Everything You Wanted To Know About The HIPAA Privacy Rule *But Were Too Afraid To Ask

HIPAA COW 2022 SPRING CONFERENCE
APRIL 22, 2022
SCOTT LEBLANC & KELSEY TOLEDO

HUSCH BLACKWELL

1

Everyone's an expert…

Image courtesy: @badhippa

HUSCH BLACKWELL

2

Everyone's an expert…

Image courtesy: @badhippa

HUSCH BLACKWELL

3

Everyone's an expert…

Image courtesy: @badhippa

4

Everyone's an expert…

Image courtesy: @badhippa

5

Don't do a HIPPA

6

The Basics – What's the Point?

- **What is HIPAA?**
  - A federal law that protects certain health information about individuals (**Protected Health Information** or "**PHI**").
  - Sets a minimum level of protection (state law may afford greater protection).
  - Restricts how PHI can be used and disclosed.
  - Gives patients greater access and control over their medical records and information about who has seen them.

HUSCH BLACKWELL

7

The Basics – The Rules

- **HIPAA Privacy Rule (45 CFR 160, 164.100s, and 164.500s):**
  - Covers when PHI may be shared and when PHI may not be shared.
  - Addresses whether patient authorization is required in order to use or disclose PHI.
  - Requires implementation of administrative policies and procedures to protect the confidentiality of PHI
- **Other important HIPAA Rules:**
  - **HIPAA Security Rule (45 CFR 164.300s)**
  - **Breach Notification Rules (45 CFR 164.400s)**

HUSCH BLACKWELL

8

The Basics - PHI

- **What is PHI?**
  - Information that relates to past, present, or future:
    - Physical or mental health or condition of an individual;
    - Provision of health care to an individual; or
    - Payment for health care.
  - To be protected under HIPAA, must be identifiable.

HUSCH BLACKWELL

9

The Basics - Coverage

- **When does HIPAA apply?**
  - ➢When PHI is involved; and
  - ➢When the individual or entity involved is:
    - A "**Covered Entity**";
    - A "**Business Associate**" of a Covered Entity; or
    - The "**Subcontractor Business Associate**" of a Business Associate or Subcontractor Business Associate.

HUSCH BLACKWELL

10

The Basics – Covered Entities

- **What is a Covered Entity?**
  - ➢ A "**health care provider**"
    - Includes (amongst others):
      - Hospitals
      - Doctors
      - Clinics
      - Nursing Homes
      - Pharmacies
      - Certain medical device manufacturers
    - The term "health care provider" also refers to all employees of the health care provider.
    - Must engage in "covered transactions" i.e. billing insurance
  - ➢ A "**health plan**"
    - Group health plans
    - Health insurance issuer
    - HMOs
    - Certain government payor programs
  - ➢ A "**health care clearinghouse**"
    - Companies that translate health claims and billing information

HUSCH BLACKWELL

11

The Basics - Business Associates

- **What is a Business Associate?**
  - ➢ A person or entity which receives or has access to PHI from a covered entity in order to perform certain services for or on behalf of that covered entity.
  - ➢ Business Associate services include:
    - Accounting
    - Billing
    - Coding
    - Consulting
    - IT
    - Legal
  - ➢ Don't be fooled: not all recipients of PHI are Business Associates!

HUSCH BLACKWELL

12

The Basics of the Privacy Rule

- **What is the basic tenet of the Privacy Rule?**
  - "A covered entity may not use or disclose an individual's protected health information, except as otherwise permitted or required."

13

The Basics of the Privacy Rule

- **A corollary to the basic tenet – the Minimum Necessary Rule:**
  - "Covered entities and business associates must take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose, unless an exception applies."
  - Exceptions:
    - Disclosures to or requests by a health care provider for treatment purposes
    - Disclosures to the individual who is the subject of the PHI
    - Uses or disclosures made pursuant to an individual's authorization
    - Uses or disclosures required for compliance with the Simplification Rules
    - Disclosures to HHS when disclosure is required under the Privacy Rule for enforcement purposes
    - Uses or disclosures that are required by other law

14

Permitted Uses and Disclosures

- **Who may authorize the use or disclosure of protected health information under HIPAA?**
  - Individuals and Personal Representatives
- **When may a covered entity use or disclose PHI under HIPAA without authorization?**
  - Treatment, Payment, Operations
  - Business Associate Arrangements
  - Uses and disclosures for which authorization or opportunity to agree or object is not required
    - Required by law
    - For public health activities
    - Victims of abuse, neglect or domestic violence
    - For law enforcement purposes
    - For judicial and administrative proceedings
    - To avert a serious threat to health or safety

15

Individual Rights

- **What are an individual's rights under HIPAA?**
  - HIPAA objective: Maximize protection of PHI, while promoting individual access to PHI
    - Access/Right to restrict access
    - Amendment
    - Accounting
- **How are individuals informed of their rights regarding the use and disclosure of their protected health information?**
  - Covered Entity's Notice of Privacy Practices

HUSCH BLACKWELL

16

Individual Access

- **Right to Access**
  - Individuals have the right to their own PHI, subject to certain exceptions
  - Form of access
  - Scope of access
  - Timing of access
    - No later than 30 days
    - HIPAA Proposed Rule: provide access "as soon as practicable," but in no case later than 15 calendar days after receipt of the request, with the possibility of one 15 calendar-day extension.
    - Information blocking
- **Minimum Necessary Requirement not applicable**
- **Authorization is not required**

HUSCH BLACKWELL

17

HIPAA & Information Blocking

- **Information Blocking Generally**
  - A practice that, ***except as required by law or covered by an exception*, is likely to interfere with access, exchange, or use of electronic health information (EHI),** which includes electronic PHI, and the Actor has actual knowledge, or in the case of Actors who are health IT developers, HINs or HIEs, should know, that the practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.
  - Applies to ***requests*** for EHI
- **What about HIPAA?**
  - Where disclosure or the requirements facilitating disclosure are permissive under HIPAA, Information Blocking now requires disclosure of EHI
  - Overlap between Information Blocking exceptions and HIPAA rules

HUSCH BLACKWELL

18

HIPAA Authorization

- **Who has authority to authorize?**
  - Patients, guardians, persons holding durable POA, executors and administrators of estates
- **What does an authorization do?**
  - Allows a covered entity to share PHI with a third party
- **Requirements for valid HIPAA Authorization:**
  - Written in plain language
  - Client name and birthdate
  - Type of information to be disclosed
  - Identifies provider authorized to make the disclosure
  - Identifies to whom the organization may make the disclosure
  - Signature of the patient or legal representative
    - If signed by legal representative, identify their relationship to the client
  - Date authorization is signed

HUSCH BLACKWELL

19

HIPAA Authorization

- **Requirements for valid HIPAA Authorization:**
  - Period authorization is effective and expiration date/event
  - Statements informing the patient of:
    - Patient's right to revoke authorization and how to do so
    - Services can NOT be conditioned upon willingness to sign (unless limited exceptions apply, such as a court order)
    - Potential for information to be re-disclosed
    - Fact that revoked authorization will not affect previous disclosures made
    - Right to inspect/copy the PHI disclosed
  - Special rules for "Protected Records"
    - Includes mental/behavioral health, alcohol/drug abuse, HIV test results, developmental disability or sexual/child/elder abuse records
    - Specifically describe the protected records in question

HUSCH BLACKWELL

20

"If you want to achieve greatness, **stop asking for permission**."

- Internet wisdom (maybe Abraham Lincoln?)

HUSCH BLACKWELL

21

Treatment, Payment, & Health Care Operations

- **Uses and disclosures for treatment, payment, & health care operations**
  - A covered entity may use or disclose PHI for its own TPO
  - A covered entity may use or disclose PHI for treatment activities of another health care provider.
  - A covered entity may disclose PHI for the payment activities of the recipient.
  - A covered entity may use or disclose PHI for the TPO of the recipient under certain circumstances and when the patient has a relationship with both entities.
- **Obtaining consent of the patient is optional**

HUSCH BLACKWELL

22

Business Associate Agreements (BAAs)

- **In order for a covered entity to share PHI with a business associate, the covered entity must enter into a BAA with the business associate.**
- **BAAs must contain specific provisions:**
  - Business associate will make PHI accessible to individual in accordance with 45 C.F.R. §164.524.
  - Business associate will make PHI available for amendment in accordance with 45 C.F.R. §164.526.
  - Business associate will make available information required to provide an accounting of disclosures in accordance with 45 C.F.R. §164.528.
  - Business associate will make internal practices, books, records available to HHS.
  - Business associate must authorize termination by CE for breach, and require that BA return or destroy all PHI at termination (or if infeasible, maintain protection).
- **May contain additional provisions (*e.g.* indemnification, no PHI overseas).**
- **Binding contracts; can be enforced in court.**

HUSCH BLACKWELL

23

Business Associate Agreements

- **When is a BAA *not* required?**
  - Treatment disclosures
  - OHCA
  - Incidental access or no access
  - Other scenarios

HUSCH BLACKWELL

24

Authorization or Opportunity to Agree or Object Not Required

- **Key Uses and Disclosures Covered by the Exception:**
  - Required by law
  - For public health activities
  - Victims of abuse, neglect or domestic violence
  - For law enforcement purposes
  - For judicial and administrative proceedings
  - To avert a serious threat to health or safety
  - Subpoenas and court orders…but…

HUSCH BLACKWELL

25

Federal Law vs. State Law

U.S. Constitution Supremacy Clause (Article VI, Clause 2):

"This Constitution, and the laws of the United States which shall be made In Pursuance thereof: and all Treaties made, or which shall be made, under the Authority of the United States, shall be the Supreme law of the land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding."

Any state law that conflicts with a federal law is preempted.

Gibbons v. Ogden, 22 U.S. 1 (1824)

To avoid confusion, Congress may (but is not required to) explicitly express its intent as to whether federal law should preempt state law and, if so, to what extent.

HUSCH BLACKWELL

26

HIPAA and Preemption

- **General rule:**
  - When state law conflicts with HIPAA, follow federal law – unless state law Is "more stringent" than HIPAA.
  - "More stringent" means:
    - A law that prohibits or restricts a use or disclosure or PHI beyond what is required under HIPAA, unless the use/disclosure is to HHS or to the individual.
    - A law that provides the individual greater rights of access or amendment, or to information than wt.at is provided under HIPAA. ·
    - A law that requires more detailed recordkeeping or retention.
    - A law that otherwise provides "greater privacy protection" to the individual.
- **Other limited exceptions also apply.**

HUSCH BLACKWELL

27

"Be the example you want to see in the world."

- Probably not Gandhi

28

Questions?

Scott LeBlanc
Partner
Milwaukee, Chicago
414.978.5512
Scott.LeBlanc@huschblackwell.com

Kelsey Toledo
Attorney
Milwaukee
414.978.5389
Kelsey.Toledo@huschblackwell.com

29