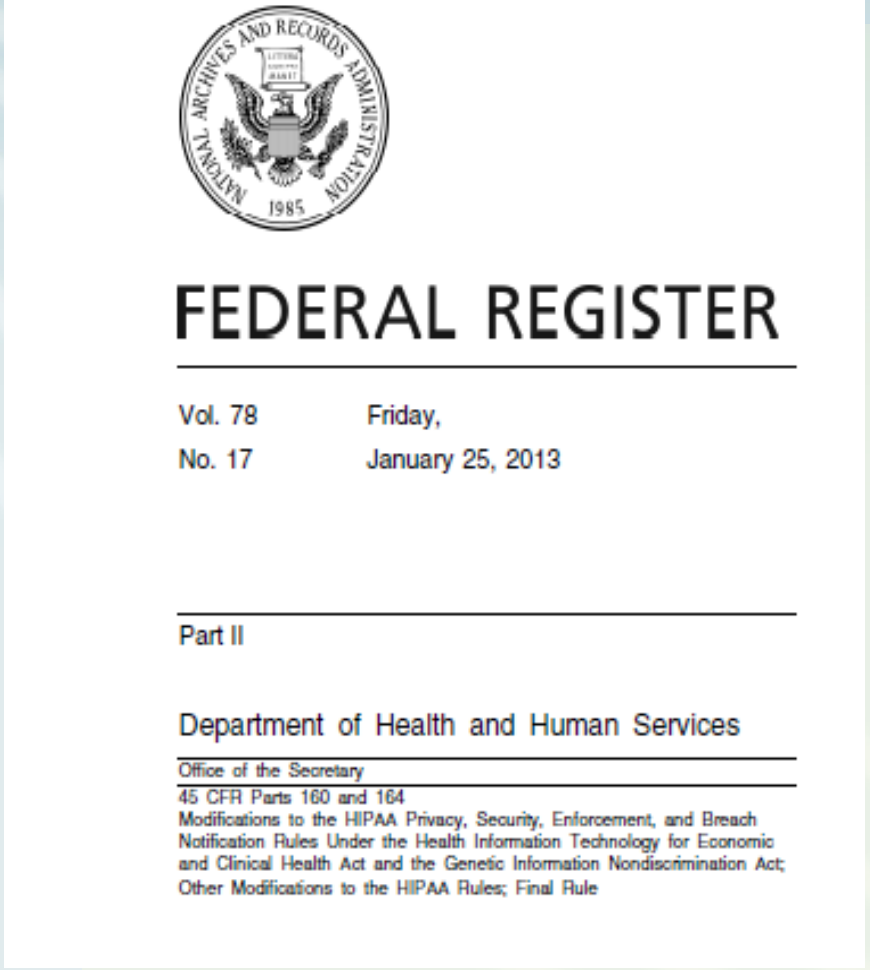
Modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules (Omnibus Rule)

Karin Bierstein, JD, MPH

February 27, 2013

ANESTHESIA
BUSINESS CONSULTANTS



FEDERAL REGISTER

Vol. 78 Friday,
No. 17 January 25, 2013

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 and 164
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

"The most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented"

ANESTHESIA
BUSINESS CONSULTANTS

4 Final Rules, Actually

1. Modifications to the HIPAA Privacy, Security & Enforcement Rules mandated by the HITECH Act
2. Breach Notification for Unsecured Protected Health Information (PHI)
3. HIPAA Enforcement Rule (HITECH)
4. Modifications to Privacy Rules as required by the Genetic Information Nondiscrimination Act (GINA)

ANESTHESIA
BUSINESS CONSULTANTS

To Do List for Anesthesiologists & Pain Physicians

- Privacy, Security and Breach Notification policies and procedures
- Notice of Privacy Practices
- Business Associate Agreements
- *Update and train*

ANESTHESIA
BUSINESS CONSULTANTS

I. Breach of PHI

- The problem:
  - 538 large breaches of PHI affecting over 21.4 million patient records (2009-2012)
  - 66%: theft or loss
  - 38% unencrypted laptops and other portable devices
  - 57% involve a business associate

ANESTHESIA
BUSINESS CONSULTANTS

Breach of PHI cont'd

- 96% of all health care organizations surveyed (n=72) had had at least 1 breach in past two years.
- But only 49% did anything to protect mobile devices
- And only 23% use encryption

Second Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute, December 2011

ANESTHESIA
BUSINESS CONSULTANTS

Breach Cont'd

- Breach = *acquisition, access, use or disclosure* of unsecured PHI not permitted by HIPAA
  - Unsecured = not secured through approved methodology that renders the PHI *unusable, unreadable or indecipherable to unauthorized individuals* (encryption, de-identification, destruction)
- Any form or medium (electronic, paper or oral)

ANESTHESIA
BUSINESS CONSULTANTS

6th Breach Notification

ANESTHESIA
BUSINESS CONSULTANTS

Breach Notification Requirements

CEs must report breach *unless after 4-factor risk analysis* there is a low probability of PHI compromise.

This is a rebuttable presumption, replacing prior subjective standard of "significant risk of financial, reputational or other harm"

ANESTHESIA
BUSINESS CONSULTANTS

Breach Notification Risk Analysis

- *How great was the risk of PHI compromise?*
- Four factors:
  - Nature and extent of PHI involved
  - Unauthorized user or recipient of PHI
  - Whether PHI was actually acquired or viewed
  - Extent to which risk to PHI was mitigated

ANESTHESIA
BUSINESS CONSULTANTS

Alternative to Risk Analysis

- Notify affected individuals of the breach
  - In writing, by mail or e-mail if preferred
  - Additionally by phone if urgent
  - Substitute methods if no contact info
- Without unreasonable delay and not more than 60 days from discovery

ANESTHESIA
BUSINESS CONSULTANTS

More than 500 Individuals Affected by Breach

- Notify major media outlets (60 days)
- Notify Secretary of HHS simultaneously
- If fewer than 500, maintain log of breaches and submit annually to HHS

ANESTHESIA
BUSINESS CONSULTANTS

Contents of Breach Notification

- Description of incident and dates
- Types of PHI disclosed
  - Name, SSN, DOB, home address, Dx, etc.
- Steps patients should take to protect themselves (e.g. notify credit card issuers)
- Actions taken by practice to investigate and mitigate
- Contact numbers for patients to ask questions

ANESTHESIA
BUSINESS CONSULTANTS

To Do: Update Policies and Procedures

- Passwords & other controls for laptops, smartphones, paper PHI

- HIPAA compliance program should address risk analysis for suspected breach
- Train staff on notification procedures
- List sanctions for staff who violate notification requirements

ANESTHESIA
BUSINESS CONSULTANTS

II. Notice of Privacy Practices (NPP)

- Revise NPP to include new Privacy and Security Rules / Post & make available
  - Breach notification
  - Physicians now required to honor patient requests to restrict disclosures to health plan for treatment paid out of pocket
    - *Consider necessary changes to workflow*
  - Copies of ePHI
    - 30 days to respond + 1 extension
    - Electronic format requested if "readily available"

ANESTHESIA
BUSINESS CONSULTANTS

NPP cont'd

- Copies of ePHI requested by patients
  - 30 days to respond + one extension
  - Electronic format requested if "readily available; otherwise mutually agreed
  - Charges may include labor costs and portable media (state limits may be lower)
  - E-mailing PHI: unencrypted only if patient is advised of risk

ANESTHESIA
BUSINESS CONSULTANTS

NPP cont'd

- Limit marketing to patients: unless written authorization, only:
  - Physician receives no compensation;
  - Communication is face-to-face;
  - Communication involves current Rx;
  - General health promotion; or
  - Government-sponsored programs.
  - OK to give drug samples.

ANESTHESIA
BUSINESS CONSULTANTS

NPP Cont'd

- Prohibit sale of PHI w/o written authorization
- Decedents' PHI:
  - May disclose to caregivers unless known preference to the contrary
  - HIPAA only protects PHI for 50 years after death
- Limits on fundraising (opt-out)
- Childhood immunizations: physicians may disclose to schools

ANESTHESIA
BUSINESS CONSULTANTS

III. Business Associates (BAs)

- Entities that create, receive, *maintain* or transmit PHI on behalf of the BA are *directly liable*
- Must fully comply with HIPAA
- BA status arises from definition even if no written agreement
- Subcontractors

ANESTHESIA
BUSINESS CONSULTANTS

BAs Cont'd

- List now includes:
  - Patient Safety Organizations (AQI)
  - "Health information exchanges" e.g. e-prescribing gateways
  - Personal health record vendors if sponsored by physician
  - Data transmission services with routine access to PHI (further guidance coming)
    - Conduit exception – "transient vs. persistent" opportunity to access PHI

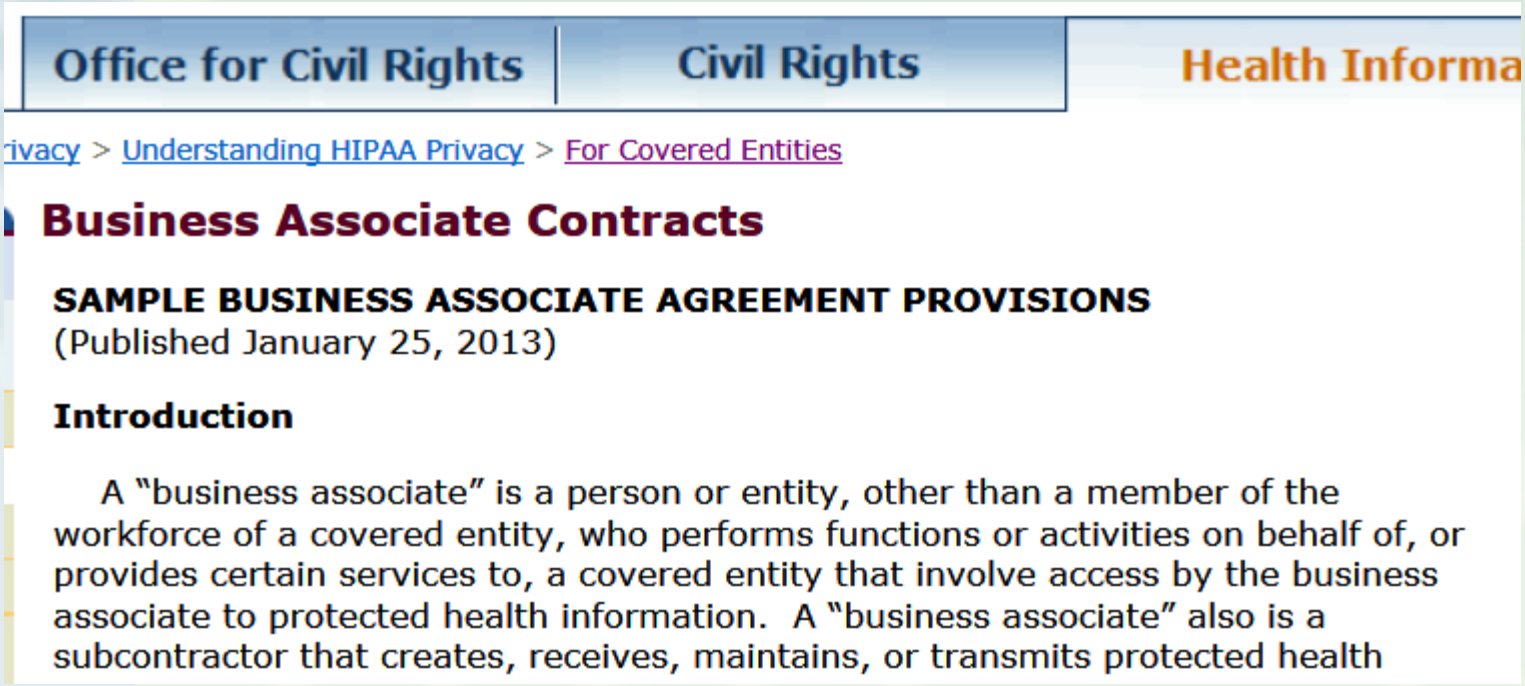
ANESTHESIA
BUSINESS CONSULTANTS

BA Agreements – To Do List

- Review relationships to see whether new BA Agreements are necessary
- Modify existing BA Agreements
  - BAs are liable for the authorized acts of their subcontractors who are *agents*
  - BAs must comply with Security and Breach Notification Rules
    - Spell out respective responsibilities/costs in case of breach by BA
  - Practices no longer have to report failures of their BAs since BAs are directly liable

ANESTHESIA
BUSINESS CONSULTANTS

BA Agreements Cont'd



Office for Civil Rights | Civil Rights | Health Informa

rivacy > Understanding HIPAA Privacy > For Covered Entities

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

ANESTHESIA
BUSINESS CONSULTANTS

IV. Deadlines

- Effective date March 26 + 180 days =

  September 23, 2013

- BAs: 1 year to renew / modify existing agreements =

  September 24, 2014

ANESTHESIA
BUSINESS CONSULTANTS

V. HIPAA Enforcement Rule

Level of Culpability	Each Violation	Maximum in Calendar Year for Identical Violations
Did not know	$100-$50,000	$1,500,000
Reasonable cause	$1,000-$50,000	$1,500,000
Willful neglect—corrected	$10,000-$50,000	$1,500,000
Willful neglect—not corrected	$50,000	$1,500,000

ANESTHESIA
BUSINESS CONSULTANTS

HIPAA Enforcement Cont'd

- HHS must conduct formal investigation for "willful neglect"
- Broad discretion. Factors:
  - Nature / extent of violation
  - Nature / extent of resulting harm
  - History / extent of prior compliance
  - Financial condition of the CE or BA
  - "Such other factors as justice may require"

ANESTHESIA
BUSINESS CONSULTANTS

Last Words

Always check State privacy laws too – if they are stricter, they generally control

Karin.Bierstein@AnesthesiaLLC.com

ANESTHESIA
BUSINESS CONSULTANTS