Upcoming And Recent OCR Guidance

1

Privacy Impacts of the Dobbs Case

2

Dobbs Case

1. Overturned Roe v. Wade and U.S. v. Casey.
2. In Wisconsin, reinstated a 170 year old criminal statute prohibiting abortion unless necessary to save the life of the mother.
3. Roe v. Wade and U.S. v. Casey had been based on an implied constitutional right of privacy which Dobbs rejected.

3

Biden Executive Order and HHS Response

1. Called on HHS to undertake initiatives to protect the privacy of individuals seeking reproductive health services and to provide guidance for HIPAA –related entities.
2. OCR concurrently issued two separate privacy-focused guidance documents.
   - In one of the guidance documents, OCR spoke directly to individuals about HIPAA's limitations in protecting their health information, and encouraged consumers to take steps to safeguard their data when using smartphones, tablets, and other devices for personal use.
   - In the other guidance document, OCR advises HIPAA-regulated entities on when they may (and may not) disclose protected health information (PHI) to state officials or law enforcement entities.

4

HHS Guidance and Examples (1)

1. Required By Law Example: An individual goes to a hospital emergency department while experiencing complications related to a miscarriage during week ten of pregnancy. A hospital workforce member suspects the individual has taken medication to end the pregnancy. Wisconsin law prohibits abortion except in life-threatening emergencies but does not require the hospital to report individuals to law enforcement. Accordingly, HIPAA would not permit a disclosure to law enforcement under the "required by law" permission, and HHS states that such a disclosure would be impermissible and constitute a breach of unsecured PHI requiring notification to HHS and the individual affected.
2. Law Enforcement Example: A law enforcement official goes to a reproductive healthcare clinic and requests records of abortions performed at the clinic. If the request is not accompanied by a court order or other mandate enforceable in a court of law, HIPAA would not permit the clinic to disclose PHI in response to the request. Therefore, such a disclosure would be impermissible and constitute a breach of unsecured PHI requiring notification to HHS and the individual affected.

5

HHS Guidance and Examples (2)

Disclosure – Warning of Dangerousness: A pregnant individual in Wisconsin informs her healthcare provider of her intent to seek an abortion in another state where abortion is legal. The provider wants to report this to law enforcement to attempt to prevent the abortion from taking place. HHS considers this an impermissible disclosure of PHI under the HIPAA Privacy Rule for several reasons, including (i) the intended legal abortion does not qualify as a "serious and imminent threat to the health and safety of a person or the public," and (ii) such disclosure would be inconsistent with professional ethical standards.

6

Potential Impact In Wisconsin

1. Clearly legislated privacy protections will remain in place, e.g. Wis. Stat. 252.11 (STDs) and Wis. Stat. 51.47 (AODA).
2. Imputed reproductive privacy protections for minors may be interpreted differently in the future – the vague constitutional right to privacy is one of the tools in the arsenal.
3. Patient records sought for criminal prosecution of a physician will require the standard analysis – authorization or court order unless they fit another exception.

7

Recent OCR Enforcement Actions and Settlements – What Can We Learn?

8

Recent OCR Enforcement Actions and Settlements – What Can We Learn?

HIPAA Right of Access Initiative

- 41 announced settlements from September 2020–September 2022 with penalties ranging from $3,500 to $240,000 and imposed on a variety of providers
- ***Example***: Children's Hospital & Medical Center (CHMC)
  - Complainant alleged CHMC failed to provide her with timely access to her deceased daughter's protected health information. CHMC provided some records but did not provide all of the requested records despite the parent's multiple follow-up requests
  - Resulted in $80k settlement and Corrective Action Plan (CAP) that includes a revision of internal policies and procedures, implementation of staff training, and a one-year reporting period regarding CHMC's compliance with the CAP

Key Takeaways:

- OCR will continue to focus on and enforce the HIPAA Right of Access by highlighting situations that commonly lead to improper denials of access requests – multiple requests, length of delay, etc.
- Increased penalties for barriers to patient access
- Covered entities should have a clear policy but be prepared to pivot with upcoming final rule

9

Recent OCR Enforcement Actions and Settlements – What Can We Learn?

Recent HIPAA Privacy and Security Rule Violation Topics

- Avoid Disclosing PHI when responding to online reviews and be responsive/cooperative to communications from OCR
- Communications that do not fall under the Privacy Rule exceptions listed at 45 CFR 164.501 and are not authorized by the patient constitute impermissible "Marketing"
- Failure to safeguard PHI, including by failing to conduct an accurate and thorough risk analysis, and by failing to implement security measures sufficient to reduce risks and vulnerabilities, can result in costly fines and Corrective Action Plans
- Conducting privacy/HIPAA due diligence during mergers and acquisitions can protect entities from costly fines and Corrective Action Plans
- HIPAA Policies and Procedures should account for the proper disposal of documents and materials containing PHI.

10

Recent OCR Enforcement Actions and Settlements – What Can We Learn?

OCR's RFI for HITECH Penalties and Security Measures

- On April 6, 2022, OCR released a Request for Information seeking input from the public for two provisions of HITECH in light of the growing number of cybersecurity threats driving the need for enhanced safeguards of ePHI.
  - How covered entities and business associates are implementing "recognized security practices" and
  - Harms that should be considered in the distribution of CMPs and monetary settlements to harmed individuals, potential methodologies for sharing and distributing monies to harmed individuals, submission of alternative methodologies.
- Comments were required to be submitted by June 6, 2022.
- No further public action since June but keep an eye out for changes to enhance safeguarding of ePHI.

11

HHS Guidance on Telehealth and Audio-Only Care Encounters

12

HHS Guidance on Telehealth and Audio-Only Care Encounters

- March 2020: in response to the COVID-19 public health emergency (PHE), OCR issued the Telehealth Notification to assist the health care industry's response to the PHE and to quickly expand the use of remote health care services.
- OCR was using its enforcement discretion in not penalizing providers who were using non-public facing video applications (e.g., Zoom, Skype, Apple FaceTime, etc.) to diagnose and treat patients remotely.
- Still in effect until the PHE is ended.
- Current extension was through 10/13/22, but the Administration said they will give at least a 60-day notice before the PHE ends.

13

HHS Guidance on Telehealth and Audio-Only Care Encounters

- June 2022: HHS issued guidance on HIPAA and Audio-Only Telehealth that would be put into effect at the end of the PHE.
  - This guidance is applicable to all types of telehealth (not just audio-only services), except where specifically identified.
  - Issued in response to Executive Order 14058 ("Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government").
  - Covered Entities can use remote communication technologies to provide audio-only telehealth services when such communications are conducted consistent with the applicable requirements of HIPAA.
  - Audio-only telehealth is helpful for populations that may have difficulty accessing in-person or video-only healthcare for various reasons (e.g., limited financial resources, limited English proficiency, disability, internet access or sufficient broadband, cell coverage, etc.).

14

HHS Guidance on Telehealth and Audio-Only Care Encounters

HIPAA Permits Telehealth in Compliance with the Privacy and Security Rules

- Privacy Rule
  - Requires CEs apply "reasonable safeguards" (e.g., providing services in private settings, using lowered voices/no speakerphone, etc.).
  - Must verify identity of unknown individuals orally or in writing - note that civil rights laws require communications with individuals with disabilities to be as effective as communication with others, which extends to identity verification procedures.
- Security Rule
  - Does not apply to communication over traditional landlines because information transmitted is not electronic
  - Does apply to other forms of remote communication, including VoIP calls, cell phones, Wi-Fi, etc.
    - CEs are not responsible for privacy/security of PHI once it has been received by the patient's phone or device
  - Risks to confidentiality, integrity, and availability of ePHI when using technology must be identified, assessed, and addressed in the CE's risk analysis and risk management process.
- BAAs with vendors
  - Need to consider whether vendor is acting as a BA (creating, receiving, or maintaining PHI on behalf of the CE), or whether vendor has only transient access to the PHI being transmitted

15

Enabling Integrated Care: Recent Changes to HIPAA Regulations and 42 CFR Part 2

Noreen Vergara
Senior Counsel
HUSCH BLACKWELL LLP
The Link Virtual Office
4801 Main Street,
Suite 1000
Kansas City, MO 64112-2551
Direct: 816-983-8252
Fax: 816-983-8080
Noreen.Vergara@huschblackwell.com
huschblackwell.com
vBio|vCard

16

Changes Coming to Treatment, Payment, and Operations Exception

The OCR announced new regulations on Dec. 10, 2020 and final regulations are expected to be. Changes focus on increasing the ability of the individual to direct how and to whom their PHI is shared include:

Reducing the time a CE must provide access to access to PHI to 15 days from 30 days.

Providing individual with greater ability to transfer their PHI and direct who receives PHI.

- Transfer to a personal health application.
- Process for individuals to direct the sharing of PHI maintained in an EHR among CEs.
- Allows patient to direct individual to request certain records from another provider.
- Added ability for individual to request a direct copy of PHI when a summary is offered as an alternative.
- Expanded definition of "healthcare operations" to include care coordination and case management.
- Added minimum necessary standard – regardless of whether a particular care coordination or case management services is considered "treatment" or "healthcare operations."

17

42 C.F.R. Part 2: Overview

Federal standard that imposes greater restrictions on the disclosure and use of Substance Use Disorder ("SUD") patient records when maintained in connection with the performance of any part 2 program.

- Prohibition on disclosure and re-disclosure without appropriate consent.
  - Including disclosures related to Treatment, Payment and Healthcare Operations ("TPO"), except in limited situations.
  - Individual "consent" to sharing substance use disorder information while individuals "authorize" the sharing of PHI beyond what is permitted under HIPAA.

18

42 C.F.R. Part 2 ("Part 2") Recent Revisions

Regulation Amended in 2017, 2018, and 2020: Before that, the regulation hadn't been amended in 30 years.

Intended to "modernize" Part 2 regulations to account for healthcare integration and technology advancements to better coordinate care delivery. Criticized at the time for failure to align more fully with HIPAA.

- *Pending changes to HIPAA regulations will better align HIPAA with Part 2.*

19

42 C.F.R. Part 2: Recent Revisions (cont'd)

2020 & 2021 Changes:

- Clarified the definition of "Program":
  - "Program: (1) An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, SUD diagnosis, treatment, or referral for treatment; or (2) an identified unit within a general medical facility that holds itself out as providing, and provides, SUD diagnosis, treatment, or referral for treatment. Or (3) medical personnel or other staff in a general medical facility whose primary function is the provision of SUD diagnosis…."
- Programs must still obtain consent. However:
  - General consent is required, and recipients can re-disclose.
  - Disclosure allowed for TPO purposes and to covered entities and business associates.
  - Purpose was to facilitate care coordination. However, the amendments did not adopt the HIPAA standard for TPO.

20

Considerations for Compliant, Efficient Sharing of SUD PHI

- Review Patient Consent forms for Part 2 Compliance and Obtain Consent: Consent is still the best method to ensure compliant sharing of PHI.
- Organized Health Care Arrangement: An agreement defined under HIPAA intended to allow for sharing among providers in clinically integrated care settings and organized systems of health care. (§160.103).
- Qualified Service Organization Agreement: An individual or entity who: (1) provides services to part 2 program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population, health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child-care and individual and group therapy, and (2) has entered into a written agreement with a part 2 program."
  - Can be added to a Business Associate Agreement.

21

Promoting Access: Interplay between HIPAA & Information Blocking

22

HIPAA & Information Blocking

Information Blocking Generally

Information Blocking objective: Advance interoperability, support the access, exchange, and use of EHI and address occurrences of information blocking, which is:

- 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.

What about HIPAA?

HIPAA objective: Maximize protection of protected health information (PHI), while promoting individual access to PHI

Where disclosure or the requirements facilitating disclosure are permissive under HIPAA, Information Blocking requires disclosure of EHI.

23

HIPAA: Right of Access

Right to Access: Individuals have the right to their own PHI, subject to certain exceptions.

- Minimum Necessary Requirement not applicable
- Authorization is not required
- Timing of access - No later than 30 days
- Right to restrict access

HIPAA Proposed Rule:

- Timing - 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.
- Right to inspect and record PHI
- Prohibition of unreasonable verification measures

24

Information Blocking: Preventing Harm

The Actor must:

- Have a **reasonable belief** that denying the request **substantially reduces a risk of harm** to the person who is subject of EHI or another person.
- Ensure that the practice is no broader than necessary to substantially reduce the risk of harm
- Meet at least **one condition from each** of the following categories:
  - **Type of Risk**
    - Be determined on an individualized basis of the facts and circumstances in the exercise of professional judgment
    - Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.
  - **Type of Harm**
    - Consistent with reasons for denial under HIPAA
  - **Implementation Basis**
    - Organizational policy
    - Determination of risk of harm by licensed health care professional, which is subject to review

25

Preventing Harm: Type of Harm

Access, exchange, or use of patient's EHI	EHI for which access, exchange, or use is affected by the interfering practice is	Applicable type of harm[1]	Regulation Text References
Patient exercising own right of access	Patient's EHI	Danger to life or physical safety of the patient or another person	§ 171.201(d)(3), referencing HIPAA Privacy Rule § 164.524(a)(3)(i)
	Patient's EHI that references another person	Substantial harm[3] to such other person	§ 171.201(d)(2), referencing HIPAA Privacy Rule § 164.524(a)(3)(ii)
Patient's personal representative as defined in HIPAA Privacy Rule (45 CFR 164.502) exercising right of access to patient's EHI *(for example, parent of a minor child)*[2]	Patient's EHI	Substantial harm[3] to the patient or to another person	§ 171.201(d)(1), referencing HIPAA Privacy Rule § 164.524(a)(3)(iii)
	Patient's EHI that references another person	Substantial harm[3] to such other person	§ 171.201(d)(2), referencing HIPAA Privacy Rule § 45 CFR 164.524(a)(3)(ii)

*This table was created by ONC in response to FAQs, available here: https://www.healthit.gov/faq/?f%5B0%5D=multopic%3A7046.

26

Preventing Harm: Interplay with HIPAA

The Preventing Harm Exception's type of harm condition relies on the *same* types of harm that serve as grounds for reviewable denial of an individual's right of access under the HIPAA Privacy Rule.

- When is this exception used?
  - Delays in disclosures?
  - High risk?
  - Minors?
- What about HIPAA's right to restrict access?

27

Enforcement: Focus on Accessibility

Enforcement efforts focus on promoting access and exchange of EHI

- HIPAA Right of Access Initiative
  - OCR settlements
- Information Blocking Complaints
  - Majority submitted by patients against providers
  - Provider penalties

28