HIPAA Update
2017 Michigan Rural Health Conference

Presented by

May, 2017

Why the IT Guys From ISC are Here

- 30 years of healthcare technology support
- Performed hundreds of Security Risk Assessments for Covered Entities
- We provide healthcare facilities with operational, tactical and strategic network reviews and assist in attaining and/or maintaining HIPAA compliancy
- We have worked closely with auditors who perform inspections for HHS/OCR

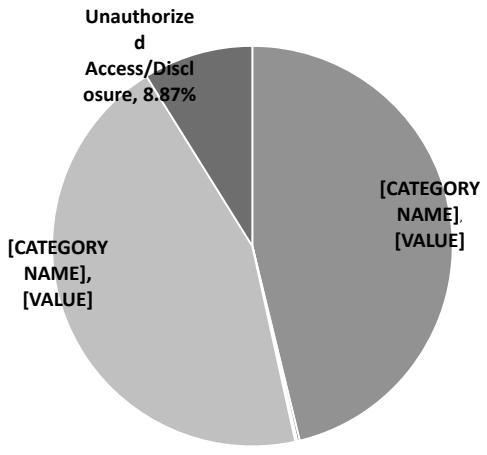
Why do I care if I am not a Covered Entity or Business Associate?

- The Federal Trade Commission (FTC), the nation's consumer protection agency, has issued the Health Breach Notification Rule to require certain businesses not covered by HIPAA to notify their customers and others if there's a breach of unsecured, individually identifiable electronic health information. FTC enforcement began on February 22, 2010.

  Found at: https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

First quarter of 2017 (Jan-Mar)

- 79 breaches involving 500 or more individuals



First quarter of 2017 (Jan-Mar) (con't)

- 4 HIPAA settlements totaling $11.375 Million ($3.2M, $2.2M, $5.5M, and $475,000) For 2016, there was a total of 12 settlements resulting in fines worth $22,855,300.
- These 4 breaches were first reported in 2010, 2011, 2012 and 2014
- Fines collected will fund continued enforcement

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

What Information is covered under HIPAA

"Individually identifiable health information" is 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,

and that identifies the individual, or for which there is a reasonable basis to believe can be used to identify the individual. Includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Privacy Rule

- Primary goal – To assure that individuals' Protected Health Information (PHI) is kept confidential 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

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

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

Manage your Business Associates

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 who hold ePHI. 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.

HHS.gov Guidance on Risk Analysis

- *"…The risk analysis process should be ongoing. In order for an entity to update and document its security measures "as needed," which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).) The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities…"*
- Retrieved from: http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

HIPAA

HIPAA Update

NIST/OCR 9th annual conference - ***Safeguarding Health Information: Building Assurance through HIPAA Security*** **:**

- Ransomware, Cloud Computing Guidance
- Breach Notification Rule and Breach Activity
- Recurring Audit Issues (BAA's; RA's; P&P; Encrypt)
- Auditing and Patching
- Insider Threat
- Backup and Contingency Planning

Recurring Audit Issues

Per OCR

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup or Contingency Plan

Breach Notification Rule

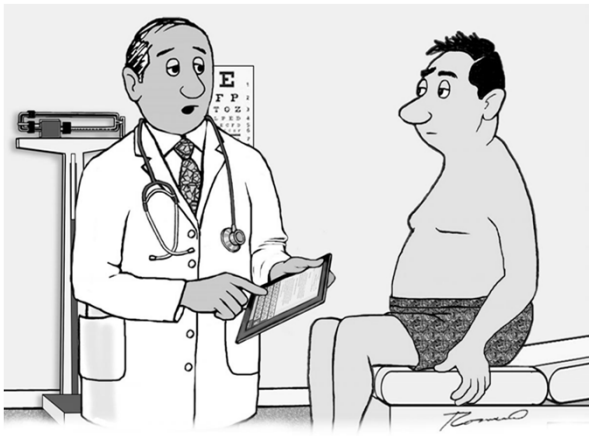
There was renewed emphasis on the Breach Notification rule:

What is a Breach - Impermissible acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of the PHI.

Safe Harbor - If the PHI is encrypted or destroyed.

More detailed reporting instructions can be found at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HIPAA



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

Business Associates

Examples of a Business Associates

- A third party administrator that assists a health plan with claims processing and/or billing
- A CPA firm or Law firm whose services involve access to PHI
- A consultant that performs utilization reviews for a hospital
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer
- An independent medical transcriptionist that provides transcription services to a physician
- A document shredding service that shreds documents containing PHI

Business Associates

Janitorial service – Business Associate?

Per HHS.gov **Situations in Which a Business Associate Contract Is NOT Required. ISC does recommend having a Security Agreement.**

> **"**With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and **where any access to protected health information by such persons would be incidental, if at all.** " (http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html)

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
- Use tools @ HealthIT.Gov

Maintain written documentation

Audit your systems to ensure compliance

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

Trusted Resources

- HHS Office for Civil rights – www.hhs.gov/ocr/privacy/hipaa
- The Office of the National Coordinator for Health Information Technology (ONC) - www.healthit.gov
- ONC Guide for Privacy/Security - www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- HIPAA Journal - http://www.hipaajournal.com/

News from HIPAA Journal

- **Simplified HITRUST CSF Program Helps Small Healthcare Organizations with Compliance and Risk Management,** March 2nd, 2017, HIPAA JOURNAL, found at: http://www.hipaajournal.com/simplified-hitrust-csf-program-helps-small-healthcare-organizations-with-compliance-and-risk-management-8713/
- **Quarter of Americans Have Been Impacted by a Healthcare Data Breach**, February 22nd 2017, HIPAA JOURNAL, found at: http://www.hipaajournal.com/8-8-million-healthcare-records-breached-in-august-3588/
- **OCR HIPAA Enforcement: Summary of 2016 HIPAA Settlements**, January 12th 2017, HIPAA JOURNAL, found at: http://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/
- **Unknown Malware Downloaded every 4 Seconds by Employees**, Sept 29th 2016, HIPAA JOURNAL, found at: http://www.hipaajournal.com/unknown-malware-downloaded-every-4-seconds-employees-3610/
- **HHS Criticized by GAO for ePHI Security Guidance and CE Oversight**, Sept 27th 2016, HIPAA JOURNAL, found at: http://www.hipaajournal.com/gao-report-hhs-improve-hipaa-oversight-ephi-security-guidance-3608/