Tools to Prepare and Protect Your Practice for HIPAA and Meaningful Use Audits

Presented by: Don Waechter, Managing Partner
Health Compliance Partners
Ann Breitinger, Attorney
Blalock Walters
Legal Disclaimer

- The information included in this presentation is for informational purposes only and is not a substitute for legal advice.
- Please consult your attorney if you have any particular questions regarding a legal issue.
Background

- HIPAA
  - Health Insurance Portability and Accountability Act
  - Enacted 1996
  - Mandates that Covered Entities have appropriate *Administrative, Technical and Physical* safeguards to protect privacy of Protected Health Information
  - Initially Not Enforced = Nominal Compliance
Background

- HITECH Act
  - Health Information Technology for Economic and Clinical Health Act
  - Extends HIPAA to Business Associates
  - Creates Meaningful Use Incentives
  - Office of Civil Rights responsible for enforcement
Background

- Office of Civil Rights
  - Leon Rodriguez named Director in 2011
  - Former prosecuting attorney
  - “Without enforcement there will be no compliance.”
  - Hires KPMG to begin “pilot” audit program in 2012
  - Pilot audit program concludes and findings are assessed in 2013
Office of Civil Rights (cont’d.)

– Pilot Audit Program Findings
  • Practitioners are largely non-compliant
  • Largest area of non-compliance is failure to perform a security risk analysis

– Recommendations
  • Increase number of audits
  • Narrow focus to a few key items including security risk analysis
  • Develop in-house resources to conduct audits
Background

- HIPAA Omnibus Rule
  - Enacted March 2013, Effective October 2013
  - Expands rulemaking authority of CMS
  - Expands enforcement authority of OCR
  - In cases of breach of PHI, shifts burden of proof to providers to show no harm
  - Puts Business Associates on notice that they will now be subject to audits
  - Providers must take reasonable actions to ensure their BA’s are compliant.
Do you see a trend here?

– More rules
– More enforcement
– More fines, penalties
Breaches involving more than 500 individuals in a jurisdiction must be reported to the Office for Civil Rights.

- Tricare breach – class action suit $4.9 Billion
- Affinity Health Plan – fined $1.2 Million for photocopier breach
- Legal costs for determining if a breach must be reported can run into the tens of thousands of dollars ($234 per patient)
Dermatologist fined $150,000 for stolen thumb drive

Fines can be as much as $150,000 per violation with an annual cap of $1,500,000 for violations involving a single requirement

In April, 2010, a physician affiliated with UCLA was sentenced to four months in jail

In April, 2014 audits resumed with 10% - 20% of providers being targeted
Interesting Facts

- Ninety-three percent of healthcare providers incur breaches of PHI
- Average cost of breach
  - Discovered on same day - $8,950
  - Discovered 1+ week later - $115,849
- Between ten and twenty percent of providers will be audited
- For every dollar invested in audits, the government receives an eight dollar return
Action Plan for Protecting Your Practice

- Sufficient legal documents
- Encrypt your data
- Perform a Security Risk Analysis annually
- Document Meaningful Use qualification requirements
All Business Associate Agreements must now be compliant with new HIPAA Omnibus Rules.

- Covered Entity
- Business Associate
- Subcontractor
Health Care Providers must have new Notice of Privacy Protection as of September 23, 2013

- Should post on website
- Display in office
- Make available to new patients and anyone who requests
There are specific uses and disclosures that the patient must authorize through the NPP.

- Fundraising Communications
- Notice of Breach
- Disclosure of PHI to a health plan
- Health plans are required to include a statement in their NPPs that they are prohibited from using or disclosing genetic information of an individual for underwriting purposes
Action Plan – Data Encryption

- Encryption defined
  “The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.”

  Federal Register

- Why is it important?
  “If protected health information is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information.”

  Federal Register

- How? See a *qualified* IT professional
Action Plan – Security Risk Analysis

- Required by law
  A Covered Entity must “implement policies and procedures to prevent, detect, contain, and correct security violations”.
  45 CFR 164.308(a)(1)(i)

  45 CFR 164.308(a)(1)(i)

- Protocols established by the National Institute of Standards and Technology, specifically NIST 800-30 and 800-66
Action Plan - Security Risk Analysis

- Evaluate Administrative, Physical and Technical safeguards through a nine step process
  1. Define scope of analysis
  2. Identify and compile relevant information
  3. Identify realistic threats
  4. Identify potential vulnerabilities
  5. Assess current security controls
  6. Determine likelihood and impact of threat
  7. Determine level of risk
  8. Recommend security controls to reduce risk
  9. Document risk assessment findings
Action Plan – Security Risk Analysis

- Recommendations
  - Perform SRA’s annually
  - Implement recommendations for remediation
  - Maintain a file of annual risk analyses
  - Ensure that you have HIPAA compliant Policies and Procedures, Incident Response Plan, Disaster Recovery Plan, and annual Staff Training in place
“Please see the attached document and submit the requested information….be aware that if the aforementioned Meaningful Use criteria are not met, the incentive payment will be recouped.”

- False attestation is a felony
- Review and document your Meaningful Use qualification criteria
- Seek the advice of a qualified professional
Action Plan - Recap

- Update your legal documents
- Encrypt your data
- Perform a Security Risk Analysis annually
- Document Meaningful Use qualification requirements
Tool Kit – Free Resources


- Sample documents including Business Associate Agreement, Notice of Privacy Practices, and Breach Notification Requirements
  [DWAechter@Healthcompliancepartners.com](mailto:DWAechter@Healthcompliancepartners.com)
Tool Kit – Free Resources

- Encryption
  - DiskCryptor – free hard drive encryption - https://diskcryptor.net/wiki/Main_Page
  - Zix - cloud based email encryption - http://www.zixcorp.com
Tool Kit – Free Resources

- Security Risk Analysis
Tool Kit – Free Resources

- **Meaningful Use**
  - [http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives](http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives)
Contact

- HEALTH COMPLIANCE PARTNERS
  - [http://www.healthcompliancepartners.com](http://www.healthcompliancepartners.com)
  - Don Waechter, Managing Partner
  - 727.366.7796
  - [DWaechter@HealthCompliancePartners.com](mailto:DWaechter@HealthCompliancePartners.com)

- BLALOCK WALTERS
  - [http://www.blalockwalters.com](http://www.blalockwalters.com)
  - Ann Breitinger, Attorney
  - 942.201.2567
  - [ABreitinger@BlalockWalters.com](mailto:ABreitinger@BlalockWalters.com)