HIPAA and Health Privacy FAQ Session

Health Law Webinar

October 11, 2023

Fredrikson

Where Law and Business Meet®

Agenda

- HIPAA
- 42 CFR Part 2
- FTC Breach Notification Rule

**Don’t forget applicable state laws.

What's new with HIPAA?

- Short Answer: Not much, yet.
- Beware of ordinary course HIPAA clickbait.
- Two Notices of Proposed Rulemaking:
  - Reproductive Health.
  - Substance Use Disorder Records.
- End of COVID-19 Enforcement Discretion.
- Guidance on Online Tracking Technologies.

HIPAA Might Change: What's Happening?

- OCR and SAMHSA have **proposed** changes to HIPAA's Privacy Rule and 42 CFR Part 2.
- Reproductive Health Care:
    - To protect information related to reproductive health care.
    - Comment period ended June 16, 2023.
    - NPRM: https://www.federalregister.gov/documents/2023/04/17/2023-07517/hipaa-privacy-rule-to-supportreproductive-health-care-privacy.
    - NPRM Fact Sheet: https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-factsheet/index.html.
- Substance Use Disorder:
    - Changes were designed to harmonize HIPAA and Part 2.
    - Comment Period ended January 31, 2023.
    - NPRM: https://www.federalregister.gov/documents/2022/12/02/2022-25784/confidentiality-of-substance-use-disorder-sud-patient-records.
    - NPRM Fact Sheet: https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-part-2/index.html.

Online Tracking Technologies

- Tracking technologies (e.g., cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts) must be used in a HIPAA-compliant manner.
  - For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
- Per the guidance all "individually identifiable health information" collected on a covered entity's or business associate's website or mobile app is protected health information (PHI) because when the user's information is collected, the information connects the user to the covered entity or business associate and relates to the user's treatment or payment for care. Even when the user does not have an existing relationship with the entity and even if the information does not include treatment or billing information.
- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

Can we send emails to patients? What about text messages?

- "A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations." 45 CFR 164.522(b).
- OCR guidance permits covered entities to send individuals unencrypted emails if:
  - They have advised the individual of the risk, and
  - The individual still prefers the unencrypted email (78 FR 5566, 5634).

Emails and texts, continued…

- As with all disclosures of PHI, a covered entity still must use reasonable safeguards when sending unencrypted email or text.
- Suggested Practices:
  - Get written consent from the patient if they wish to communicate by text or email.
  - If written consent is not feasible, document how consent was provided.
  - Additional safeguards.

Emails and texts, continued.

- Strong password protection on all devices.
- Settings that don’t allow messages to be viewed on a locked device screen.
- Minimum information necessary.
- Limits on the type of patient information that can be exchanged (e.g., no sensitive information).
- A process to promptly transfer patient information to secure systems.
- Encryption on devices.
- Security safeguards that allow remote locking of the device if it is lost or stolen.
- Restrictions on the use of personal devices for work purposes.

What about provider-to-provider texting?

- Use a standalone secure texting application that integrates with the EMR.
- Do not use for texting orders.
- Establish clear policies.

Can we release medical records we received from a third party?

- Yes. Under HIPAA, “PHI” is any health information, created, received, or maintained by a covered entity.
- HIPAA lets a covered entity disclose PHI in a designated record set.
- Substance use disorder records protected by federal law should NOT be redisclosed.
- Remember state law considerations.

What can we charge for copying medical records?

- Who is the request from?
- Three methods:
  - Actual costs.
  - Average cost.
  - Schedule of costs for labor based on average labor cost.
- Can charge per page only where PHI is in paper form and person asks for a paper copy.
- Flat fee of $6.50 maximum.
- Notify individuals in advance of the approximate fee for copies.

Can we use sign-in sheets or call patients using first and last name?

May physician's offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

Back to top

Feedback

Answer

Yes. Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

Date Created: 12/19/2002
Last Updated: 03/14/2006

Patient names, continued…

- One of many “incidental disclosures” in health care.
- Apply minimum necessary standard.
- Consider patient perceptions/best practices.
- Respect patient preferences, where possible (the patient has a right to request confidential communications).
- Where possible, avoid over-sharing, even if justifiable under HIPAA.

Can I leave a voicemail?

- Generally, yes.
- Use good judgement and apply reasonable safeguards.
- Careful with storing numerous phone numbers.
- See FAQ: https://www.hhs.gov/hipaa/for-professionals/faq/198/may-health-care-providers-leave-messages/index.html.

Can we respond to online reviews?

- Proceed with extreme caution, particularly with negative reviews.

How often do I have to…

- Train?
- Risk Assessment?
- Keep records?
- Monitor access?

Can a patient sue under HIPAA?

- No private right of action under HIPAA.
- Indirect causes of action (see e.g., Pixel tracking suits).
- Watch out for state laws.

What are the quickest ways to get in hot water?

- Patient complaints (e.g., right of access complaints).
- Mishandling a Breach.
- Large Breaches

….which leads to an investigation and finds:

- Failure to perform risk analysis.
- Insufficient safeguards/security measures.
- Failure to have/implement policies.
- Failure to have BAAs.

My practice is entirely cash pay, am I still covered by HIPAA?

- Covered Entities = providers, health plans and clearinghouses.
  - Must furnish, bill, or receive payment for health care in the normal course of business.
  - Must transmit “covered transactions” electronically.
- Covered Entity Decision Tool: https://www.cms.gov/about-cms/what-we-do/administrative-simplification/hipaa/covered-entities.

No Standard Transactions, No Problem?

- Applicability of FTC Health Breach Notification Rule.
  - FTC Policy Statement expands scope of the Health Breach Notification Rule, (16 C.F.R. Part 318).
  - Proposed Rule would codify that policy in regulation.
  - A vendor of personal health records includes:
    - "[A]ny online service such as a website, mobile application, or internet connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools."

Is my business a business associate?

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

Do we need indemnification in our BAAs?

- Recommended, unless too narrow.
- Not included in the “model” BAA provided by HHS.
- Confirm scope.
- Confirm applicability of any caps/limitations in underlying agreement.
- Consider reimbursement provisions.

My vendor is “HIPAA-compliant,” so no further questions, right?

- Careful: Purchasing “HIPAA compliant” products and services does not guarantee HIPAA compliance.
- Choose vendors wisely by reviewing:
  - HIPAA experience and knowledge.
  - BAA terms.
  - Risk Assessments and policies.

Including BAAs in EVERYTHING – Good? Bad? Ugly?

- It depends, but it usually gets ugly.
- A thoughtful analysis upfront can avoid disputes later.
  - Qualifying language.
  - Indemnification implications.
  - Confusion with OCR.

Our practice works directly with employers, can I share PHI with them?

- Generally, no. Not without an authorization from the patient.
- Exceptions for workers' compensation disclosures allowed by state law.

…what if the Employer has a self-insured plan?

- Disclosures to the Plan may be permitted, but confirm applicable personnel and be cautious.
- Separate legal entity.

Do I need to do a Security Rule risk analysis?

- YES.
- An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the Covered Entity.
- Risk Analysis vs. Gap Analysis.
- Ransomware, encryption, software patches.

Do I need to have a third party perform my Security Rule risk analysis?

- No, but depending on the size and complexity of your organization, it can be a good idea.
- ONC and OCR have a HIPAA Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

How do I determine if there's a low probability of compromise?

- An impermissible acquisition, access, use, or disclosure of PHI is **presumed to be a breach,** unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.

Is it a Breach?

- Mailing PHI to the wrong patient?
- Employee snooping?
- Sending information to the wrong health plan? Wrong provider?
- Stolen laptop?
- Social media posting?

It’s a Breach, now what?

- Assess scope to determine your notification obligations.
- Watch the clock.
- Assess impact of state laws.
- Notify insurer, as appropriate.
- Prepare notices, credit monitoring, etc.

Is this a security incident?

- ***Security incident*** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- ***Information system*** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Do I have to monitor EHR access?

- Certain Security Rule standards are “required” others are “addressable.”
- Audit Controls (Required).
- Information System Activity Review (Required).

Can I disclose information to a credit card company if a charge is disputed?

- Credit card companies are not a “business associate.”
- Disclosure for payment purposes are permitted.
- Minimum necessary.

We've de-identified the PHI, so HIPAA no longer applies, right?

- The analysis is different for a covered entity vs. business associate.
- De-identification is harder than most people think.
  - Safe Harbor:
    - Removal of 18 types of identifiers.
    - No actual knowledge residual information can identify individuals.
  - Expert Determination:
    - Hire statistical expert.
    - Very small risk of re-identification.
    - Documentation.

How should we handle subpoenas and other document requests?

Be Suspicious

- Person demanding info (attorney, administrator, law enforcement) may not understand or care about HIPAA.
- They have one goal = get the information they need.
- Do not trust their understanding of HIPAA or what it does (or does not) require of you.

Request Analysis

Before disclosing information, ask yourself:

1. Does HIPAA apply? What other laws apply?
2. Do HIPAA and other laws allow disclosure?
3. Even if the laws allow disclosure, should you?

Prohibitions

- May not use or disclosure PHI unless:
  - For purposes of treatment, payment, or healthcare operations;
  - Have written, HIPAA compliant authorization;
  - Disclosure is required by law; or
  - An exception that allows disclosures.

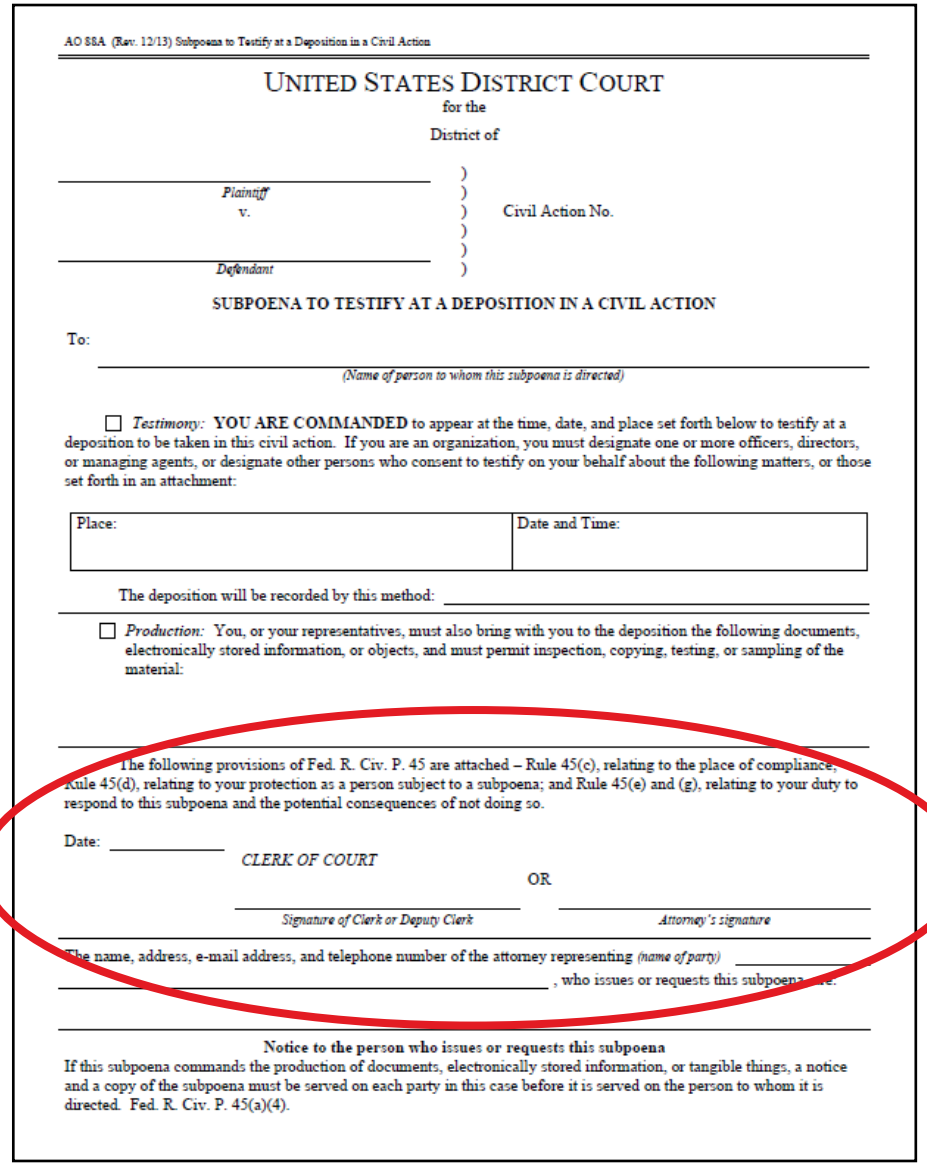
See 45 CFR § 164.502.

Examples of Permitted Disclosures

- Disclosures required by law.
- Disclosures in administrative or judicial proceeding.
- Court order or warrant signed by judge.
- Grand jury subpoena.
- Disclosures to law enforcement.
- Subpoena if certain conditions satisfied.

See 45 CFR § 164.510 and § 164.512

Subpoena (Not Signed By Judge) for Documents



AO 88A (Rev. 12/13) Subpoena to Testify at a Deposition in a Civil Action

UNITED STATES DISTRICT COURT
for the
District of

_____ Plaintiff
v.
_____ Defendant

Civil Action No.

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: _____
(Name of person to whom this subpoena is directed)

☐ *Testimony:* **YOU ARE COMMANDED** to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about the following matters, or those set forth in an attachment:

Place:	Date and Time:

The deposition will be recorded by this method: _____

☐ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: _____

CLERK OF COURT

OR

_____ *Signature of Clerk or Deputy Clerk*

_____ *Attorney's signature*

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* _____, who issues or requests this subpoena, are:

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

- *Duces tecum.*
- Under HIPAA, need "satisfactory assurances" 45 CFR § 164.512(e)(1)(ii).
- BUT state law may be stricter.
- Out-of-state subpoenas must be domesticated.

Subpoena (Not Signed By Judge) for Testimony

- Depositions, trial testimony, or other proceedings.
- Would testimony require disclosing PHI?
- Does the court have jurisdiction?
- If yes:
  - Motion to quash.
  - Appear and object.
  - Work with subpoenaing party.

Court Order or Subpoena Signed by Judge

- Comply.
- Petition the court.
- Limit disclosure to extent required.
- Notify patient.

Law Enforcement Administrative Request

- *May* disclose per administrative request, subpoena, summons or demand authorized by law if:
  - State or other law allows it;
  - Info relevant and material to legitimate law enforcement inquiry;
  - Request is reasonably specific and limited to purpose; and
  - De-identified info could not be used.

45 CFR 164.512(f)(1)(ii)

Accounting of Disclosure Log

- Log response in accounting of disclosure log required by 45 § CFR 164.528.

Is a subpoena or warrant sufficient under Part 2?

- No. Warrants and subpoenas are not sufficient to compel disclosure of Part 2 protected records.
- Court order must meet the specific criteria set forth in 42 CFR 2.65.

Does 42 CFR Part 2 apply to clinics?

- Yes, if it holds itself out as providing substance use disorder services.
- "Part 2 Program" means a federal assisted:
  - Individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
  - Identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
  - Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

Applicability of 42 C.F.R. Part 2

- The phrase “holds itself out” is not defined in the regulations, but could mean a number of things, including but not limited to state licensing procedures, advertising or the posting of notices in the offices, certifications in addiction medicine, listings in registries, internet statements, consultation activities for non-“program” practitioners, information presented to patients or their families, or any activity that would lead one to reasonably conclude that the provider is providing or provides alcohol or drug abuse diagnosis, treatment or referral for treatment.

Presenters

Marguerite Ahmann
Attorney
612.492.7495
mahmann@fredlaw.com

Mary Heath
Attorney
612.492.7272
mheath@fredlaw.com

Thank you!

Fredrikson

Where Law and Business Meet®

Family/Friends FAQ