Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The Basics for Beginning HIPAA Privacy Professionals

February 5, 2014

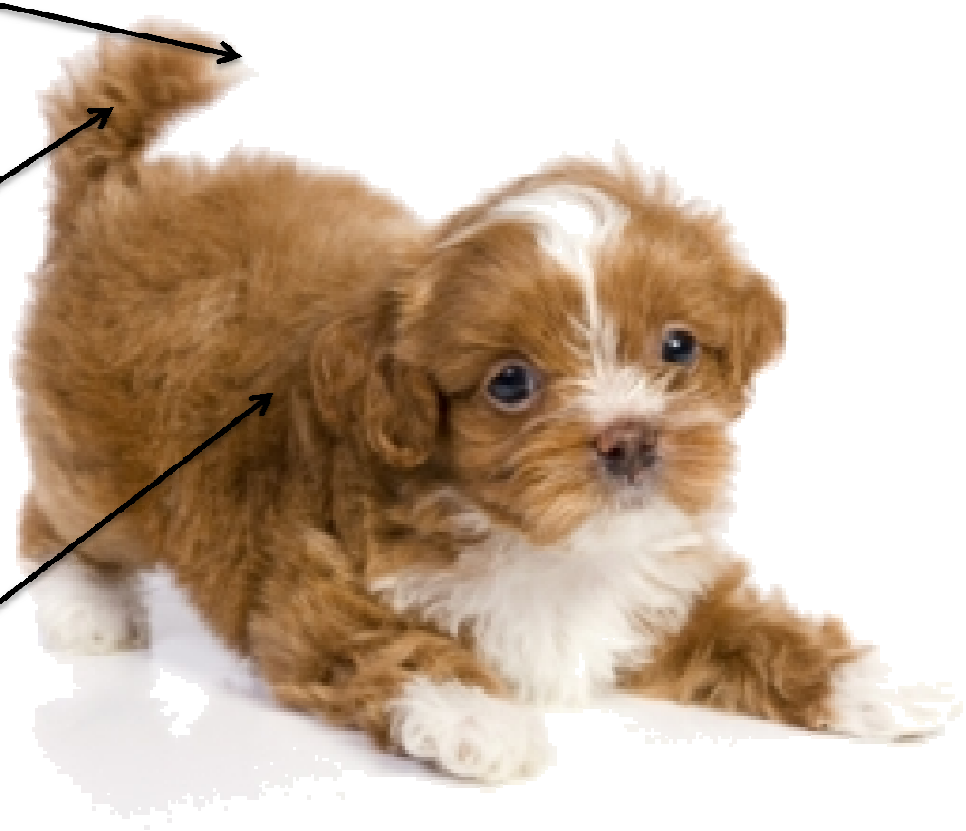
Adam H. Greene, JD, MPH
Partner, Davis Wright Tremaine LLP

HIPAA Privacy & Security Standards

Privacy and Security Standards

Administrative Simplification Subtitle

Health Insurance Portability and Accountability Act of 1996



Who's Covered?

- Covered Entities
  - Health care provider who electronically conducts a covered transaction (e.g., electronically bills insurers)
  - Health plan
  - Health care clearinghouse (converts transaction from standard to non-standard or vice versa)
- Business Associates

Who Is a Business Associate?

Person/entity that:

- Creates, receives, maintains, or transmits
- Protected health information
- On a covered entity's (or another business associate's) behalf

Protected Health Information

Protected Health Information = Individually Identifiable + Health Information, except:

- Records covered by (or treatment records excluded by) Family Educational Rights and Privacy Act (FERPA)
- Employment records held by a covered entity in its role as an employer
- Regarding person who has been deceased for > 50 years

Protected Health Information

- Health information:
  - Relates to the past, present, or future physical or mental health or condition of an individual;
  - Provision of health care to an individual; or
  - Past, present, or future payment for the provision of health care to an individual
- Individually identifiable unless:
  - Expert determines very small risk of identifiability; or
  - 18 identifiers removed (including dates related to individual (other than year), zip codes and smaller, any unique identifiers)

The Privacy Rule

Limits on Uses and Disclosures

Individual Privacy Rights

Administrative Requirements

Limits on Use and Disclosure

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

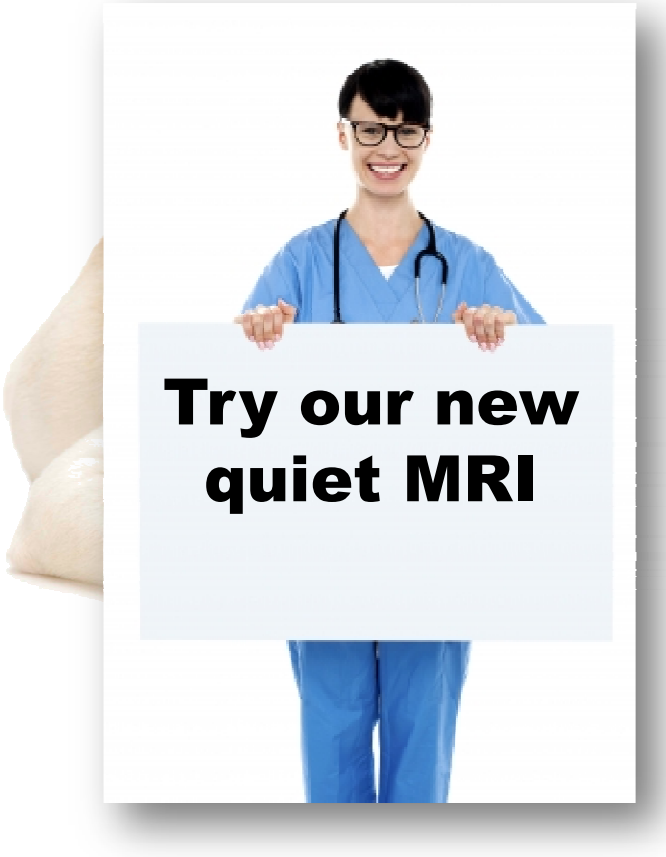
Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Permitted Uses and Disclosures

1. Without authorization
   - Treatment, payment, health care operations
   - Public policy purposes (required by law, law enforcement, judicial proceeding, research, public health, imminent danger)
2. Opportunity to object
   - Facility directory
   - Persons involved in care/payment
3. Limited data set and data use agreement
   - Research, public health, health care operations
4. Authorization

Special Authorization Requirements

- Sale of PHI
  - Includes financial and nonfinancial remuneration
- Marketing
  - Financial remuneration
- Psychotherapy notes
  - Requires separate authorization

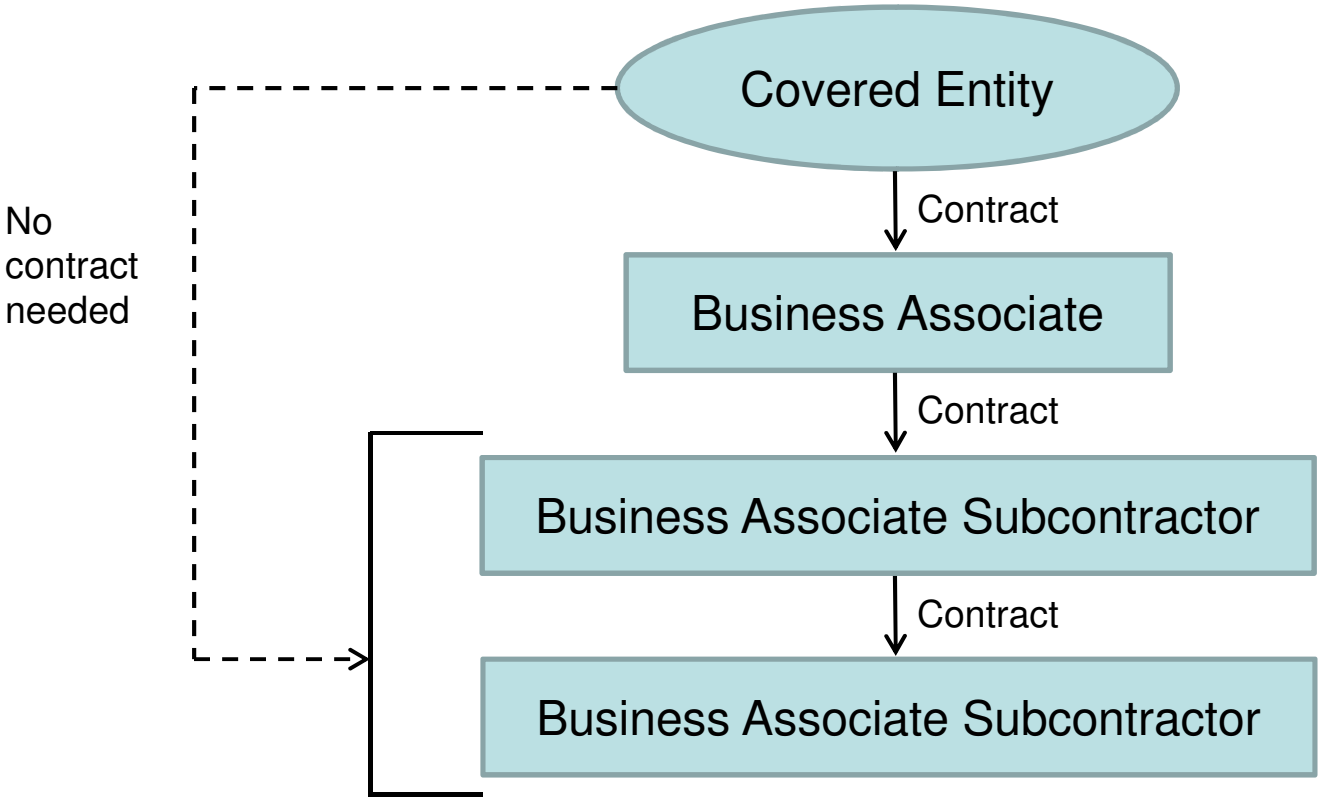


Limits on Use and Disclosure

Minimum Necessary Standard

- Uses – Limit people who have access to PHI, and amount of PHI accessible
- Disclosures – Limit amount of PHI disclosed
  - HIPAA requires policies (e.g., protocols) for routine disclosures
  - HIPAA requires criteria for non-routine disclosures
  - Can reasonably rely on covered entity's request
- Requests – Limit amount of PHI requested
  - HIPAA requires policies (e.g., protocols) for routine requests
  - HIPAA requires criteria for non-routine requests

Business Associate Contracting



Each contract in the chain must be at least as restrictive as the contract above it with respect to uses and disclosures.

Individual Privacy Rights

- Notice of privacy practices
- Right to request restriction (including related to out-of-pocket payments)
- Right to alternative form of communication
- Right of access (designated record set)
  - Medical record, billing records, other records used to make decisions about the individual
- Right of amendment (designated record set)
- Right to accounting of disclosures

Administrative Requirements

- Privacy officer
- Training
- Safeguards
- Complaint process
- Sanctions

Administrative Requirements

- Mitigation
- Refraining from retaliation
- No waivers of rights allowed
- Policies and procedures
- Documentation

BA Requirements

- Limit uses and disclosures of PHI
  - Pursuant to HIPAA
  - Pursuant to business associate agreement
- Use appropriate safeguards (hard copy and verbal)
- Comply with the Security Rule
- Report impermissible uses and disclosures
- Report security incidents
- Report breaches of unsecured PHI

Blue indicates contractual obligation only.

BA Requirements

- Pass on obligations to subcontractor BAs
- Provide e-copy of electronic designated record set
- Provide hard or e-copy of hard copy designated record set
- Incorporate amendments to designated record set
- Provide an accounting of disclosures
- Delegation of Privacy Rule obligation
- Cooperate with HHS investigation
- Return or destroy PHI at termination

Blue indicates contractual obligation only.

Other HIPAA Requirements

- Breach Notification
  - BA to CE
  - CE to individuals, HHS, and (sometimes) media
- Security Rule
  - Administrative, physical, and technical safeguards
  - Risk analysis and risk management process
- Transactions Rule and Code Sets (ICD-10)
- Identifiers

Civil Penalties

- HHS:
  - $100 to $50,000 or more per violation
  - Up to $1.5 million per calendar year for all violations of an identical provision
  - Limits are per type of violation, e.g., four types of continuous violations over three years can equal $18 million

Civil Penalties

- State attorneys general:
  - Up to $100 per violation
  - Up to $25,000 per calendar year for all violations of an identical provision
  - Attorneys' fees
- Likely to combine with charges under state law
- May not adhere to HHS guidance

Criminal Penalties

- Department of Justice (knowingly obtaining or disclosing PHI in violation of HIPAA):
  - $50,000 and/or up to one year imprisonment
  - $100,000 and/or up to five years imprisonment if false pretenses
  - $250,000 and/or up to ten years imprisonment if commercial advantage, personal gain, or malicious harm

Questions