Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

HIPAA Privacy Basics

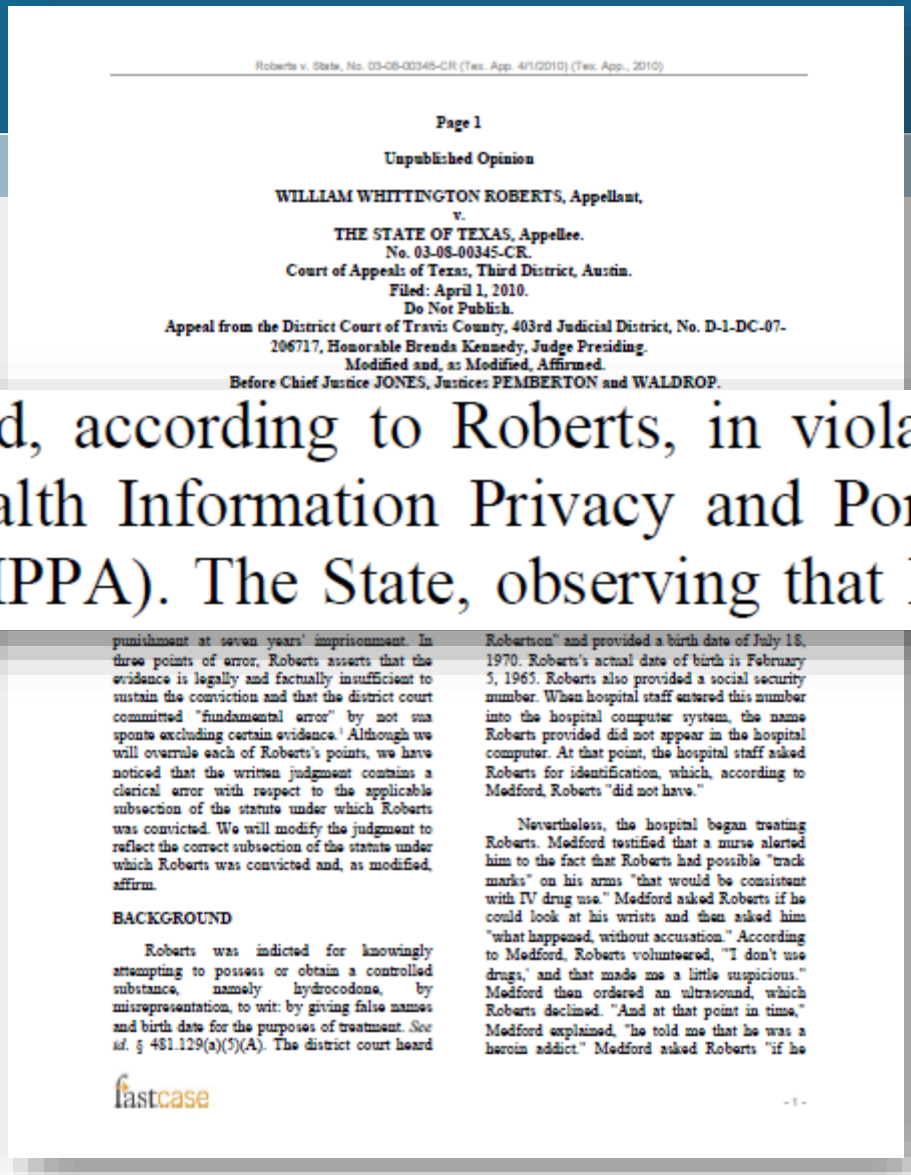
HIPAA Summit
March 4, 2019

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

Agenda

- Some relevant HIPAA history
- Key concepts
- Limits on Uses and Disclosures
- Individual Privacy Rights
- Administrative Requirements

SOME RELEVANT HIPAA HISTORY



Roberts v. State, No. 03-08-00345-CR (Tex. App. 4/1/2010) (Tex. App., 2010)

Page 1

Unpublished Opinion

WILLIAM WHITTINGTON ROBERTS, Appellant,
v.
THE STATE OF TEXAS, Appellee.
No. 03-08-00345-CR.
Court of Appeals of Texas, Third District, Austin.
Filed: April 1, 2010.
Do Not Publish.
Appeal from the District Court of Travis County, 403rd Judicial District, No. D-1-DC-07-206717, Honorable Brenda Kennedy, Judge Presiding.
Modified and, as Modified, Affirmed.
Before Chief Justice JONES, Justices PEMBERTON and WALDROP.

obtained, according to Roberts, in violation of the Health Information Privacy and Portability Act (HIPPA). The State, observing that Roberts

punishment at seven years' imprisonment. In three points of error, Roberts asserts that the evidence is legally and factually insufficient to sustain the conviction and that the district court committed "fundamental error" by not sua sponte excluding certain evidence.[1] Although we will overrule each of Roberts's points, we have noticed that the written judgment contains a clerical error with respect to the applicable subsection of the statute under which Roberts was convicted. We will modify the judgment to reflect the correct subsection of the statute under which Roberts was convicted and, as modified, affirm.

BACKGROUND

Roberts was indicted for knowingly attempting to possess or obtain a controlled substance, namely hydrocodone, by misrepresentation, to wit: by giving false names and birth date for the purposes of treatment. *See id.* § 481.129(a)(5)(A). The district court heard

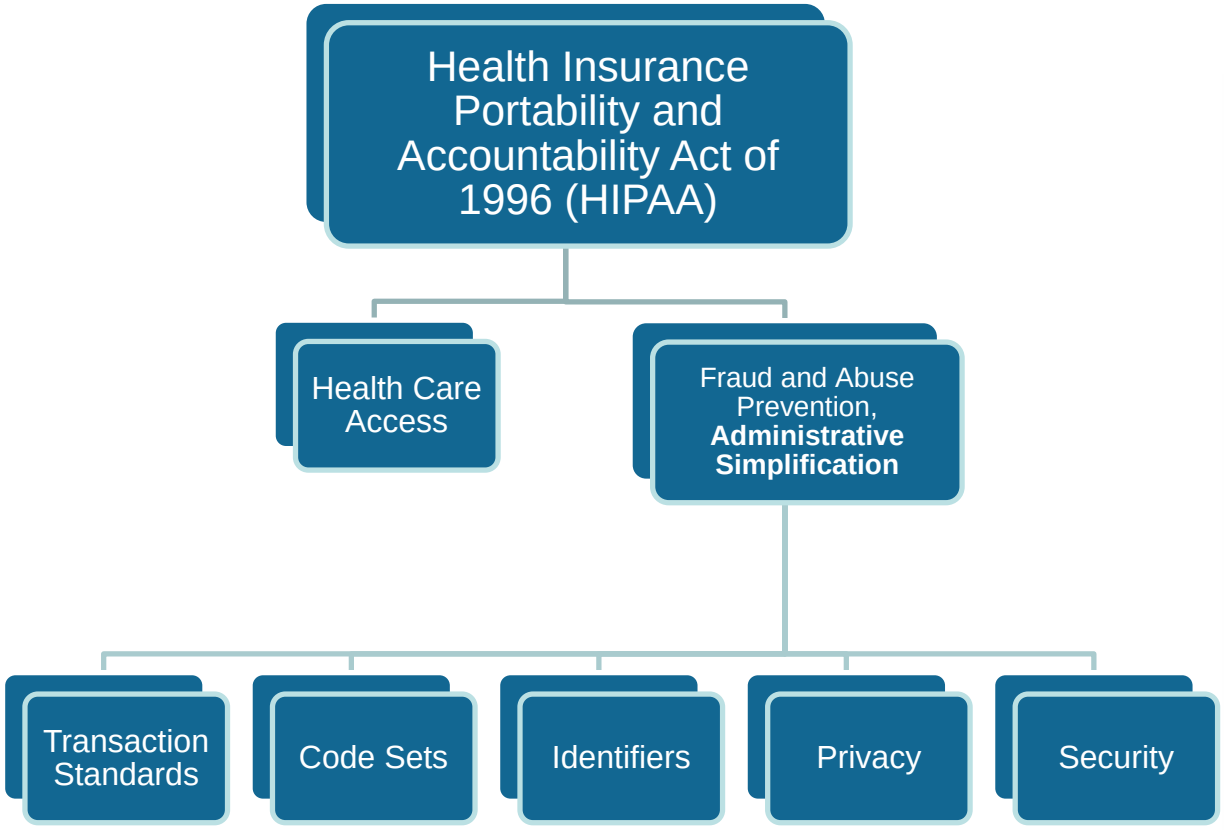
Robertson" and provided a birth date of July 18, 1970. Roberts's actual date of birth is February 5, 1965. Roberts also provided a social security number. When hospital staff entered this number into the hospital computer system, the name Roberts provided did not appear in the hospital computer. At that point, the hospital staff asked Roberts for identification, which, according to Medford, Roberts "did not have."

Nevertheless, the hospital began treating Roberts. Medford testified that a nurse alerted him to the fact that Roberts had possible "track marks" on his arms "that would be consistent with IV drug use." Medford asked Roberts if he could look at his wrists and then asked him "what happened, without accusation." According to Medford, Roberts volunteered, "I don't use drugs,' and that made me a little suspicious." Medford then ordered an ultrasound, which Roberts declined. "And at that point in time," Medford explained, "he told me that he was a heroin addict." Medford asked Roberts "if he

fastcase

- 1 -

The Role of Privacy & Security in HIPAA



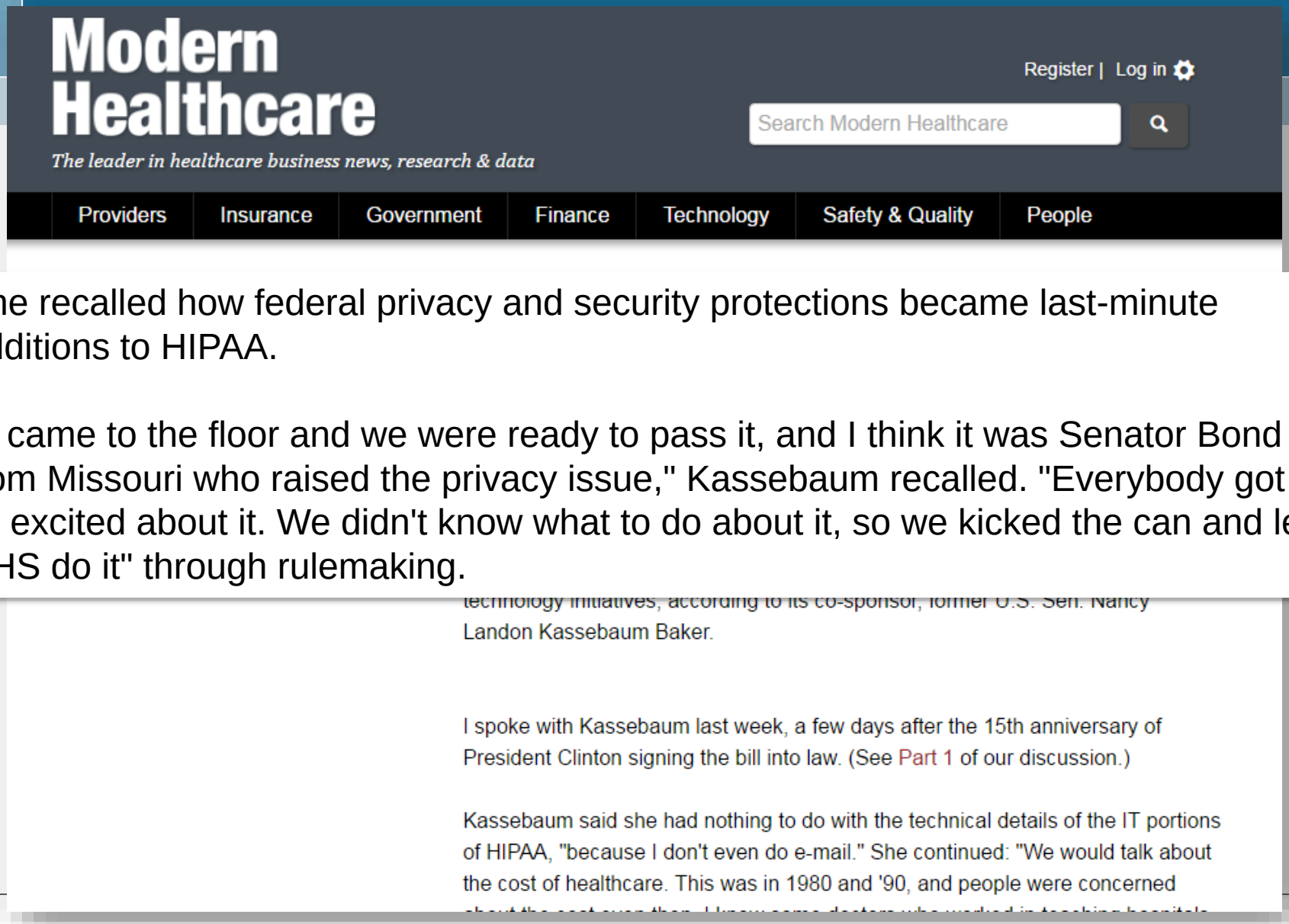
Why HIPAA was enacted…

Provider 5432025
Ptname#Ptaddress#HCIN → Medicare

Provider x943253
HCIN#MDname#Ptname → Medicaid MD

Provider 665b43254
PtSSN#Ptname#HCIN → Medicaid VA

Provider 232x6546545
Mdname#Mdaddress#HCIN → Insurer 1



She recalled how federal privacy and security protections became last-minute additions to HIPAA.

"It came to the floor and we were ready to pass it, and I think it was Senator Bond from Missouri who raised the privacy issue," Kassebaum recalled. "Everybody got all excited about it. We didn't know what to do about it, so we kicked the can and let HHS do it" through rulemaking.

technology initiatives, according to its co-sponsor, former U.S. Sen. Nancy Landon Kassebaum Baker.

I spoke with Kassebaum last week, a few days after the 15th anniversary of President Clinton signing the bill into law. (See Part 1 of our discussion.)

Kassebaum said she had nothing to do with the technical details of the IT portions of HIPAA, "because I don't even do e-mail." She continued: "We would talk about the cost of healthcare. This was in 1980 and '90, and people were concerned

KEY CONCEPTS

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)

Protected Health Information

[P]rotected health information created, received, maintained, or transmitted by a business associate may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, ….

The Privacy Rule

Limits on Uses and Disclosures

Individual Privacy Rights

Administrative Requirements

LIMITS ON USES AND DISCLOSURES

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.

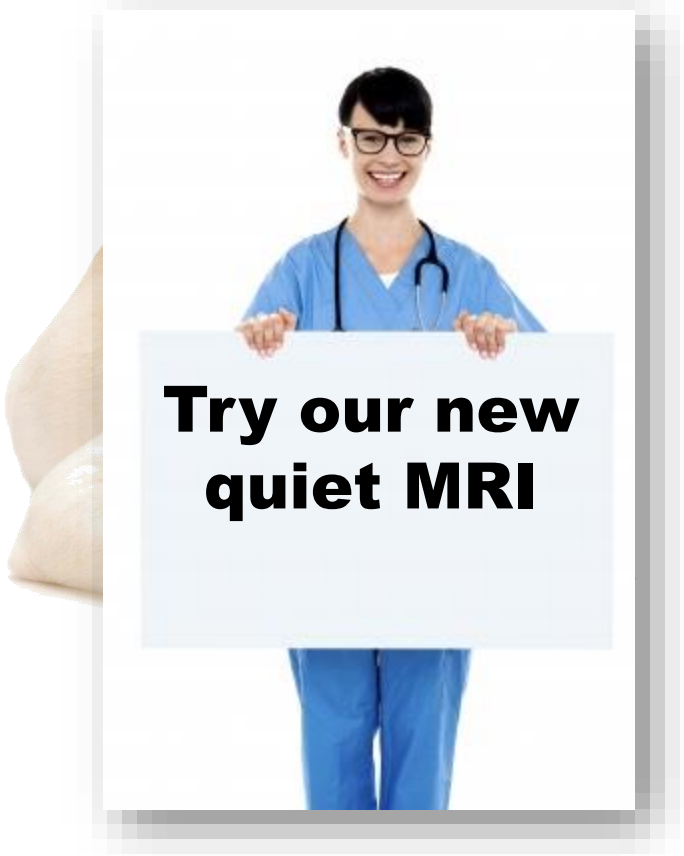
Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

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

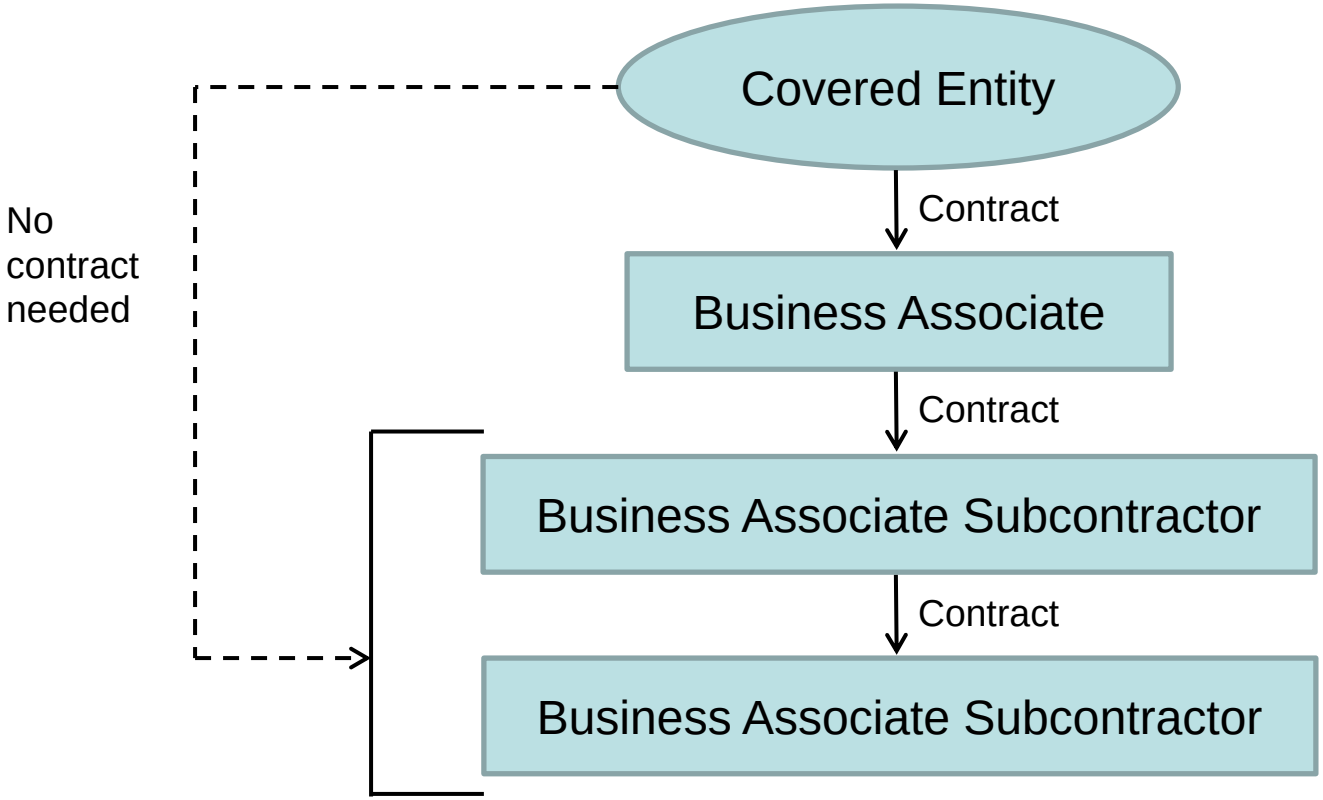


Limits on Use and Disclosure

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.

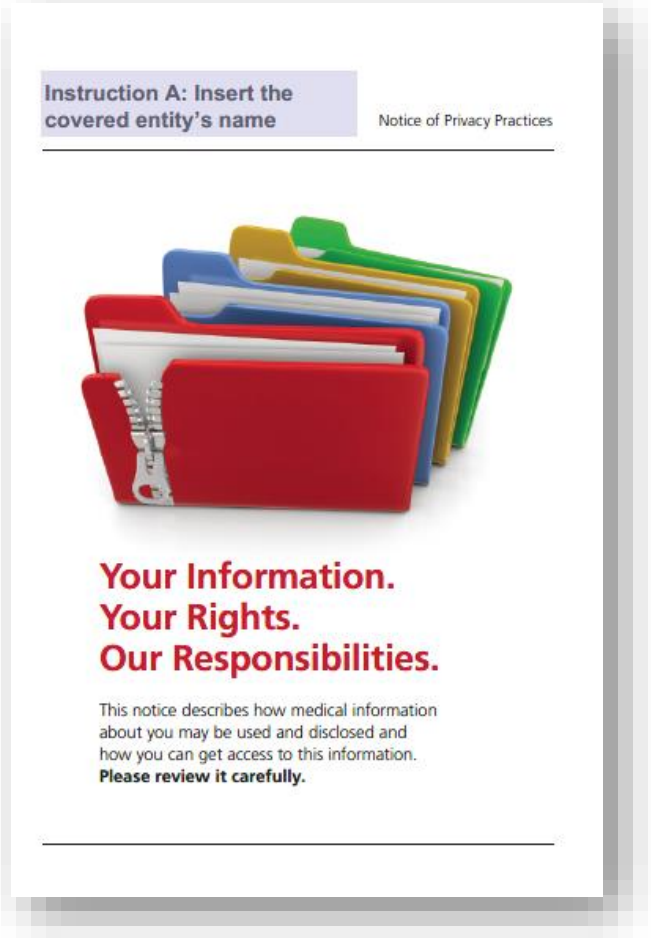
INDIVIDUAL PRIVACY RIGHTS

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

Notice of Privacy Practices

- Specific content requirements
- Specific distribution requirements
  - Posting
  - Copies to new patients
  - Acknowledgment of receipt
  - Website



Restriction Requests

- Right to request restriction
  - Patient can request restriction on certain uses and disclosures (e.g., “please don’t tell my primary care physician”)
  - Covered entity generally can deny any request.
  - Genarlly must accept request to restrict disclosure to health plan for health care services paid out of pocket

Alternative Form of Communication

- Right to alternative form of communication
  - Provider must accommodate reasonable requests (e.g., “please call my work number” or “do not leave a voicemail”)
  - Plan only must accept where disclosure could endanger the individual.

Rights of Access and Amendment

- Right of Access
  - Applies to “designated record set”
  - Must respond within 30 days (30-day extension available)
  - Individual’s preferred form and format, if readily producible
  - Limited to reasonable, cost-based charge
- Right of Amendment
  - Amend if amendment is accurate
  - If disagree with the amendment, individual can have the disagreement reflected in the record

Accounting of Disclosures

- Listing of disclosures for up to six years
  - Does not include internal uses
  - Does not include treatment, payment, health care operations, to individual, or pursuant to authorization
  - Does include impermissible disclosures, required by law, public health, law enforcement, etc.
- Applies to covered entities and business associates
- High burden to track, rarely requested

ADMINISTRATIVE REQUIREMENTS

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.

Questions

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213