HIPAA 101
For Business Associates

Sarah E. Coyne,
Quarles & Brady LLP

Today's Webinar is Sponsored by:

Date Recorded:
August 7, 2019

HIPAA COW Mission

- Assist HIPAA Covered Entities, Business Associates, and other interested parties in implementing HIPAA's Privacy, Security and EDI Standard Transaction provisions, as amended over time.
- Foster public education about HIPAA.
- Facilitate and streamline HIPAA implementation through identification of best practices.
- Reduce duplicate efforts among entities obligated to comply with HIPAA.
- Offer opportunities for partnering and collaborating between entities implementing HIPAA.
- Identify and evaluate new or difficult HIPAA interpretation issues.

hipaacow.org®

Disclaimer

HIPAA Collaborative of Wisconsin ("HIPAA COW") holds the Copyright © to this HIPAA 101 for Business Associates Webinar ("Document"). HIPAA COW retains full copyright ownership, rights and protection in all material contained in this Document. Any HIPAA COW copyrighted document may be downloaded from the web, printed, and distributed in its entirety as long as: (i) the reproduced document contains the original HIPAA COW copyright and disclaimer and (ii) the document is provided free of charge. Any entity who wishes to adopt part or all of a document for its own internal compliance may do so without the copyright as long as the document is adopted solely for internal purposes and HIPAA COW is referenced as a source. Any other use of copyrighted material is prohibited without the express written permission of HIPAA COW. This Document is provided "as is" without any express or implied warranty. This Document is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney. Unless otherwise noted, HIPAA COW has not addressed all state pre-emption issues related to this Document. Therefore, this Document may need to be modified in order to comply with Wisconsin/State law.

LEGAL NOTICE: HIPAA Collaborative of Wisconsin Content and Liability Disclaimer

The HIPAA Collaborative of Wisconsin (HIPAA COW) shall not be responsible for any errors or omissions contained in materials provided by HIPAA COW. All information is provided on an "AS IS" basis.

HIPAA COW MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED (INCLUDING ANY WARRANTIES OF TITLE, NON-INFRINGEMENT AND IMPLIED WARRANTIES OF MERCHANT-ABILITY OR FITNESS FOR A PARTICULAR PURPOSE) REGARDING ANY INFORMATION CONTAINED IN ITS MATERIALS. THE USER OF THE MATERIALS SHALL ASSUME TOTAL RESPONSIBILITY AND RISK FOR THE USE OF THE MATERIALS. IN NO EVENT SHALL HIPAA COW BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO ANY INFORMATION CONTAINED IN THE MATERIALS PROVIDED BY HIPAA COW, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW OR OTHERWISE.

The content of the materials provided by HIPAA COW is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that HIPAA COW is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Today's Host

Sarah E. Coyne

Partner

Quarles & Brady LLP

Parts of HIPAA Affecting Business Associates

- Health Insurance Portability and Accountability Act
- Federal law designed to protect the privacy and security of patient information
- Includes the following:
  - Privacy Rule
    - Prohibits the use/disclosure of patient information without patient authorization except in certain limited instances; sets forth certain patient rights
  - Security Rule
    - Identifies a set of security safeguards (physical, technical, and administrative) that must be implemented to safeguard electronic patient information
  - Breach Notification Rule
    - Addresses steps that must be taken when the privacy of patient information is breached

Business Associate

- A business associate is a person or entity that creates, receives, transmits, or maintains PHI in performing services on behalf of a covered entity
- Includes:
  - Health information organizations (HIOs)
  - Data storage companies
  - Lawyers, accountants, consultants, etc. that get PHI
  - Subcontractors that create, receive, maintain or transmit PHI on behalf of another BA

To Whom Does HIPAA Apply?

- Covered Entities (CEs)
  - Health Care Providers
  - Health Plans
  - Health Care Clearinghouses
- Business Associates of Covered Entities (BAs)
  - And their subcontractors!

Protected Health Information

- Protected Health Information (PHI)

- Relates to the past, present or future:
  - Physical or mental health condition of an individual
  - Provision of health care to an individual
  - Payment for the provision of health care to an individual

Privacy Safeguards

- Privacy Rule:
  - CEs and BAs must:
    - Implement reasonable safeguards, and policies and procedures to protect patient privacy and avoid prohibited uses and disclosures
    - Appoint a Privacy Officer
    - Review their own practices and determine what steps are reasonable to safeguard their patient information
    - Train workforce members on HIPAA requirements and applicable policies and procedures
    - Enforce policies and procedures with sanction policy

Security Safeguards

- Security Rule:
  - Identifies a set of security safeguards (physical, technical, and administrative) that covered entities and business associates must implement to safeguard electronic PHI
  - Some safeguards are very technical (i.e., for IT Dept) others apply directly to general workforce
  - Must develop policies and procedures to address Security Rule requirements
  - Must appoint a Security Officer

Privacy vs. Security – Scope

- The Privacy Rule covers all PHI
  - Electronic
  - Paper
  - Spoken
  - Recorded in ANY form

- The Security Rule covers only electronic PHI (ePHI)

What Information is NOT Covered?

- Information that has been "de-identified"
  - De-identification involves removing all 18 identifiers or having an expert certify that the risk of re-identification is very small
  - Alternative: limited data set – which is covered, but fits into an exception
- Employment records
- Education records (Family Education Rights and Privacy Act)
- Information regarding individuals who are deceased for more than 50 years

The General Rule Under HIPAA

- Do not use or disclose PHI without patient authorization
  - Use = within the organization
  - Disclosure = outside the organization

- Unless the rules permit or require the use or disclosure

Major Exceptions that Permit CEs and BAs to Use or Disclose PHI Without a Patient Authorization Include

- Treatment
- Payment
- Health Care Operations

***Keep in mind that other laws may impose additional restrictions*

Minimum Necessary Doctrine

- HIPAA requires covered entities and business associates to limit the use or disclosure of PHI to the minimum necessary to accomplish the purpose of the use or disclosure

- For example, if you don't need to disclose an entire file or patient record – only disclose the limited portions that you need to disclose

Privacy and Security Officer

- The privacy officer and a security officer may be the same person BUT
  - Must be a designated person – not a group
  - Security officer is often an IT person
  - Privacy officer is often a compliance person
  - Should have job descriptions for each

Business Associate Agreements (BAAs)

- CEs are required to have a BAA with all BAs
- BAs are required to have a BAA with all subcontractors – also defined as BAs
- It can be tricky to figure out who the BAs are
- Start by remembering when you do NOT need a BAA:
  - Workforce
  - Treatment
  - Organized Health Care Arrangement
  - Conduits (just pass the PHI through – no access to it – e.g. email service providers like gmail)

Examples of Business Associates

- Lawyers, accountants, personal health record vendors, e-prescribing gateways, other service providers where PHI is involved
- Subcontractors of BAs that create, receives, maintain, or transmit PHI on behalf of the BA.
- Companies providing data transmission services to a CE involving PHI where routine access to PHI is required
- Companies that store PHI (these are not "conduits"

Liability for the BA's Actions

- Is the BA an agent?
  - A CE 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"
  - This means:
    - An entity can be penalized for its agent's violations
    - Knowledge by the agent will be imputed to the principal (e.g., knowledge of a breach or other violation)
  - Federal common law of Agency will govern whether an agency relationship exists between the parties – regardless of what the contract actually says

Business Associates Must Self Report Breaches (to the CE)

- The Business Associate Agreement (BAA) must ensure that the BA reports breaches to the CE within a designated number of days
- The obligation is to report a patient's PHI was accessed, acquired, used, or disclosed as a result of breach
- Applies to unauthorized uses and disclosures in any format – paper, verbal, electronic (does not apply to data that was encrypted)

What is a "Breach"

- Impermissible use or disclosure of PHI that is "unsecured" (not encrypted, essentially)
- Presumed to be a breach unless rebutted by a showing that there is a "low probability that PHI has been compromised" based on a four factor risk assessment:
  1. Nature of PHI
  2. Whether retained
  3. Whether person authorized
  4. Mitigation

Patient Rights Under HIPAA

- Gain access to medical records
- Request restrictions on uses and disclosures of PHI
- Request an amendment of PHI
- Accounting of disclosures
- Can “opt out” of patient directory
- Can submit grievance about privacy

BAs Are Limited in How They May Use/ Disclose CE's PHI

- Business associates may only use and disclose PHI for purposes of conducting the services it performs for the covered entity – and only as permitted by the business associate agreement
- This means BAs may not:
  - Sell data to third parties
  - Use/ disclose PHI for BA's own marketing

Sensitive Records

- Some "sensitive" records have additional protections on disclosure under state law
  - AODA
  - Mental health
  - Developmental Disability
  - HIV
  - Family Planning
- Must analyze these requirements in addition to HIPAA – not always consistent

Common Breach Risks

- PHI maintained on computers in high traffic areas
- Mobile devices (e.g., laptops, smartphones, etc.)
- Remote devices (e.g., home computer)
- Papers containing PHI left out on employees' desks
- PHI sent via unencrypted email and without password protection

Snooping is Illegal

- Accessing records of “interesting” patients out of curiosity
  - VIP/Celebrity patients
  - Patients under criminal investigation
  - Mental health patients
  - Friends or family members
- Don’t do it! This is a violation of HIPAA

Civil and Criminal Penalties for HIPAA Violation

- Tiered (and increased) civil monetary penalties
- Penalties range from $100 – $50K per violation (depending on type of violation) up to a total of $1.5 million per year
- Individuals with egregious violations could have criminal implications

Workforce Sanctions

- Employee Sanction Policies
  - CEs and Bas are required to maintain policies for privacy or security violations
  - Sanctions can range from additional education to termination
  - CEs and BAs must enforce sanction policies or could face penalties under HIPAA
  - CEs do not need to ensure that BAs enforce their own sanctions policy – that is the BA's problem

Workforce Training

- Absolutely required by CEs and BAs for their workforce members who encounter PHI
- Upon hire and regularly thereafter (ideally annually and whenever material changes)
- Training must be documented
- For Security Rule – periodic reminders to workforce

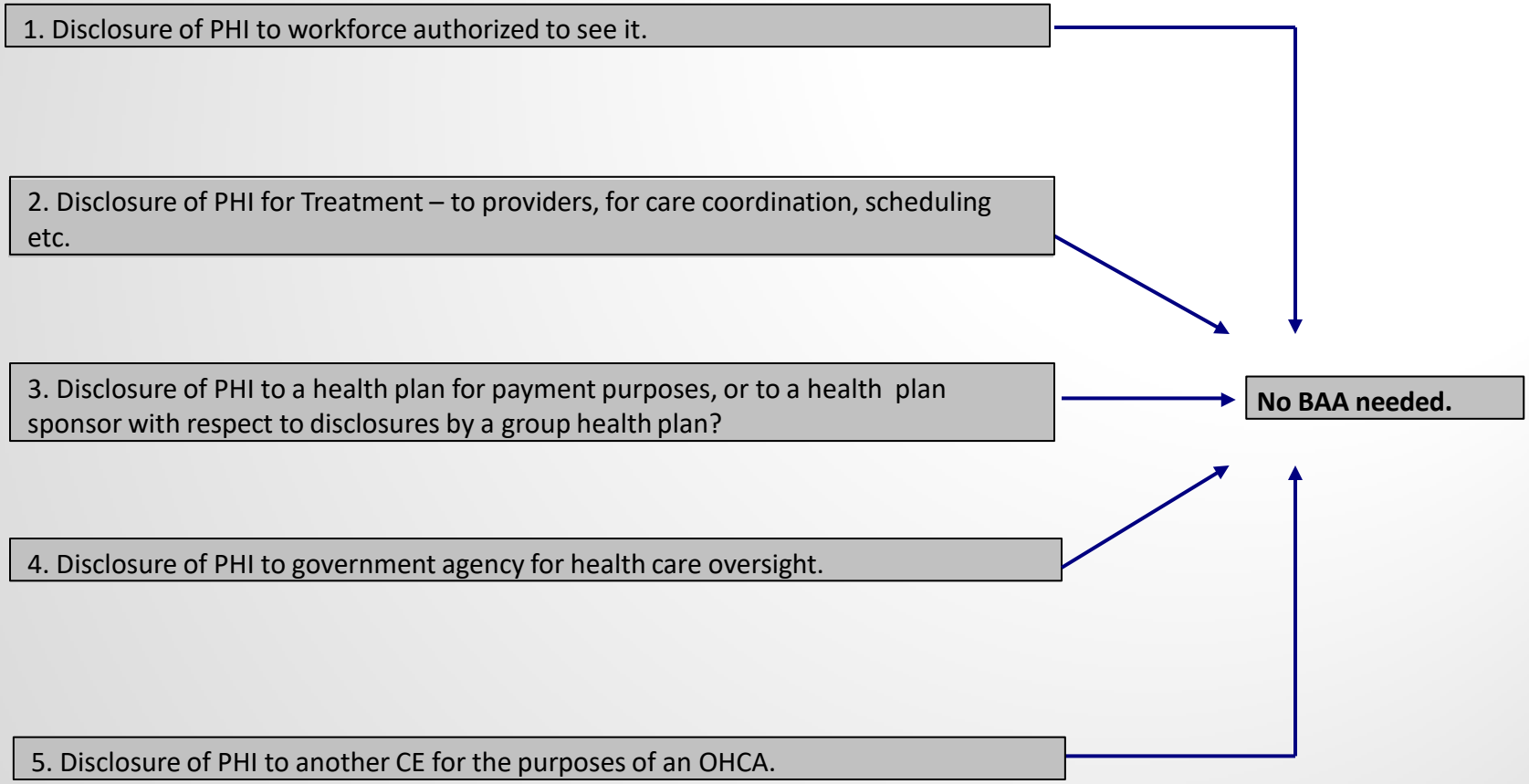
Policies, Procedures and Documentation

- Certain standards are required to be in a policy (e.g. minimum necessary, workforce sanctions)
- Toolkits/ samples are out there
- Documentation of compliance must be maintained for six years

Notice of Privacy Practices

- BAs do NOT have to do this
- May be delegated to BA by CE
- CEs do – it means telling patients how you may use or disclose their PHI without consent
- Required content (again, just for CEs)

Summary: When a BAA Is Not Needed



When a BAA Is Needed

1. Disclosure of PHI to a person or entity who creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA, including: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, and repricing.

→ **BAA IS needed.**

2. Disclosure of PHI to a person or entity who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial service

→ **BAA IS needed.**

Release of Information

General Wisconsin "Confidentiality" Laws

Law	Summary
146.82, Wis. Stat.	Covers general medical health care PHI and authorization requirements
51.30, 146.816, Wis. Stat.	Covers PHI relating to mental health, AODA, and developmentally disabled treatment, authorization requirements, and penalties – updated by "HIPAA Harmonization" law.
Wis. Adm. Code Ch. DHS 92	Further covers confidentiality of mental health treatment records (with 51.30)
Wis. Adm. Ch. DHS 144	Covers release of immunizations between vaccine providers, and to schools specifically for minors

Release of Information

General Wisconsin "Confidentiality" Laws

Statute	Summary
102.13 & 102.33, Wis. Stat.	Covers records reasonably related to a worker's compensation claim and release to the employee (patient), employer, worker's compensation insurer, or Department with a written request
610.70, Wis. Stat.	Covers disclosure of personal medical information by insurers
252.15, Wis. Stat.	Covers health care information relating to HIV testing and authorization requirements

Compliance Tips (1 of 3)

- Don't try to sneak a peek at PHI if not authorized – most entities now have audit trails
- Don't share passwords
- Use extra caution with laptops and PDAs – encrypt data when possible
- Move computer monitors so others can't see
- Don't let unauthorized people into restricted areas

Compliance Tips (2 of 3)

- Avoid discussions about patients in hallways or elevators
- Don’t leave confidential information unattended (e.g., top of your desk is not secure)
- Log off when you leave your workstation
- Don't post PHI on Facebook!

Compliance Tips (3 of 3)

- Don't leave laptops, files, charts, etc. in the car or in public areas
- Make sure you are leaving a voice message at the correct phone number and limit the information you provide
- When transmitting PHI, make sure you have the right email address and fax number and that you have attached the right document

Questions?

Sarah Coyne
Quarles & Brady LLP
(608) 283-2435
sarah.coyne@quarles.com

Thank You!

Thank you for viewing this webinar. If you have any comments or feedback, please feel free to email us at admin2@hipaacow.org.

Visit our website at hipaacow.org!!

hipaacow.org®

"Like Us" on facebook

"Follow Us" on LinkedIn