

NPO PAAC Meeting

May 8, 2014

Attendees:


Hannah Howard – GLDHA
Pam Stoner – GLDHA
Vickie Slifka – PCHA
Laurie Hughey – PCHA
Bob Farrell – IMNM
Karen Williams – IMNM
Mark Crosby – IMNM
Marty Whitcomb – Bayside
Rosemary Fielding – IMNM
Tersa Migda, IMNM

Speakers: ISC is an Information Technology Company specializing in Healthcare IT.
Topic: HIPPA Security & risk analysis.

Submitted By: Pam Stoner


HIPAA Update

Presented by




HIPAA - History

- The Health Insurance Portability and Accountability Act (**HIPAA**) was enacted by Congress in 1996 in response to several issues facing health care coverage, privacy, security, and fraud in the United States.
 - Dec. 2000 – Privacy Rule Published
 - Apr. 2003 – Privacy Compliance Required
 - Feb. 2003 – Security Rule Published
 - Apr. 2005 – Security Compliance Required

May 2014 Confidential & Proprietary  2

Privacy Rule


- Primary goal – To assure that individuals' Protected Health Information (PHI) is protected while allowing the flow of health information needed to provide and promote high quality health care.
- The Rule attempts to strike a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.
- Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

May 2014 Confidential & Proprietary  3

What Information is covered under HIPAA

Protected Health Information (PHI)

- Information health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's information systems
- Billing information about you at your clinic
- Most other health information about you held by those who must follow these laws

May 2014 Confidential & Proprietary 


HIPAA Privacy Rule Provisions

Use/Sharing of PHI

- Can be used for purposes of treatment, payment or business operations without an individual's express permission or consent
- Requires an individual's express permission for marketing, advertising and other purposes

Minimum Necessary Rule

- A covered entity generally may only use as much information as is necessary for accomplishing the intended purpose
- Does not apply to disclosures of PHI to other healthcare providers for treatment

May 2014 Confidential & Proprietary 

Policies & Procedures


Establish policies that cover activities in your practice

- Policies should be in writing and updated when there are changes in your business

Train Staff

- New hires
- Changes in responsibility
- As policies change

Audit your systems to ensure compliance

May 2014 Confidential & Proprietary 

Safeguards for PHI

Physical Security

- Lock offices and cabinets containing PHI
- Screen PHI from public view

Technical Security

- Use passwords on desktops and portable devices
- Encrypt your data!

Instill a Culture of Compliance

- Treat information as you would treat the patient
- Provide leadership

May 2014

Confidential & Proprietary



7

Questions to Ask

- What PHI is collected?
- Who collects it?
- How is it stored?
- Who has access to it?
- Who are you sharing it with?
- Is there particularly sensitive data?
- How is the data used?
- Is data stored in devices or other uncontrolled

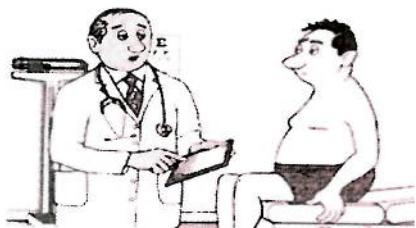
May 2014

Confidential & Proprietary



8

HIPAA



"According to your HIPAA release form I can't share anything with you."

May 2014

Confidential & Proprietary



9

HIPAA-HITECH

FINAL RULE RELEASED - Effective 3/26/2013

- Impacts Covered Entities, Business Associates and Subcontractors that perform activities involving use or disclosure of PHI
- BAs directly liable for compliance
- BAs need BA Agreements with Subs/Vendors
- BAs subject to HIPAA Audits

May 2014

Confidential & Proprietary



10

HIPAA-HITECH

FINAL RULE RELEASED - Effective 3/26/13

- Imposes notification requirements if a breach of PHI occurs
- Prior Standard: Risk of harm (financial/reputational) analysis
- New Standard: Use or disclosure of PHI is PRESUMED to be a breach unless low probability of compromised PHI
 - Four Factors now used
 - Covered Entity must provide notification within 60 days of breach discovery
 - If more than 500 individuals impacted, must give notice to HHS
 - If more than 500 from one state, media notice must be provided

May 2014

Confidential & Proprietary



11

Security Rule

- Covered Entities Must:
 - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
 - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
 - Protect against reasonably anticipated, impermissible uses or disclosures; and
 - Ensure compliance by their workforce.

May 2014

Confidential & Proprietary



12

HIPAA Enforcement

Privacy Rule

- Health & Human Services' Office for Civil Rights (OCR) has had enforcement responsibility since 2003

Security Rule

- OCR takes over enforcement of Security Rule in 2009

May 2014 Confidential & Proprietary 13

HIPAA Enforcement

Overview: The 2009 HITECH Act requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules.

- To implement this mandate, OCR implemented a pilot program to perform up to 150 audits of covered entities to assess privacy and security compliance.
- Audits conducted during the pilot phase concluded in 2013

May 2014 Confidential & Proprietary 14

How does HIPAA impact your organization?

- HIPAA now has solid enforcement standards
- Enforced by the Office for Civil Rights
- Maximum fines raised from \$25K to \$1.5M
- \$1.5M maximum penalty per year per violations
- Fines collected will fund continued enforcement
- OCR has an audit candidate target list (built primarily through complaints received)
- Practitioners and facilities face fines up to \$50K for falsely attesting to "Meaningful Use"
- States' Attorneys General may also pursue civil actions

May 2014 Confidential & Proprietary 15

FROM HHS WEBSITE

- A **HIPAA Security Risk Analysis** (§164.308(a)(1)(ii)(A)) is required by law to be performed by every Covered Entity and Business Associate. Also, completion of the Risk Analysis is a core requirement to meet Meaningful Use.

- Section 164.308(a)(1)(ii)(A) of the HIPAA Security Final Rule states:

RISK ANALYSIS (Required).

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the Covered Entity.

May 2014

Confidential & Proprietary



16

OCR Audit Results

2013 Photocopier Breach Case

- Affinity Health Plan, Inc. settled with OCR for \$1,215,780.
- Affinity filed a breach report with OCR in 2010 after it was informed by the CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

May 2014

Confidential & Proprietary



17

OCR Audit Results

Mass. provider settles with OCR for \$1.5M

- The investigation followed a breach report submitted by Massachusetts Eye and Ear Infirmary (MEEI) reporting the theft of an unencrypted laptop.
- OCR investigators also found that MEEI failed to comply with certain requirements of the Security Rule, such as conducting a thorough analysis of the risk to the confidentiality of ePHI and implementing security measures sufficient to ensure the confidentiality of the ePHI that MEEI created, maintained, and transmitted using portable devices.

May 2014

Confidential & Proprietary



18

OCR Audit Results

HHS settles with Phoenix Cardiac Surgery

- OCR received a report that the practice was posting clinical and surgical appointments on an Internet-based calendar that was publicly accessible.
 - Settlement Fee of \$100,000
 - Performance of a Security Risk Analysis
 - Implementation of a corrective action plan to develop policies and procedures to come into full compliance with the Privacy and Security Rules.

May 2014

Confidential & Proprietary



19

When should an organization re-evaluate HIPAA readiness?

- An organization should conduct an assessment at least once a year, with IP testing quarterly
Note: an annual assessment is now required by CMS
- Technology advances faster than many business models, why is this important?
 - Some organizations are performing some form of vulnerability assessment as often as monthly depending on the business model.

May 2014

Confidential & Proprietary



20

Other Steps to Take

Build a culture of compliance

- Establish Policies and Procedures to control ePHI
- Train your employees (document the training)
- Enforce your policies
- Perform a risk analysis
- Shore up risk areas identified
- Everyone needs to see themselves as responsible for privacy and security of PHI
- Managers establish importance of data privacy
- Make privacy a part of daily operation of business

May 2014

Confidential & Proprietary



21

How ISC can Help?

- An ISC HIPAA Security Risk Analysis includes:
 - Reviewing your organizations current HIPAA policies
 - Reviewing your organizations current HIPAA procedures
 - Assess your organizations current HIPAA technology policies
 - Assess your organizations current HIPAA technology procedures
 - Conduct an Internal Network Vulnerability Assessment
 - Conduct an External Network Vulnerability Assessment
- In addition ISC prepares a Security Risk Analysis Report detailing the issues identified and the risk level (H,M,L) for both the likelihood and the impact of those issues
- ISC will present the report and review course of action

May 2014

Confidential & Proprietary



23

Background and Services

- Nearly 30 years of business in the technology field
- Communication Network Infrastructure
- Voice and Data solutions
- Managed Services
- Disaster Recovery Planning
- Business Continuity Planning
- Technology Project Management
- Healthcare Focused Solutions

May 2014

Confidential & Proprietary



23

Background and Services

- Don Golinski, Account Executive
 - (989) 284-4730
 - dgolinski@i-s-c.com
- Troy Fairchild, Partner
 - (231) 492-0472
 - tfairchild@i-s-c.com
- Mike Zamiara, Partner
 - (517) 281-1528
 - mzamiara@i-s-c.com

May 2014

Confidential & Proprietary



24
