO 17090:2008, Health informatics – Public Key Infrastructure. This defines how digital certificates can be used to provide security services in the health industry.	Public key cryptography and digital certificates protecting information in transit	
HIPAA	Health Insurance Portability and Accountability Act - The Act establishes regulations designed to protect health insurance benefits, as well as sensitive information about the insured.	Overall Information Security Plan, Secure User Authentication, Access Control Mechanisms, Information Access Monitoring/Audit Trails, Physical Security and Disaster Recovery, Data Integrity Monitoring, Communication and Awareness, Risk Assessments, Documentation.	

Healthcare Industry
Frameworks & Standards (Continued)

Authority	Description	Areas Affected	Cross-Ref.
NIST	National Institute of Standards and Technology	Healthcare Standards Roadmap Development; Healthcare Standards Gap Analysis; Conformance Test Development of Appropriate Healthcare Standards; Validation Program Guidance for Relevant Healthcare Standards Bodies and Guidance on Appropriate Use of IT Security Technologies; Guidance on Developing Appropriate User Interfaces, Including Speech Recognition Information Modeling Integration of Healthcare Information Models; and Neutral Facilitator for Building Bridges between Healthcare Standards Bodies Analysis and Modeling of Healthcare documents workflow process.	ITIL
COBIT	Control Objectives for Information and Related Technology. These control objectives detail best practices for Information Technology management	IT Management, specific and detailed control objectives through IT processes	
ITIL	Information Technology Infrastructure Library details a set of concepts and techniques for managing information technology infrastructure, development, and operations	IT Service Management	

Healthcare Industry
Frameworks & Standards (Continued)

Authority	Description	Areas Affected	Cross-Ref.
HITSP	Health Information Technology Standards Panel. This panel will be the intermediary between the public and private sectors with the purpose of achieving accepted and useful standards to enable and support widespread interoperability among healthcare software applications, as they will interact in a local, regional and national health informati	Work groups include: Security and Privacy, Electronic health records, Consumer Empowerment, Biosurveillance	CCHIT, HISPC
HISPC	Health Information Security and Privacy Collaboration	Goals: Identify both best practices and challenges, develop consensus-based solutions for interoperable electronic health information exchange (HIE) that protect the privacy and security of health information, and to develop detailed implementation plans to implement solutions.	ONCHIT
NHIN	Nationwide Health Information Network Architecture Projects. This network would link disparate health care information systems together to allow patients, physicians, hospitals, public health agencies and other authorized users across the nation to share clinical information in real-time under stringent security, privacy and other protections.	Electronic health records	ONCHIT

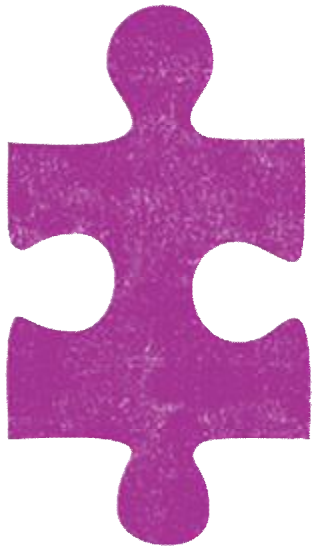
Who is enforces HIPAA?

The Department of Health and Human Services (HHS) is currently responsible for overseeing HIPAA

- Initially the Office for Civil Rights (OCR) was responsible for overseeing Privacy rule compliance
- Initially the Centers for Medicare & Medicaid Services (CMS) was responsible for overseeing Security rule compliance
- Initially limited enforcement to complaints by consumers
- Initially, the civil penalties were $100 per violation not to exceed $25,000 per year for identical violations

CMS HIPAA Enforcement Woes

A nationwide review of CMS HIPAA oversight performed by the OIG in 2008 found that:



- CMS had not provided adequate oversight for three (3) years
- CMS was authorized to conduct reviews as of 2/16/2006 but failed to conduct any
- After receiving OIG's report – CMS started auditing security rule compliance at CE's where complaints had been filed

Results of these initial CMS audits showed numerous, significant violations of HIPAA's security rule

Reactive HIPAA audits by regulators

During 2008, CMS contracted with PWC in a 1-year, $898K contract to conduct on-site reviews of security rule compliance at 10 HIPAA Covered Entities (CEs)

During 2009, CMS conducted a review of 5 more HIPAA CE's

CMS initiated these reviews based on complaints filed against the entities, identification of potential Security Rule violations through the media, or recommendations from HHS or the OCR

Weakest Areas of Security Rule Compliance per CMS 2008-09 Audits		
BAA's	Security Training	Workforce Clearance
Policies & Procedures	Workforce Security	Encryption
Currency and Adequacy of Policies and Procedures		

Regulators shift to **proactive** HIPAA audits

During 2010-11, OCR engaged Booz Allen Hamilton for covered entity identification and cataloging

During 2011, HHS entered into a $9.2M contract with KPMG for a protocol and audit performance program to

> *"…assist OCR in operating an audit program that effectively implements the statutory requirement to audit covered entity and business associate compliance with the HIPAA privacy and security standards"*

2012 Pilot Audit Program

During 2012, 115 covered entities were proactively audited during 2012 under the HHS/KPMG contract (which was referred to as the "pilot audit program")

- Created an OCR audit protocol of the security, privacy and breach notification safeguards included

- Security findings account for 60% of all findings

- *Only 11% of audited CE's had no findings*

During 2013, the OCR engaged PWC to evaluate the pilot audit program to "further improve it"

What's next for HIPAA enforcement by regulators?

In **March 31, 2014:** OCR announced plans for "Phase 2" of HIPAA security, privacy and breach notification rule audits

- OCR planned to randomly audit 350 CE's and 50 BA's
  - 35 "IT related" BA's (e.g., cloud hosting providers)
  - 15 "Non-IT related" BA's
  - Between Oct 2014 through June 2015
- Those audits were delayed
- OCR decided to issue HIPAA surveys to a random list of 550-800 CE's and BA's and provide a portal for responses
- Surveys are in process and **Audits to Come**

AGENDA

About HIPAA

HIPAA Rules

- Privacy
- Security
- Breach Notification

Current Regulatory Environment

Addressing HIPAA

Types of Projects

- ePHI discovery scans
- HIPAA risk assessment
- HIPAA compliance gap analysis
- HIPAA AT- 601 compliance report

ePHI discovery scan

- **Goal:** Identify where customer medical data resides on the network

- **Tasks:**
  - Scan file extensions of live network hosts to identify medical image files
  - Scan file contents of all files on a selection of servers and workstations to find other ePHI

- **Deliverable:** Inventory consisting of host name and (where possible) system user / owner name and department

- **Typical duration:** 1-3 weeks (start to finish)

HIPAA risk assessment

- **Goal:** Formally assess risks around the security and privacy of customer medical data residing in the organization's network (required by HIPAA)

- **Tasks:**
  - Interview members of business and IT management to identify the threats and vulnerabilities to PHI/ePHI stored, accessed, maintained or transmitted
  - Identify controls in place to mitigate these threats and vulnerabilities
  - Review documentation (e.g., policies, procedures, SOP's, screenshots, reports)
  - Develop and evaluate residual risks to customer PHI security and privacy

- **Deliverable:** Populated and categorized risk assessment matrix

- **Typical Duration:**
  - Depends on size of organization, CE or BA, and if being performed in conjunction with gap assessment
  - About 3-8 weeks for mid-sized business associates

HIPAA compliance gap analysis

- **Goal:** Assess the current state of the organization's systems and processes against HIPAA requirements and make recommendations for improvement
- **Tasks:**
  - Interview business and IT management to understand current controls and processes contributing to HIPAA compliance
  - Review relevant documentation (e.g., policies, procedures, SOP's, screenshots)
  - Conclude on the design and/or effectiveness of controls in place which contribute to HIPAA compliance
- **Deliverables:**
  - Internal Report of detailed recommendations for areas found lacking
  - Indication of which HIPAA requirements are and are not currently being achieved
- **Typical Duration:**
  - Depends on size of organization, CE or BA, and if being performed in conjunction with gap assessment
  - Can last anywhere from 1 week to 4 months

HIPAA compliance AT-601 report

- **Goal, Tasks, and Duration:** Similar to the HIPAA compliance gap analysis
- **Deliverable:** A **HIPAA compliance attestation report** under AICPA standards that can be provided externally
- The final report could be provided to **third parties** such as:
  - Auditors
  - Customers' Auditors
  - Customers
  - Regulators

QUESTIONS