

June 26, 2024

HHS Finalizes Amendments to HIPAA Privacy Rule to Strengthen Privacy Protections for Reproductive Health Information Post-Dobbs

By Andrea Frey and Rachel Zacharias

Share:



On April 26, 2024, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) finalized a rule, entitled "HIPAA Privacy Rule to Support Reproductive Health Care Privacy" (hereinafter, the "Final Rule"), that amends the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to include specific privacy safeguards for reproductive healthcare information. ¹

The Privacy Rule, codified at 45 C.F.R. Part 160 and Subparts A and E of Part 164, establishes national standards to safeguard "protected health information" (PHI), which includes individuals' medical records and other individually identifiable health information. ² The Privacy Rule sets a floor of limits and conditions on the uses and disclosures of PHI, including those that may be made without the authorization of the individual to whom the information belongs. Entities regulated by the Privacy Rule, which includes health plans, clearinghouses, and healthcare providers who conduct certain healthcare transactions electronically, as well as their business associates, can face civil and criminal liability for failure to comply with the Privacy Rule.

The Final Rule amends the Privacy Rule to specifically require that regulated entities

may not disclose PHI that is sought for the purposes of investigating or imposing liability on individuals merely for seeking, obtaining, providing, or facilitating lawful reproductive healthcare. The Final Rule further requires regulated entities to obtain valid attestation from certain requestors that they are not seeking PHI for specified prohibited purposes and requires changes to covered entities' notice of privacy practices (NPP) to reflect the above requirements (and recent changes to 42 C.F.R. Part 2, if the covered entity is also a Part 2 program). Regulated entities have until December 23, 2024, to comply with the applicable requirements of the Final Rule, except that covered entities have until February 16, 2026, to update their NPPs.

This article discusses the justification for the amendments included in the Final Rule, provides a summary of the new obligations imposed on regulated entities, and provides practical takeaways for practitioners advising clients on compliance with the updated Privacy Rule.



Justifications and Context for the Final Rulemaking

The Final Rule comes in the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* and the subsequent patchwork of restrictive state abortion laws. **3** In an effort to enforce these restrictive laws, state prosecutors, law

enforcement agencies, as well as individuals exercising private rights of action will no doubt turn to patients' medical records and related health information to investigate or impose liability on patients, their providers, and their friends and family members for seeking, obtaining, providing, or facilitating reproductive healthcare. ⁴ In commentary to the Final Rule, the Office for Civil Rights (OCR) explained that “[n]ow that states have much broader power to criminalize and regulate reproductive choices—and that some states have already exercised that power in a variety of ways—individuals legitimately have a far greater fear that especially sensitive information about lawful healthcare will not be kept private.” ⁵ The Final Rule seeks to address such concerns that medical records will be used against individuals by bolstering protections for individuals providing or obtaining lawful reproductive healthcare.

Throughout the Final Rule, OCR explains the agency's goal of aiming to strike a balance between “the interests of the individual in the privacy of their PHI,” on the one hand, and accommodating on the other, “state autonomy to the extent consistent with the need to maintain rules for health information privacy that serve HIPAA's objectives.”

⁶ In seeking such a balance, the Final Rule presents a middle-ground approach in establishing a purpose-based prohibition to safeguard reproductive health information that would preempt contrary state law in narrow situations. OCR did not go as far as it arguably could have, however; for example, it could have established that reproductive health information itself is a new category of particularly sensitive PHI (similar to HIPAA's treatment of psychotherapy notes). ⁷ Nevertheless, as states continue to pass increasingly disparate laws regarding reproductive healthcare, compliance with the regulations may prove legally and practically challenging for regulated entities. For instance, regulated entities refusing to disclose may face conflicts between federal and state law, where a court order or health oversight agency requests PHI that HIPAA prohibits the regulated entity from disclosing, requiring the entity to challenge the request and potentially face consequences for refusing to turn over PHI.

Final Rule Amendments to the Privacy Rule

Creating a Purpose-Based Prohibition Against Certain Disclosures of Reproductive Healthcare Information and Presumption of Lawful Care

Under the Privacy Rule, at 45 C.F.R. § 164.502(a)(1)(iv), a regulated entity is generally permitted to use or disclose PHI pursuant to a valid authorization (*see* 45 C.F.R. § 164.508). ⁸ Without individual authorization, regulated entities are generally prohibited from using or disclosing PHI except as permitted or required by the Privacy Rule, including for certain law enforcement purposes under certain circumstances (*see*, e.g. 45 C.F.R. § 164.512(f)). ⁹ The Final Rule creates a new requirement, codified at 45 C.F.R. § 164.502(a)(5)(iii), that prohibits regulated entities from using or disclosing PHI for activities undertaken with the purpose of investigating or imposing criminal, civil, or administrative liability on any person “for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare” that is lawful under the circumstances in which it was provided, or activities to identify any person for such purposes. ¹⁰ This prohibition only applies to unauthorized disclosures of PHI; in light of public comments, HHS decided not to finalize a related proposal that would prohibit a regulated entity from using or disclosing PHI for the same specified purposes even when an individual authorizes such use or disclosure of their PHI. ¹¹

For what purposes are PHI disclosure prohibited?

The Final Rule makes clear that “the prohibition does not prevent the use or disclosure of the PHI about reproductive healthcare obtained by an individual in all circumstances.” ¹² Instead, the regulation prohibits the use or disclosure by a regulated entity of PHI “when the purpose of the [requested] disclosure is to investigate or impose liability ¹³ on a person because they sought, obtained, provided, or facilitated reproductive healthcare that was lawful under the circumstances in which such healthcare was provided.” ¹⁴

The prohibition is written to apply only where “individuals’ privacy interests outweigh the interests of law enforcement, and private parties afforded legal rights of action, in obtaining individuals’ PHI for the non-health care purpose of investigating or imposing liability for reproductive health care” where such care was lawfully provided. (15)

HHS reiterated that the Final Rule does not foreclose *all* methods to investigate the lawfulness of reproductive healthcare; for instance, the prohibition does not apply where a person requesting PHI identifies a (non-pretextual) legal basis for the request “beyond the mere act of a person having sought, obtained, provided, or facilitated reproductive healthcare,” nor does the prohibition apply where the reproductive healthcare was unlawful. (16) HHS clearly stated it “is not otherwise changing the existing permissions in the Privacy Rule that permit regulated entities to use or disclose PHI for law enforcement purposes and other important non-health care purposes.”

(17)

By way of example, the Final Rule provides that regulated entities would be prohibited from disclosing PHI sought for civil suits brought by individuals exercising private rights of action provided for under state law against individuals or healthcare providers who obtained, provided, or facilitated a lawful abortion. (18) Regulated entities would be similarly prohibited from disclosing PHI sought for a law enforcement investigation into a healthcare provider for lawfully providing or facilitating the disposal of an embryo at the direction of an individual. (19) An investigation into whether an abortion was necessary to save a pregnant person’s life would also constitute an investigation into the “mere act” of “seeking, obtaining, providing, or facilitating” reproductive healthcare, such that disclosure would be prohibited if the care was lawful. (20)

In contrast, the Final Rule provides that a regulated entity would not be prohibited from disclosing an individual’s PHI when subpoenaed by law enforcement for the purpose of investigating allegations of sexual assault by or of the individual (assuming law enforcement provided a valid attestation, *see* below, and met other necessary

conditions). (21) A regulated entity would also not be prohibited from disclosing PHI when it is sought to investigate or impose liability on a person for submitting a false claim for payment to the government for the provision of reproductive healthcare; when PHI is sought by a health oversight agency for oversight activities; when PHI is sought for an investigation into substandard medical care, patient abuse, or violations of nondiscrimination laws; or when it is requested by an Inspector General to conduct a Medicare or Medicaid audit. (22)

What does it mean for an individual to “seek, obtain, provide, or facilitate” reproductive healthcare?

“Seeking, obtaining, providing, or facilitating” is defined to include, but not be limited to, “expressing interest in, using, performing, furnishing, paying for, disseminating information about, arranging, insuring, administering, authorizing, providing coverage for, approving, counseling about, assisting, or otherwise taking action to engage in reproductive health care; or attempting any of the same.” (23)

How is the Legality of the Reproductive Healthcare at Issue Determined?

The Final Rule clarifies that the amended regulation encompasses and prohibits the use or disclosure of PHI for any activities conducted for the purpose of investigating or imposing liability on any person for applicable acts “that the regulated entity that has received the request for PHI has *reasonably determined is lawful* under the circumstances in which such health care is provided.” (24) Legality is determined by the law of the state in which the healthcare was provided and/or federal law (including the U.S. Constitution and relevant federal statutes, regulations, and policies). (25) The Final Rule is clear that it “in no way supersedes applicable state law pertaining to the lawfulness of reproductive health care.” (26)

To adhere to this reasonableness requirement, regulated entities “must evaluate the facts and circumstances under which the reproductive health care was provided,” which may include facts regarding the individual’s diagnosis and prognosis, the time and location at which such care was provided, and the particular healthcare provider who provided the care. (27) HHS recognizes that this approach may prevent uses or disclosures where a healthcare provider reasonably determines that its provision of reproductive healthcare was lawful, even when law enforcement disagrees, but believes that in these circumstances, “the interests of law enforcement and private parties afforded legal rights of action are outweighed by privacy interests.” (28)

The regulation includes a presumption provision, which requires regulated entities that receive a request for PHI that was provided by another person to presume that reproductive healthcare was lawful under the circumstances in which it was provided.

(29) This presumption can be overcome where the regulated entity has sufficient knowledge that the healthcare was not lawful under the specific circumstances in which it was provided, either because the regulated entity has actual knowledge or the person requesting the PHI supplies “factual information that demonstrates a substantial factual basis” that the care was not lawful. (30) HHS believes this presumption provision is necessary for workability, clarifying that “regulated entities are not expected to conduct research or perform an analysis of an individual’s PHI to determine whether prior reproductive health care was lawful under the circumstances.” (31)

How Does this Regulation Interact with State Privacy Laws?

The Final Rule maintained that, in cases in which the Privacy Rule (including these amendments) imposes greater restrictions on uses and disclosures of PHI than state privacy laws, “the provisions of the Privacy Rule would preempt the application of contrary provisions of state law, and the regulated entity could not disclose the PHI.”

Requirement for Signed Attestation

To facilitate compliance with the above prohibition while allowing appropriate disclosures of PHI to continue, the Final Rule also creates a new section, 45 C.F.R. § 164.509, that requires regulated entities obtain a signed and dated attestation from a requestor for PHI potentially related to reproductive healthcare for healthcare oversight activities, judicial and administrative proceedings, law enforcement purposes, and disclosures to coroners and medical examiners. (33) A valid attestation must be in plain language and must include the required elements as described in Section 164.509, such as a clear statement that the use or disclosure of PHI related to reproductive healthcare is not for a prohibited purpose and a statement that a person may be subject to criminal penalties if that person knowingly uses or discloses individually identifiable health information in violation of HIPAA. (34) The attestation generally cannot include an element or statement not specifically required or be combined with any other document, except for certain additional documents to support the information provided in the attestation. (35) Each use or disclosure request would require a new attestation. (36) Failure to obtain an attestation or disclosing PHI based on receipt of an attestation known to be defective may subject a regulated entity to liability under the Privacy Rule and give rise to breach notification obligations.

The Final Rule clarifies that covered entities and business associates are not required to investigate the validity of an attestation and can reasonably rely on the representations in the attestation if, under the circumstances, it determines “that the request is not for investigating or imposing liability for the mere act of seeking, obtaining, providing, or facilitating allegedly unlawful reproductive health care.” (37) However, a regulated entity cannot rely on a facially invalid attestation (e.g., where not all required elements

are included), or where the covered entity or business associate reasonably would not believe that the attestation is true or has actual knowledge that material information in the attestation is false. (38) For example, the Final Rule describes the following situation:

“A regulated entity receives an attestation from a Federal law enforcement official, along with a court ordered warrant demanding PHI potentially related to reproductive health care. The law enforcement official represents that the request is about reproductive health care that was not lawful under the circumstances in which such health care was provided, but the official will not divulge more information because they allege that doing so would jeopardize an ongoing criminal investigation.” (39)

In this situation, the Final Rule explains that where the regulated entity itself provided the reproductive healthcare and, “based on the information in its possession,” reasonably determines that such services were lawfully provided, “the regulated entity may not disclose the requested PHI.” (40) Where the regulated entity did not provide the reproductive healthcare, it also may not disclose the requested PHI absent additional factual information “because the official requesting the PHI has not provided sufficient information to overcome the presumption” that reproductive healthcare provided by another is presumed lawful. (41)

However, for example, where the official were to provide additional facts “for the regulated entity to determine that there is a substantial factual basis that the reproductive health care was not lawfully provided,” or where the official provides a sworn statement “that the PHI is necessary for an investigation into violations of specific criminal codes unrelated to the provision of reproductive health care (e.g., billing fraud),” the Final Rule states that the regulated entity would be permitted to make the disclosure in such instances. (42)

HHS intends to publish model attestation language before the compliance date of the

Final Rule. ⁴³

Mandatory updates to Notice of Privacy Practices

Under the Privacy Rule, a covered entity generally must provide individuals with a Notice of Privacy Practices (NPP) outlining individuals' rights and covered entities' duties regarding the use, disclosure, and protection of their PHI. ⁴⁴ In this Final Rule, HHS added a number of modifications to the HIPAA NPP requirements, which include modifications pertaining to reflect the above requirements as well as new requirements for covered entities that are also substance use disorder programs subject to 42 C.F.R. Part 2 (referred to as "Part 2 Programs" under the regulations) or that receive Part 2 records. ⁴⁵ (Earlier this year, HHS published the 2024 Part 2 Final Rule, which modified the Part 2-required Patient Notice to align more closely with HIPAA's NPP requirements. ⁴⁶)

Relevant to reproductive health information, the Final Rule requires that an NPP: (1) must include a statement explaining that disclosed PHI "may be subject to redisclosure and no longer protected by the Privacy Rule" ⁴⁷ and (2) must contain a sufficiently detailed description, with examples, of the types of uses and disclosures prohibited under the new purpose-based prohibition, and those requiring of an attestation. ⁴⁸

Other Proposed Changes

Clarification of terms and definitions

To facilitate the implementation of the amendments discussed above, the Final Rule adds and clarifies certain terms and definitions to the Privacy Rule:

- For example, the Final Rule clarifies that the term "person," as defined by HIPAA and its implementing regulations, does not include a fertilized egg, embryo, or fetus. The definition of "person" refers only to a "natural person (meaning a human being

who is born alive), trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.” ⁴⁹

- The regulations also refine the term “public health,” as used in “public health surveillance,” “public health investigation,” and “public health intervention,” to mean *population-level* activities “to prevent disease in and promote the health of populations.” ⁵⁰ This definition expressly carves out the collection of PHI for the purpose of investigating or prosecuting individuals involved in reproductive healthcare.
- The Final Rule also adds the term “reproductive health care” to the Privacy Rule as a subcategory of the existing term “health care.” “Reproductive health care” is broadly defined as healthcare “that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes.” ⁵¹ The Final Rule’s preamble includes a “non-exclusive list of examples” of “reproductive health care” to help regulated entities evaluating what information would fall within the Final Rule’s scope. ⁵² Notably, the term is not confined to a specific gender or age of an individual, nor is it tied to any specific set of codified information.

Administrative requests

In addition to setting forth additional safeguards with respect to the privacy of reproductive healthcare information, OCR also amended 45 C.F.R. Section 164.512(f)(1)(ii)(C) to permit disclosures in response to an administrative request only “for which response is required by law.” According to OCR, the clarification is necessary as some covered entities interpreted that any written request from law enforcement that contains certain required statements was sufficient for disclosure of PHI, so long as the law enforcement official was acting within their legal authority. Under the so-called clarifying amendments, disclosure in response to administrative requests from law enforcement will only be permissible if the covered entity is mandated by law to

respond to the request. Notably, this update is not limited just to PHI containing reproductive healthcare information, but rather applies broadly to all PHI requested by law enforcement.

Practical Takeaways

Practitioners advising regulated entities are encouraged to familiarize themselves with the updated regulations to help guide such clients navigating compliance with the Final Rule prior to the December 23, 2024, deadline. For example, covered entities and business associates will need to carefully evaluate what information they collect and maintain to determine whether it relates to reproductive healthcare and therefore subject to the new requirements. Operationally, regulated entities may need to implement mechanisms to identify, tag, and/or segment such data to appropriately safeguard PHI relevant to reproductive health information and prevent disclosures of PHI for prohibited purposes (or verify that an appropriate attestation is in place). This may also require updates to existing Business Associate Agreements to reflect the new protections under the Final Rule. Additionally, regulated entities will need to revise and post their NPPs and update their internal privacy policies and procedures to address the disclosure prohibition and attestation requirements. Along those lines, an attestation template will need to be adopted and administered in accordance with the Final Rule. To ensure the new requirements are successfully carried out by workforce members, regulated entities should also provide compliance training that carefully details the Final Rule's limitations on disclosures of PHI and the new attestation form requirement. Finally, regulated entities operating in states with restrictive abortion laws should be mindful of the enforcement environment and prepare for challenges from law enforcement and oversight agencies if the Final Rule prohibits disclosure of PHI.

Authors



Andrea Frey

Hooper, Lundy & Bookman, P.C., San Francisco, CA

Andrea Frey is a partner in the San Francisco office of Hooper, Lundy & Bookman, and co-chair of the firm's reproductive health and digital health practices. She specializes in digital health, technology, and data sharing issues, and regularly supports healthcare clients navigating the complex web of federal and state laws that govern the exchange of health information, such as HIPAA. She can be reached at afrey@hooperlundy.com

Rachel Zacharias

Hooper, Lundy & Bookman, P.C., Washington, DC

Rachel Zacharias is an associate in the Washington, DC, office of Hooper, Lundy & Bookman, focusing on litigation and regulatory matters involving Medicare and Medicaid reimbursement, medical ethics and consent, patient privacy, organ donation, clinical research, and reproductive health. She can be reached at rzacharias@hooperlundy.com.

Endnotes



ENTITY:

HEALTH LAW SECTION

TOPIC:

HEALTH

The material in all ABA publications is copyrighted and may be reprinted by permission only. Request reprint permission [here](#).

ABA American Bar Association

[/content/aba-cms-dotorg/en/groups/health_law/publications/health_lawyer_home/june-2024/hhs-finalizes-amendments-to-hipaa-privacy-rule-to-strengthen-privacy-protections-for-reproductive-health-information-post-dobbs](https://www.americanbar.org/groups/health_law/publications/health_lawyer_home/june-2024/hhs-finalizes-amendments-to-hipaa-privacy-rule-to-strengthen-privacy-protections-for-reproductive-health-information-post-dobbs)