HIPAA Privacy 101

Sarah E. Coyne,
Quarles & Brady LLP

Today's Webinar is Sponsored by:

GODFREY KAHN S.C.

Quarles & Brady LLP

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 Privacy 101 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

What is HIPAA?

- 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

To Whom Does HIPAA Apply?

- Covered Entities
  - Health Care Providers
  - Health Plans
  - Health Care Clearinghouses
- Business Associates of Covered Entities
- For full definitions, see 45 C.F.R. § 160.103

Health Care Providers

- ONLY IF THEY TRANSMIT INFORMATION IN ELECTRONIC TRANSACTIONS FOR WHICH HHS HAS ADOPTED A STANDARD
- Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, Assisted Living Facilities, Pharmacies

Health Plans

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care (Medicare/ Medicaid, others)

Health Care Clearinghouses

- Entities that process nonstandard health information into a standard format
- Classic example – billing company that receives Medicare claims and converts them to a format that Medicare's electronic system will understand

Part D Sponsors

- Prescription Drug Plans under Part D – Sponsors are covered entities under HIPAA
- Voluntary outpatient prescription drug programs

Business Associates

- 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

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)

Who Is A Business Associate – Examples:

- 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"

The BA Relationship is Not Contingent on the BAA

- Having a BAA does not make everything you do compliant
- Not having a BAA does not excuse you from liability if a BA relationship exists
- A BA relationship exists if the person performing the services meets the definition of “business associate”
- This is true even if the parties fail to enter into a BAA – but then the failure is a HIPAA violation – for BOTH the CE and the BA

What Does HIPAA Cover?

- 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; or
  - Payment for the provision of health care to an individual

  - See 45 C.F.R. § 160.103

What Does HIPAA Cover?

- Includes both oral or recorded information
- Electronic or paper – any form

NOT PHI:

- Information that has been "de-identified"
  - De-identification requires removing all 18 identifiers or obtaining an opinion from a qualified expert that the risk of re-identification is "very small"
  - Limited data set is another option
- Employment records
- Education records (Family Education Rights and Privacy Act)
- Information regarding individuals who are deceased for more than 50 years

Patient Identifiers that Render Information PHI

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

The General Rule Under HIPAA

- Do not use or disclose PHI without patient authorization
  - Use = within the covered entity
  - Disclosure = outside the covered entity, even to business associates
- HIPAA carves out exceptions where PHI may be used or disclosed, i.e., where the general prohibition does not apply

- See 45 C.F.R. § 164.502

Major Exceptions to Privacy Prohibition

- TO THE PATIENT (or legal representative)
- TPO
  - Treatment – provision, coordination, management of care/ related services including consults and referrals
  - Payment for health care – reimbursement for health care, coverage, all related activities
  - Health care operations – slide coming up

Exception – Health Care Operations

- Quality assessment and improvement
- Competency assurance/peer review/ credentialing
- Audits, legal or medical reviews, compliance
- Insurance functions
- Business planning, development, management administration
- General administrative activities including de-identification/creating limited data set

45 C.F.R. § 164.501

Exceptions – Opportunity to Agree or Object

- Facility directories (may disclose condition and location in facility to those who ask by name, and religious affiliation to clergy)
- Family/friends – Disclosure okay if relevant to that person's involvement in care or payment for care
  - Example: Your spouse can pick up your prescriptions from the pharmacy
  - 45 C.F.R. § 164.510

Exception – Incidental Disclosures

- At times it is unavoidable that some people will hear PHI (but must try to limit)
- Examples (these are not violations under HIPAA):
  - Staff Member A sitting next to Staff Member B overhears B's conversation with a covered entity client involving PHI.
  - Attorney A and Attorney B print at the same time. Attorney A's document contains PHI. Attorney B inadvertently views A's document while trying to obtain his own document.

Other Major Exceptions to Privacy General Prohibition

- Where required by law (e.g. child abuse reporting)
- Certain communications about decedents
- Public Health Agencies (like CDC)
- Health Oversight Agencies (like DHHS)
- Disaster/ Emergency
- Clinical Research (with lots of caveats)

Other Major Exceptions to Privacy Prohibition

- Judicial and Administrative Proceedings
- Certain Disclosures to Law Enforcement
- Serious Threat to Health or Safety
- Essential Government Functions
- Workers' Compensation

- See 45 C.F.R. § 164.512

Minimum Necessary Rule

- 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.

- 45 C.F.R. §§ 164.502(b); 514(d)

Fundraising

- A CE may use or disclose to a BA or an institutionally related foundation certain PHI for fundraising without a patient authorization!
- PHI that may be disclosed:
  - Individual's demographic information (name, address, contact information, age, gender and birth date)
  - Dates of health care provided to an individual
  - Department of service information (e.g., cardiology, oncology, pediatrics)
  - Treating physician
  - Outcome information (e.g., information regarding death of patient, sub-optimal result of treatment of services)
  - Health insurance status

45 C.F.R. § 164.514(f)

Fundraising Opt Out

- Each fundraising communication to an individual must:
  - Provide “clear and conspicuous” opportunity to opt-out
  - Be written in clear, plain language
- Opt-out method may not cause an undue burden or more than a nominal cost
  - OKAY: toll-free phone number; email address; pre-printed, pre-paid postcard; can offer multiple methods
  - NOT OKAY: writing a letter

Patient Rights Under HIPAA

- Right to Access
- Right to Request Restrictions on Uses and Disclosures of PHI
- Right to Request Amendment of PHI
- Right to an Accounting of Disclosures
- Right to Request Confidential Communications
- Right to Complain About Disclosures
- Notice of Privacy Practices

See 45 C.F.R. §§164.520-164.528

Request for Access

- Individuals have a right to access and copy their health information, with certain limited exceptions
- If an individual requests an electronic copy of PHI that is maintained electronically, the CE must provide it in the form and format requested by the individual if readily producible, or if not, in a readable electronic form and format as agreed to by the CE and the individual

Request for Access

- Fees:
  - Covered entity may impose reasonable cost-based fee that includes cost of:
    - Labor for copying (paper or electronic)
    - Supplies for creating the paper copy or electronic media if patient requests the electronic copy be provided on portable media
    - Postage (if records will be mailed)
    - Prepare summary or explanation of PHI
  - But – remember state laws may impose additional restriction on permitted fees

Request for Restrictions

- Privacy Rule requires covered entities to permit individuals to request a restriction on the use or disclosure of PHI
- A covered entity must agree to a request to restrict disclosures of PHI to a health plan if:
  - The disclosure is for purposes of payment or health care operations, and is not otherwise required by law; and
  - The PHI pertains solely to the health care items or services the individual paid out-of-pocket in full
- Required restriction may only be terminated if the individual agrees

Request for Restrictions

- Identifying restricted PHI:
  - Providers are not required to create separate medical records or segregate PHI that is subject to a restriction
  - But – will need to use some method to flag or make a notation in the record to identify restricted PHI to ensure such PHI
    - Paper records
    - Electronic records

Accounting and Amendment

- Individuals have right to an accounting of certain disclosures of the individual's PHI made in the previous six years
- Individuals have right to request amendment to PHI
  - CE does not have to agree if the PHI is accurate and complete, among other exceptions

Confidential Communications

- Individuals have right to request to receive communications of PHI by alternative means or at alternative locations
- Health care providers must agree to reasonable requests
- Health plan must agree only if individual clearly states the disclosure of PHI could endanger the individual

Notice of Privacy Practices

- CE must inform patients how PHI about that patient will be used or disclosed
- Lots of picky stuff has to be in there
- Providers must give it to patient at first delivery of service
- Every CE must post it on their website
- Notify patients/health plan members when materially changed

HIPAA Enforcement

- Used to be complaint driven only – now affirmative audits
  - More audits coming "soon"
- Penalties used to be mostly theoretical – now being imposed
  - Criminal and civil
  - CMPs range from $100 – $50,000 per violation, cap of $1.5 million for identical violations in a year
- State Attorney Generals can get in on the action

Incidental Disclosures

- At times it is unavoidable that some people will hear information about other patients (but must try to limit)
- Examples (these are not violations under HIPAA):
  - Patient in a semi-private room overhears a discussion between the physician and patient
  - Person in line overhears a conversation between another patient and the registrar

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

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

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

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

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

HIPAA Preemption

- Other federal and state laws to consider in addition to HIPAA
- If you can follow BOTH laws, no problem
- If contrary, then the more "stringent" law controls, which means:
  - More restrictive on uses and disclosures of PHI, OR
  - Provides greater rights to patients with regard to PHI.

Wisconsin Law

- Key confidentiality laws:
  - Wis. Stat. 146.82: Disclosure of general patient records
  - Wis. Stat. 51.30 and Wis. Admin. Code ch. DHS 92: Disclosure of treatment records (mental health, AODA, developmental disabilities)
  - Wis. Stat. 252.15: Disclosure of HIV test results
  - NEW-ISH Wis. Stat. 146.816: HIPAA Harmonization

Wis. Stat. 146.82: Disclosure of General Patient Records

- Renders a patient's health care records confidential and provides that they may be released only with the patient's informed consent or where a statutory exception applies including:
  - TPO
  - Court order
  - Where de-identified
  - Child abuse
  - many more…

HIPAA Harmonization

- HIPAA Harmonization for Mental Health Care Coordination Law ("HIPAA Harmonization")
  - Effective since April 10, 2014
- Aligns Wisconsin's law with HIPAA regarding use and disclosure of all records for TPO, which makes a big difference for mental health and AODA treatment records
  - HIPAA does not treat mental health information differently, except for "psychotherapy notes"
- PERMITS providers more freedom in using, disclosing or requesting disclosure of mental health records, if the provider so chooses

42 CFR Part 2

- BIG CAVEAT to harmonization analysis
  - Applies to treatment records of federally assisted drug and alcohol abuse programs and certain third parties who receive records from such programs
  - Imposes restrictions above and beyond HIPAA and Wisconsin law
  - Harmonization law does NOT change this

Wis. Stat. 252.15: Disclosure of HIV Test Results

- Prohibits requiring a person to authorize disclosure of HIV test results as a condition of administering a test
- Only person tested or his/her authorized representative may disclose the HIV test results unless either person has signed authorization for the disclosure
  - Limited exceptions

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