HIPAA – Overview and updates since HITECH and PPACA

Presented by: Angela Miller, CMC, CHC
Medical Auditing Solutions LLC

2013

Learning Objectives

- Overview the high level HIPAA privacy and security rules resulting from HITECH Act
- Understand HIPAA changes resulting from the introduction of the Affordable Care Act
- Understand the nature of Security/Privacy breaches associated with PHI
- Gain a general understanding of how the regulatory changes will affect organizations in general

Overview - HIPAA & HITECH

Description

- HIPAA rules were significantly modified in 2009 with the HITECH act. Since then HIPAA rules have undergone further refinement and modification with implementation deadlines in 2013. The Affordable Care Act begins implementation in the fall and brings with it HIPAA implications.

- This presentation will provide a high level update regarding recent HIPAA regulatory changes, pending changes, and anticipated operational impacts resulting from the Affordable Care Act. The presentation will give insight into the topics auditors and security professionals should be aware of in assessing their internal privacy and security compliance programs.

HIPAA Implementation Deadlines

- HIPAA – 2003
  - Primarily paper, Notice of Uses, and access to information
    - Requirement for all healthcare providers to be fully EMR for clinical documentation
      - Documentation is worse now than ever before
      - Templates do not contain all information to justify E&M billing or they auto populate without performing
      - Brings up discussions of cloud hosting versus servers in office

Elements of HIPAA Programs

- Identify Privacy & Security Officer(s)
- Advisory Committee
- Have Written Policies & Procedures with Forms
  - Complete, Current, Applicable, Implemented!
  - Review periodically
    - Including Credit Card Processing Policies
- Perform Annual Training
  - Keep reminders in front of ALL employees
  - **Federal is annually**; State may be less

Elements of HIPAA Programs

- Perform Risk Assessments AT LEAST annually
  - Know who has access & where PHI & e-PHI is kept and stored
  - What works and what doesn't
- PCI - Credit Card encryption
  - Some machines are outdated & not compliant
  - Self certification is really not sufficient
  - There is a PCI discussion will be later today be sure to attend
    - Fines on Credit Card breach are significant

Elements of HIPAA Programs

- Perform Audits at least annually
  - Are patients provided access to Notice of Uses
  - Is staff compliant on PHI disclosures
  - Is your IT network secure, does it have risks
- Complaint Reporting Process/Method
- Organization Chart
- Network Diagram

Policies

- Written Policies & Procedures
  - Approximately 75 policies added with HITECH,
  - Initial HIPAA policies approximately 40 policies
  - See handout for policies I audit for with healthcare providers
  - This may be electronic and posted on your intra-net within your organization
  - But must be accessible to all employees

Auditing

- Auditing and Monitoring
  - These systems must be designed to detect and prevent breaches
  - No less than annual monitoring
  - Need to assess your risk areas
    - Number of PC, mobile devices, VPN, remote access, non-company computers, encryption or not, etc.

Complaints & Reporting

- Reporting Options for Communication
  - Hotline Poster (nothing fancy)
  - Open access to the officer
  - In auditing, make sure that each complaint is taken seriously and addressed timely

Enforcement & Discipline

- Enforcement and Disciplinary Standards
  - A strong, fair, and consistent stance is very important
  - Be careful not to create a “precedence” for future issues
    - Example: This time a person forges your signature, you write them up but next time you want to fire them

HITECH Changes

- HITECH - 2009
  - All things electronic, access to, networks, PC, mobile devices.
  - Added ~75 required policies specific to Networks, Facility, Administrative, Disaster planning, etc.
  - Some references to expanding to Business Associates (BA)

  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

HIPAA Omnibus Rule

- Effective 2013
- HHS will investigate any breach now not just "may"
- Have to go to Secretary of HHS to get a waiver on investigation
- Easier to prosecute and include Willful Neglect charges
- Clearly expanded language to Business Associates

HIPAA OMNIBUS –Extends to BAA

- All the previous responsibility extends to Business Associates
- Business Associates are now just as liable as Covered Entity
- Business Associate is anyone providing service, labor, etc to a covered entity who may see or have access to PHI

BAA Extension Impacts Covered Entity

- BAA Log include date, why, their username provided, etc
- BAA Contract ALL need to be revised by 9/23/13 includes the new language
  - This may eliminate many BAAs
  - BAAs need to have breach insurance
  - BAA need all elements previously discussed
  - How they store and/or return documents
    - Encryption
  - What types of security and malware software

BAA Extension Impacts Covered Entity

- Covered Entities will vary in what BAA must provide as proof
  - Larger facilities may require proof of all items, including risk assessments
  - Smaller facilities may require nothing more than BAA explaining responsibility to perform
    - Currently, law firms are only requiring me to sign a BAA

Offshore Business Associates

- Covered Entities need to be cautious about using offshore companies
  - Rules state CE can use an offshore BA
  - However, loophole is DHHS cannot pursue them for violations
  - Supreme Court Case makes it "very doubtful" that U.S. regulators would be able to take HIPAA **enforcement** actions against offshore vendors even if U.S. patient data is exposed in a security incident, he notes.

HealthInfoSecurity.com Sept. 5, 2013 article HIPAA Omnibus Rule
http://omnibus.healthcareinfosecurity.com/interviews/offshore-vendors-enforcing-compliance-i-2054?rf=2013-09-05-eh&elq=990ebae5382845f092eaf34c6aa1a1f5&elqCampaignId=7690

Audit and Enforcement

Auditors

- OCR – Office for Civil Rights
  - 10 day response deadline, no extensions
    - Being extended to 15 days still no extension
  - With or without a complaint
  - Including Self Insured Plans
- KPMG
  - Audited approximately 150 companies in 2011-2012
  - Varying sizes & type of providers
    - and self insured businesses
    - Doubt chance of audit

Audit Notification

- Consensus has been the letters are going to the "CEO"
  - Even with named Privacy or Security Officer
  - Letter may or may not include a name with the title.
  - All types of healthcare providers and self insurance plans
- Provides the document request with production in 10 -15 days

Site Visit of Audit Phase

- Site Visit in 30-90 days from date of the letter
  - 3-10 days in length
  - May not have notice
  - Additional inquiry and analysis
  - Exam of physical business, location, records
  - Employee interviews
- Draft audit report 20-30 days after on-site
  - Usual Methodology, Findings, Best Practices, Option to Appeal
- Appeal Comments due within 10 days of report
- Final Report is due to OCR within 30 days

Common Errors

- Misuse of PHI
- Failure to follow policies and insufficient policies
  - Checklist
    - http://www.medicalauditingsolutions.com/services/
- No contingency plan
- Failure to monitor access
- Failure to perform risk assessments and audit
- Just a few reference Mentz Levin Whitepaper
    - http://www.jdsupra.com/post/documentViewer.aspx?fid=b4c67253-787e-4acb-8865-5796f03fa348

Healthcare Provider Employee/Contractor Monitoring

- Monitoring – must be done by healthcare providers/ BA
  - Monitoring Employees and Vendors
    - OIG & EPLS Sanction Provider Databases
      - **Monthly!**
      - Fine is $10K per day for employing or doing business with the referral source or vendor that is sanctioned
    - Criminal background checks
      - If going in patient homes, no less than annually and best to do bi-annually
      - If they are involved in patient care and have possibility to abuse a patient

PPACA Adds Changes

- Insurance Expansion of Coverage, No Max Lifetime, No Pre-existing
- Affordable Care Organizations
- State Health Insurance Exchanges
- Companies with 50 employees or greater to provider health insurance to employees
  - Penalties to companies who do not
  - Penalties to individuals without insurance
- Standard Transaction Sets and Health Plan Compliance
- Several Billing Requirements

Patient Protection Affordable Care Act (PPACA) – Insurance Expansion

- PPACA has several other requirements, although not limited to; requirements for:
  - Businesses to provider health insurance for groups >=50 FTEs; Employees mandated to purchase insurance
  - State Health Insurance Exchanges (HIE)
    - Businesses can shop HIE
      - TX will not offer HIE the government will operate for TX
      - Other states may so your employees can shop there
  - Accountable Care Organizations (ACOs)
    - How to share PHI and medical info yet be compliant

PPACA – Insurance Expansion

- Providers must ensure they bill correctly for:
  - Preventative services (reimbursed 100%)
  - New limits on MRI and CT Scans (Medicare)
  - Subsequent diagnostic images reduced by 25% (Medicare)
  - Physician new ownership in hospitals is restricted
  - Overpayments must be refunded within 60 days or will be considered false claims
  - Ant-kickback violations will result in false claims

PPACA – Insurance Expansion

- Providers must ensure they bill correctly for:
  - New self disclosure protocol for Stark Law violations
    - Stark and Anti-Kickback Violations are now subject to False Claims
  - PQRI – Physician quality reporting for specific disease states will impact physician pay rate

PPACA – Transmission Standards

- In addition to Privacy, PPACA also has several other requirements such as although not limited to; requirements for:
- Issue Final Rules to adopt standards for:
  - Electronic Funds Transfer (EFT),
  - Unique Health Plan Identifier (HPID),
  - and Health Claim Attachments
- Adopt a single set of Operating Rules for each standard transaction adopted under HIPAA
  - Consider recommendations for the Operating Rules developed by a qualified non-profit entity that meets specific criteria

PPACA

- Adopt a single set of Operating Rules for each standard transaction adopted under HIPAA …Continued
  - Consider recommendations of the National Committee on Vital and Health Statistics (NCVHS) when adopting Operating Rules
- Conduct periodic audits of health plans (including entities providing contracted services to health plans) to ensure compliance with HIPAA standards and Operating Rules
- Assess penalty fees against health plans that fail to certify and document compliance

PPACA

- Billing Compliance Programs are now required by 2013 with the new Health Care Reform bill & Patient Protection & Accountable Care Act signed in 2010, in addition to HIPAA
  - Primarily about relationships, contracts, and billing and coding
  - Applies to ALL Medicare & Medicaid type providers

Risks

- Tax Penalties for lack of health insurance
- Audits for billing errors which can expand to investigations
- State Licensure Investigation/Sanctions
- Business Closure
- Civil and/or Criminal Penalties
  - Fines and Penalties
    - Small health care providers $350K+-
    - Larger health care providers $7.2M
  - Can shut a business down without the other ramifications

Breaches Are Growing

Few Healthcare Industry Related Facts

- Healthcare is ranked No 1 for threats of data breach and identity theft
- >60% of breaches are due to theft, loss mishandling of PHI
- By far, paper PHI is still the greatest risk for breach.
- Breaches on average have a cost of $7.2M
  - Includes common fine amount of $1.5M
    - $350K for small providers
  - Balance is down time, lost revenue, victim notification and protection costs, legal cost

Breach Reporting for HIPAA

- Itemized detail, Cause, & Remediation
- <500 records can be reported to HHS Annually
- > 500 records must be reported within 60 days of indentifying the breach
  - Must use media notification to public
- Patient notification
  - If 10 or more patient notifications return for bad address, must go to media
- BA has 60 days and as soon as reasonable to report to CE
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Healthcare Breach Data – Ponemon Institute

- 94% of healthcare reported at least 1 incident in the last 2 years
  - 45% reported have 5=>incidents
  - While in 2010, only 29% reports 5 incidents
- Medical ID Theft 2-10 incidents 33%
- This is a drastic increase
- A reason for:
  - Training!
  - Cause
  - Prevention Strategy

- From Ponemon Institute LLC 3rd Annual Report Dec 2012

Healthcare Breach Data – HHS

- HHS Wall of Shame
  - 2013 of 54 cases; 463K records
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
- Privacy Rights Clearinghouse 2012 Reports
  - 1.18M Records with 224 public notification center
  - From: Unintended Disclosure, Hacking, Payment Card Fraud, Insider, Physical Loss, Portable or Stationary Devices, and & Unknown

Healthcare Breach Data - Newsday

- Reports March 2013 – Medical Identify Theft up 61.5%
  - Someone stealing information to use to see a healthcare professional

- http://www.newsday.com/news/health/federal--stats--identity--theft--of--medical--records--on--rise--1.4744135

HIPAA Violation Settlements 2013

- The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health & Human Services' (DHHS) $50,000 to settle potential violations of unsecure laptop stolen 441 records
  http://www.hhs.gov/news/press/2013pres/01/20130102a.html
- Calif.-based Shasta Regional Medical Center, a Prime Healthcare Services hospital, has agreed to pay DHHS $275,000 for sending PHI by email to >900 employees
  http://www.healthcareitnews.com/news/prime-healthcare-pays-275k-breach
  - Remember, this is settlement costs only!
  - See HHS link for more
    http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

CONCLUSION

- These requirements are not going away
- Risk are growing with Technology, HIE and ACO data sharing
- Your clients may have been doing this already, you just need it on paper
- Clients don't have the time to keep up with all these rules, they look to you for direction
- Ensure IT person/company has data security experience and is capable
  - The family & friends could prove costly
- The keys are Support, Teamwork, Training & Audits

Medical Auditing Solutions LLC

- Compliance & HIPAA Programs
- Billing & Coding Audits
- Payer Audit and Appeals
- Provider Credentialing
- IT Audits done by one of the business partners

We work with #medical providers on #billing and #coding audits, OIG Compliance Programs, HIPAA and Security Programs, insurance audit appeals, Medicare, Medicaid, Physicians, Dentists, Medical Equipment Providers, and Home Health

Contact Information

Angela Miller, CHC, CMC
President/CEO
Medical Auditing Solutions, LLC
& MAS Compliance University
972-459-1508 or 409-673-7103
angela@medicalauditingsolutions.com
(if you do not hear back via email in 24 hours, call me)
www.MedicalAuditingSolutions.com
ComplianceUniversity.MedicalAuditingSolutions.com
Follow me on Linkedin & Facebook

General References

- OIG Compliance Guidance - http://oig.hhs.gov/compliance/
- Federal Register – Employing a Sanctioned Person Pg 14393 & 14399 (search $10,000)
- http://oig.hhs.gov/authorities/docs/hipaacmp.pdf
- Audit Protocol – do not let this fool you "inquire of management" does not mean this is it. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- Texas Medicaid Audit http://wp.me/pyziu-5T
- Compliance Program http://wp.me/pyziu-3p

General References

- Tricare's comments http://www.tricare.mil/tma/hipaa/ppaca.aspx
- Fox Group Article http://www.foxgrp.com/blog/affordable-care-act-implications-for-medical-practices/
- Specific quotes are noted on those slides