"Do You Know When a HIPAA Business Associate Agreement is Required?"

TAANA Annual Meeting 2014
Las Vegas, Nevada
Oct. 11, 2014

Randi Kopf, RN, MS, JD
Kopf HealthLaw, LLC
Rockville, Maryland
www.kopfhealthlaw.com
301-251-2788

Rose M. Matricciani, RN, JD
Whiteford, Taylor & Preston LLP
Baltimore, Maryland
rmatricciani@wtplaw.com
410-347-9476

DISCLAIMER

This information is being provided as general education for informational purposes only and not for the purpose of providing legal advice. Although it was prepared by a professional it is not to be utilized as a substitute for personal legal counsel.

ARE YOU A BUSINESS ASSOCIATE?

When an attorney creates, receives, maintains or transmits protected health information on behalf of a Covered Entity (CE) or Business Associate (BA)
HITECH ACT Commentary 78Fed.Reg.at 5598

ARE YOU A BUSINESS ASSOCIATE?

- Examples
  - 1. Your client is a billing company and asks you to review patients' billing reports in their dispute with a physician practice for which they bill.
  - 2. Your client is a drug store that is being audited by the State licensing body. They want you review records that include patient prescriptions.

ARE YOU A BUSINESS ASSOCIATE?

YES

Attorneys and Law Firms need to develop and implement polices and procedures for HIPAA, HITECH and the 2013 Omnibus Rule

HIPAA OVERVIEW

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and effective 2003
  - Established standards to protect the privacy of an individual's identifiable health information;
  - Applied to protected health information (PHI);
  - Established rights for the health care consumer;
  - Had to be implemented by health care providers, health plans and health care clearinghouses (Covered Entities);
  - Required implementation by Covered Entities of privacy and security standards according to size and resources;
  - Required a Notice of Privacy Practices (NPP) for Covered Entities; and
  - Required a Business Associate Agreement with contractors (e.g., accountants, lawyers, billing company, technology vendors, third-party administrators).

BUSINESS ASSOCIATE AGREEMENTS

- Law firms subcontract with third parties which may include, but are not limited to:
  - Expert witness
  - Auditors
  - Forensic computer experts
  - Investigators
  - Special outside counsel
  - Accountants
  - Consultants

BUSINESS ASSOCIATE AGREEMENTS

- Agreement should include:
  - Description of permitted and required uses of PHI
  - Provision that BA will not use or further disclose other than as permitted or required by contract or law
  - Requirement that BA use appropriate safeguard to prevent inappropriate use or disclosure
  - Use minimum necessary disclosure standards
  - Reporting of suspected or actual disclosure
  - See HHS Sample BA Agreement in materials to be modified for legal services

HIPAA OVERVIEW

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and effective 2003
  - To be "HIPAA compliant", your practice must take steps, implement and strive to be in compliance with all applicable federal, state, local laws and regulations and professional codes and guidelines that pertain to health care businesses and the practice of medicine/healthcare.
  - HIPAA preempts State laws that are not as stringent.

HIPAA OVERVIEW

- American Recovery and Reinvestment Act of 2009 (ARRA)
  - Portion of ARRA - The Health Information Technology for Economic and Clinical Health Act ("HITECH Act")
  - The HITECH Act expanded HIPAA by:
    - Establishing mandatory federal breach reporting requirements for Covered Entities and their Business Associates (BAs);
    - Codifying the previously-proposed Security Rule;
    - Appling HIPAA privacy and security requirements directly to BAs;
    - Creating new privacy requirements, restrictions on disclosures to health plans, changes to minimum necessary standard and accounting through an electronic health record;

HIPAA OVERVIEW

- The HITECH Act expanded HIPAA by:
  - Creating new restrictions on marketing and fundraising;
  - Requiring HHS to conduct additional education on privacy;
  - Prohibiting the sale of PHI without patient consent;
  - Applying HIPAA preemption standards to the new requirements;
  - Instituting new criminal and civil penalties for noncompliance and breach as well as new enforcement responsibilities;
  - Establishing liability of Covered Entities' employees for breach or noncompliance;
  - Identifying electronic risk assessment criteria; and
  - Requiring changes to the Notice of Privacy Practices (NPP).

HIPAA OVERVIEW

- Key Aspects of the 2013 Omnibus Rule
  - Changes as they relate to Business Associates:
    - Revised definition of Business Associates to include eRx, EMR, Cloud and data storage entities
    - Revised terms of new BA Agreements
    - Specifically makes all Business Associates liable for HIPAA violations – Business Associates are responsible for their subcontractors down the line
    - Compliance deadline was September 23, 2013 unless:
      - HIPAA compliant BA Agreement before 1/25/13 and if not renewed or modified between 3/26/13 and 9/23/13.
      - If requirements are met for prior BA Agreements and agreement is not modified or renewed, then the compliance date is September 22, 2014.

HIPAA OVERVIEW

- **Key Aspects of the 2013 Omnibus Rule**
  (The new Omnibus HIPAA HITECH Amendment compliance was due for most providers Sept. 2013, certain providers have until 2014.)
  - **Revised definition of breach;**
  - **Removed the risk of harm standard;**
  - **Eliminated intent to disclose;**
  - **Required evidence to rebut the presumption there was a breach;**
  - **Provided for notification based upon<500 or 500> patients involved;**
  - **Directed Covered Entity to perform and document risk assessment.**
- **Clarification of who Providers can disclose patient information to without consent, unless the patient specifically asked for no disclosure:**
  - **Family members, adult children, close relatives, involved caregivers**
    - **See January 15, 2013 letter from OCR**

HIPAA, HITECH Act, 2013 Omnibus Rule

- **Who and What Is Covered?**
  - **A Covered Entity (CE) is:**
    - **Health care providers**
    - **Health care plans**
    - **Health care clearing houses:**
      - that perform a covered transaction; or
      - that utilize electronic media for any health care information purpose, including making patient notes in a personal or business computer, smart phone, pad, tablet or electronic device

HIPAA, HITECH Act, 2013 Omnibus Rule

- **Who and What Is Covered?**
  - **Any health care information that is:**
    - **Maintained in any media, stored on business or personal computers, smart phones, flash drives, tablets, notepads, and digital device**
    - **Transmitted electronically or digitally**
    - **Written, and**
    - **Communicated orally**

HIPAA, HITECH Act, 2013 Omnibus Rule

- "PHI" Protected Health Information
  - Names
  - All geographical information, including zip code
  - Any and all dates – including admissions, discharge, birthday, date of death
  - Telephone and fax numbers
  - Email addresses
  - Social Security number
  - Medical record identification numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers – including vehicle license plates
  - Biometric identifiers
  - Photographic images
  - Genetic information and testing
  - Bills for medical care (Maryland statute)
  - Any information that relates to the individual's past, present or future physical or mental health condition or payment for health care
  - Any information that can be used to identify the individual

PRACTICE ACTIONS FOR COMPLIANCE

- Risk Assessment
  - Conduct an accurate and thorough assessment of potential risks and vulnerabilities
    - Risk - potential threat or impact on confidentiality, integrity and availability of ePHI
    - Threats – intentional (hackers, spyware authors) or unintentional (e.g., floods, earthquakes, storms, tornados, power surges, accidental deletions, data entry error, accidental transmission, etc.)
    - Vulnerability – flaw or weakness in a system security procedure, design, implementation or control
  - Identify where ePHI is created, maintained, received, processed or transmitted
    - Physical boundaries, remote access, removable media, portable computing devices

PRACTICE ACTIONS FOR COMPLIANCE

- Risk Assessment
  - Inventory assets to be protected – walk through inspection;
  - Identify employees with authorized access;
  - Gather information about conditions under which PHI is created, maintained, received, processed or transmitted and the security controls currently being used to protect the PHI;
  - Identify potential threat sources (e.g., natural disasters, power surges, fire, electrical problems, hackers, unintentional deletions, internet searches, inadvertent data entry, malicious software upload, unauthorized access, etc.);
  - Review current security controls; and
  - Identify where ePHI is created, maintained, received, processed or transmitted.

PRACTICE ACTIONS FOR COMPLIANCE

- **Risk Assessment**
  - Use NIST HIPAA Security Tool Kit – http://scap.nit.gov/hippa
    - Only Federal agencies are required to use NIST Tool Kit
  - Determine the level of potential risk and vulnerabilities;
    - Low, moderate, high risk
  - Recommend security controls
  - Determine mitigation options
    - Security Incident/Breach plan
  - Document risk assessment results
    - Action plan

PRACTICE ACTIONS FOR COMPLIANCE

- **Practical applications of Risk Assessment**
  - Examine infrastructure of work site;
  - Assess integrity of protected information;
  - Identify sensitive information and data;
  - Identify how health information flows throughout the system;
  - Review for legally sufficient consent;
  - Identify individuals or offices with access to PHI information and methods they utilize for confidentiality; and
  - Review former incident reports for related regulatory noncompliance.

PRACTICE ACTIONS FOR COMPLIANCE

- **Practical applications**
  - Determine computer security and file access;
  - Identify security of electronic communications – Electronic Health Records, Email, PDA, Texting, Website; and
  - Identify any current noncompliant individuals or processes.

PRACTICE ACTIONS FOR COMPLIANCE

- Practical applications
  - Create security policies and procedures for your workplace, remote access and devices;
  - Do not leave screens of computer, laptop, PDA, cell phone unattended, unlocked or open to PHI;
  - Limit use, access and disclosure of PHI to minimum necessary;
  - Use and safeguard assigned access codes;
  - Program auto-lock & auto-log out features;
  - Encrypt ePHI (only recommended);
  - Provide for HIPAA compliant back-up of data offsite; and
  - Prohibit access to and downloading of non-authorized data or sites.

PRACTICE ACTIONS FOR COMPLIANCE

- Practical applications
  - Bring Your Own Device (BYOD) policies
  - Destroy, appropriately, hard drive, multi-function machines (copier, fax & scanner), laptops or any data devices containing PHI;
  - Train and educate all staff regularly & as needed;
  - Perform internal audits to monitor office compliance;
  - Provide for levels of discipline for violations of policies and procedures;
  - Consider cyber security insurance; and
  - Encourage a culture of compliance.

HIPAA, HITECH Act, 2013 Omnibus Rule and the Medical Record

- Consequences of breach or violation
  - Civil penalties:
    - $100 - $50,000 per violation (did not know & by exercising reasonable diligence would not have known it violated HIPAA)
    - $1,000 -$50,000 per violation (reasonable cause, not willful neglect)
    - $10,000 - $50,000 per violation (willful neglect that was corrected within 30 days)
    - $50,000- $1.5M per violation (willful neglect not corrected within 30 days)

  Maximum penalty for violation of an identical provision of HIPAA- $50,000 per violation, annual cap $1.5M regardless of penalty tier

HIPAA, HITECH Act, 2013 Omnibus Rule and the Medical Record

- Consequences of breach or violation
  - Criminal penalties
    - Fines - $50,000- $250,000
    - Imprisonment – 1-10 years

HIPAA, HITECH Act, 2013 Omnibus Rule and the Medical Record

- Other potential consequences
  - Loss of employment
  - Professional discipline
  - Harm to professional reputation
  - Loss of Client
  - OIG power to exclude the provider from any Federal healthcare program
  - Enforcement authorities have the power to freeze personal and business assets including bank accounts and any property that was acquired directly or indirectly from the commission of these federal health care offenses and during the investigation
  - Filing a complaint with JCAHO, OCR, HHS, CMS, DOJ, OIG, EEOC, FBI, US Attorney General, or State AG office

PRACTICE ACTIONS FOR COMPLIANCE

- Current compliance challenges
  - Email, texting
  - Social media, Tweets
  - Digital photographs
  - Employee's personal electronic devices
  - Remote access
  - Website searches and search engines
  - Wi-Fi security
  - Cloud storage
  - International intruders
  - Cyber terrorism (worms, viruses, malware)
  - Outsourcing of services
  - Portability of data
  - Integrated information systems
  - Inoperability

HIPAA Includes Compliance with Multiple Federal Statutes and Regulations

- Privacy Rules 76 Fed Reg 53182
- Security Rules 68 Fed Reg 8334
- HITECH Act (Health Information Technology for Economic and Clinical Health Act) American Recovery and Reinvestment Act of 2009 (ARRA) 42 CFR: Parts 412, 413, 422 and 495
- Patient Protection and Affordability Act (ACA) (Healthcare Reform legislation) 42 U.S.C. § 18001 et seq. (2010)
- Public Health Confidentiality of Alcohol and Drug Abuse Patient Records 42 CFR Part 2
- Family Educational Rights and Privacy Act of 1974 (FERPA) 34 CFR Part 99
- E-Prescribing Act of 2005
- Genetic Information Nondiscrimination Act of 2008 (GINA) 74 Fed Reg 51698
- Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the HITECH Act and GINA; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed Reg 5565 (Jan. 25, 2013) (amending 45 CFR parts 160-164.) (HIPAA OMNIBUS RULE)

Resources

- Office of the National Coordinator for Health Information Technology (ONC)
- CMS HIPAA - http://www.cms.gov/Regulations-and-Guidance/HIPAA Administrative Simplification/HIPAAGenInfo/index.html
- Health Information Technology.gov – http://healthit.hhs.gov
- Certification Commission for Health Information Technology – www.cchit.org
- Healthcare Information and Management Systems Society –www.himss.org
- American Health Lawyers Association (AHLA) –www.ahla.org
- Patient Privacy Rights – www.patientprivacyrights.org
- Office of Civil Rights – www.OCR.gov
- American Medical Association – www.ama-assn.org
- Dept. of Health & Human Services – HIT – www.hhs.gov
- American Medical Informatics Association - www.amia.org
- American Health Information Management Association - www.ahima.org
- American Telemedicine Association – www.atmeda.org
- HIPAA Security Series – www.hhs.gov/ocr/privacyhipaa/administrative/securityrule/securityruleguidance.html
- "Lawyers As Business Associates: No Excuse" Apple et al, AHLA Connections, Vol. 18, Issue 6, page 42 (June 2014)

Thank you