PRESENTATION

The HIPAA in the Room:

New Developments in HIPAA and Security Laws

May 16, 2013

Alisa L. Chestler

Of Counsel

Agenda

1. HIPAA – Changes to the Law
2. BYOD
3. Social Media

Still Need the Basics

- Adequate separation between the Plan and HR functions
- Plan Certification
- Plan Document requirements
- Documented Policies and Procedures
- Privacy Officer
- Security Officer
- Training for employees
- Security Risk Analysis
- Business Associate relationships

HIPAA

THEN

- Off the Shelf P & P
- Privacy
- Security

NOW

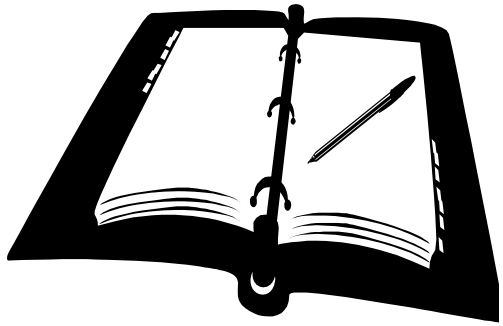
- Customized P & P
- Privacy
- Security
- Compliance Audits
- Data Breaches
- Vendor Assessments

Important Dates - HIPAA

Effective Date: March 26, 2013
Compliance Date: September 2013

Contracts renewed or amended after March 26, 2013 should have new BA language.

For contracts untouched: September 22, 2014



Overview of Omnibus Rule Changes

- Increased tiered monetary penalties & expanded enforcement structure introduced in HITECH
- Business associates directly liable for compliance with most privacy and security rules
- Breach notification change- risk of harm now a risk assessment
- Required changes to NOPP

Changes (continued)

- Strengthens limits on Marketing and Sale of PHI
- Expands rights to electronic copies of DRS
- Solidifies right to restrictions on disclosures to Health Plans if treatment has been paid in full
- GINA – limits on genetic information

Breach Notification

September 2009

- Risk of Harm
  - Likelihood of *significant risk* of financial, reputational or other harm
  - Encryption was a big key factor

January 2013

- Risk Assessment
  - If it can be demonstrated there is a *low probability* the information has been compromised
  - 4 factor assessment in text of Rule
  - Encryption will continue as an important first question

Agency Relationship

- CE (The Plan) is liable for the acts or omissions of its BA acting within the scope of "agency"
- BAs are likewise liable for the acts or omissions of its Subcontractor acting within the scope of "agency"
- Federal common law of agency- contract language may not help
- Knowledge by the agent will be imputed to the principal

Business Associate Agreement Changes

- Must explicitly state BA will comply with privacy and security regulations
- Include notification of breaches of unsecured PHI
- "Create, receive, maintain or transmit"
- Subcontractor arrangements
- Carry out privacy requirements

NOPP Changes

- Right to receive breach notification
- Prohibition on the use of genetic information for underwriting purposes
- Authorization requirements, description of types of uses and disclosures requiring an authorization

BYOD: Bring Your Own Device

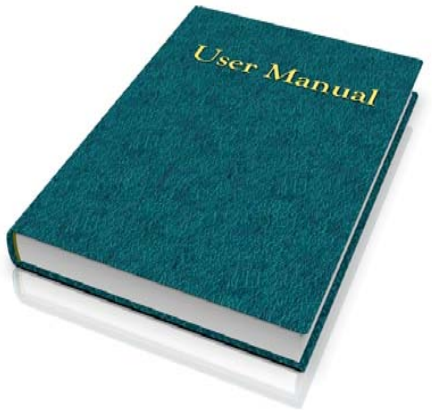
- What is on your device now?
- Single Biggest Threat to HR Departments today
- Expand this consideration to your entire company
- Control issues

BYOD: Legal Risks

- Privacy
- Security
- Discoverability
- Tax Implications
- End Game (Termination)

BYOD: User Guidelines & Training

- Must have User Guidelines in writing
- Train employees
- Registration of devices that require 1+2 above



BYOD: User Guidelines

- Scope
- Device Registration
- Corporate Expectations
- Privacy
- Costs

Social Media

- Need to have a policy – current employees
- What about prospective employees
- Facebook, Instagram, SnapChat, Twitter

16

Questions??

Alisa Chestler

Baker, Donelson, Bearman, Caldwell & Berkowitz
920 Massachusetts Avenue, NW
Washington, DC 20001
202.508.3475

achestler@bakerdonelson.com

Twitter: @alchestler