

July 11, 2024

# HHS Finalizes New HIPAA Privacy Protections for Reproductive Health Care

In late April, the U.S. Department of Health and Human Services (HHS), acting on behalf of the Biden Administration, published [final HIPAA Privacy regulations](#) for reproductive health care (the “final rules”).

The final rules provide new protections to prevent uses or disclosures of information related to abortion services that may cause harm to the interests that HIPAA seeks to protect, including the trust of individuals in health care providers, their health plans, and the health care system.

This Alert: (i) provides a quick refresher on some HIPAA basics; (ii) discusses the federal government’s concern and basis for the final rules; (iii) addresses the new HIPAA Privacy protections for reproductive health care; and (iv) identifies the actions certain employers as plan sponsors must take to comply. This Alert is relevant for all employers, but it is most relevant for employers sponsoring self-insured medical plans.

## Some HIPAA basics

At a high level, the HIPAA Privacy and Security rules apply to *protected health information* (PHI) maintained, used, and/or disclosed by *covered entities* and their *business associates*.

- **Protected health information** is information identifiable to a specific individual about: (i) a past, present, or future health condition, (ii) treatment for a health condition, or (iii) payment for treatment of a health condition. This information must be maintained, used, and/or disclosed by a covered entity or a business associate acting on behalf of the covered entity. The manner or format in which the information is maintained or disclosed does not matter.
- **Covered entities** are: (i) health care providers who conduct certain standard electronic transactions (e.g., billing); (ii) health plans;<sup>1</sup> and (iii) health care clearinghouses.

---

<sup>1</sup> A self-insured health plan is generally subject to all of HIPAA’s compliance obligations (the plan administrator usually addresses this on behalf of the plan). The HIPAA

## Highlights

### Overview

In late April, HHS published final HIPAA Privacy regulations providing new privacy protections related to reproductive health care.

This Alert is relevant for all employers, but it is most relevant for employers sponsoring self-insured group health plans.

### Key Provisions

The new protections generally

- Prohibit the use or disclosure of PHI related to lawful reproductive health care to punish the parties involved in the care; and
- Limits other uses or disclosures of PHI related to lawful reproductive health care.

### Employer action items

Employers sponsoring self-insured medical plans must:

- Update their HIPAA Privacy and Security materials (including reviewing business associate agreements) by December 23, 2024; and
- Update their HIPAA notices of privacy practices by February 16, 2026.

Employers sponsoring fully insured medical coverage that have access to PHI may need to take similar action.

- **Business associates** are third parties that require PHI to perform some function or service on behalf of a group health plan. The third party might create, receive, store, or transmit PHI in this role, but it must be “PHI sticky” in at least one of these ways to be considered a business associate.

While the final rules apply to all covered entities and business associates, the remainder of this Alert will focus on the rules as they related to employer-provided group health plans.

## The federal government’s concern

The existing HIPAA regulations allow a covered entity or business associate to disclose PHI without a participant’s authorization to comply with federal or state law for a variety of purposes, including: (i) to report abuse, neglect, or domestic violence, (ii) for judicial or administrative proceedings, and (iii) upon request by law enforcement if certain conditions are met.<sup>2</sup>

HIPAA does not require the disclosure of PHI in these situations, but covered entities and business associates may be unaware of this, feel pressured to comply, or believe they are at some risk if they fail to do so. The federal government also believes this uncertainty about the privacy of their information may have a chilling effect that keeps individuals from seeking reproductive health care for fear of prosecution or other liability. HHS expressed concern that individuals residing in a state broadly prohibiting or restricting abortion may be afraid to have the procedure in another state where it is legal if information about the procedure might be shared with authorities in their home state.<sup>3</sup>

The final rules attempt to address this concern through new HIPAA Privacy protections for reproductive health care.

## New HIPAA Privacy protections

The final rules implement the new HIPAA Privacy protections for reproductive health care by:

1. Defining reproductive health care;
2. Prohibiting the use or disclosure of PHI related to lawful reproductive health care for civil, criminal, or administrative proceedings to punish the parties involved in the care (the “general restriction”); and
3. Requiring an attestation from the party requesting the PHI for other certain uses or disclosures of PHI related to lawful reproductive health care (the “attestation rule”).

The compliance effective date is **December 23, 2024**, but the final rules do not require corresponding updates to the HIPAA notice of privacy practices until **February 16, 2026**.

## Reproductive health care

**Reproductive health care** means health care that affects the health of an individual in all matters relating to the reproductive system, its functions and processes, and includes:

- Abortion-related services,
- Contraceptive services,
- Fertility services, and
- Other procedures performed on the reproductive system.<sup>4</sup>

---

compliance obligations for a fully insured health plan generally belong to the insurance carrier if the employer/plan sponsor is “hands off” PHI related to the plan. Further discussion of “hands on/hands off” PHI status is beyond the scope of this Alert.

<sup>2</sup> 45 CFR §164.512(a), (c), (e), and (f).

<sup>3</sup> Preamble to HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 89 Fed. Reg. 32978 (April 26, 2024).

<sup>4</sup> 45 CFR §160.103.

This definition gives the new HIPAA Privacy protections broad reach, but the federal government's immediate goal is clear. The word "abortion" does not appear in the regulations, but it appears 63 times in their preamble. By contrast, "fertility" and "infertility" appear a combined 7 times.

## The general restriction

Under the general restriction, a covered entity or business associate **cannot** use or disclose PHI related to "lawful" reproductive health care for:

1. A criminal, civil, or administrative investigation into any person for seeking, obtaining, providing, or facilitating reproductive health care;
2. To impose any criminal, civil, or administrative liability against any person for seeking, obtaining, providing, or facilitating reproductive health care; or
3. To identify any person for the purposes of 1 or 2.<sup>5</sup>

Reproductive health care is lawful if: (i) the services were legal in the state where performed; and/or (ii) the services are otherwise protected by federal law.<sup>6</sup> The final rules require a covered entity or business associate to assume that reproductive health care services were lawful unless they have actual knowledge or substantial evidence that they were not.<sup>7</sup>

### Not domestic violence, abuse, or neglect

The final rules make clear that lawful reproductive health care obtained by an individual is not a form of abuse, neglect, or domestic violence reportable to authorities or usable as a basis to reject a person as an individual's personal representative.

**Note:** The general restriction does not apply to unlawfully obtained reproductive health care, which may allow the covered entity or business associate to make the disclosure.

## The attestation rule

If a covered entity or business associate receives a valid attestation from a party requesting PHI that meets certain requirements (see *Requirements for a valid attestation* below), the attestation rule allows – but does not require – a covered entity or business associate to use or disclose PHI related to reproductive health care without the participant's authorization for:

- a health oversight activity conducted by a federal or state/local agency;
- a judicial or administrative proceeding;
- a law enforcement purpose; or
- for a matter related to a deceased person.<sup>8</sup>

The covered entity or business associate must receive the completed attestation before the use or disclosure of the requested PHI. Among other items, the attestation must certify that the use or disclosure is not for or related to a

<sup>5</sup> 45 CFR §164.502(a)(5)(iii)(A).

<sup>6</sup> 45 CFR §164.502(a)(5)(iii)(B). An example of reproductive health care protected by federal law includes certain women's contraceptive services covered under the Affordable Care Act's preventive services mandate for non-grandfathered plans. This language may anticipate future federal protection.

<sup>7</sup> 45 CFR §164.502(a)(5)(iii)(C).

<sup>8</sup> 45 CFR §164.509(a).

criminal, civil, or administrative matter related to the reproductive health care that violates the general restriction.

### Requirements for a valid attestation

The attestation must be written in plain language and include the following elements:

- A description of the requested PHI that identifies the affected individual or class of individuals;
- The party or parties requested to make the disclosure;
- The party or parties who will receive the requested PHI;
- A clear statement that the use or disclosure will not violate the general restriction;
- A statement that criminal penalties apply for knowingly violating the protections; and
- The signature of the party (or the party's representative) requesting the disclosure and date.<sup>9</sup>

The regulations allow for electronic attestations and generally require attestations to be standalone documents. HHS published a [model attestation](#), and a copy is attached to this Alert.

### Example of attestation rule in practice

Following a series of patient complaints, a state medical board reviews whether a physician is meeting the state's standard of medical care. The board requests PHI from an employer's medical plan related to a participant's recent failed reproductive health care procedure solely for this purpose. If the plan receives a valid attestation, it may disclose the requested PHI to the state medical board in this situation.<sup>10</sup>

## Updated HIPAA notice of privacy practices

The final rules require certain updates to HIPAA notices of privacy practices (NPPs), including:

- A description of the general prohibition on unauthorized disclosures of reproductive health care PHI with at least one example;
- A description of the uses and disclosures allowed under an attestation with at least one example; and
- A statement that PHI may lose its "protected" status once disclosed to a third party.

HHS will publish updated model NPPs (in various formats) in the future but did not provide an expected delivery date. We expect many covered entities will wait for the models prior to updating their own NPPs for consistency purposes. As a reminder, the due date to update NPPs is **February 16, 2026**.

**Why February 16, 2026?** Earlier HIPAA regulations related to substance use disorder PHI require changes to NPPs by February 16, 2026. Those changes generally affect health care providers more than group health plans. HHS chose the same due date for the required reproductive health care NPP updates for administrative convenience.

## Employer action

Employers sponsoring self-insured medical plans that are covered entities for HIPAA purposes<sup>11</sup> should review the final rules with their legal advisors and/or HIPAA subject matter experts and complete the following actions by or before December 23, 2024:

<sup>9</sup> 45 CFR §164.509(c).

<sup>10</sup> The participant could also directly authorize the plan to release the PHI and would obviously do so or self-disclose the PHI in a lawsuit against the health care provider.

<sup>11</sup> This includes fully insured plans if the plan sponsor/plan administrator has access to PHI (i.e., is "hands on" PHI).

1. Update their existing HIPAA Privacy & Security policies and procedures as necessary to reflect the new HIPAA Privacy protections for reproductive health care;
2. Update their HIPAA training materials to reflect the new protections and conduct training for the covered entity workforce;
3. Review existing business associate agreements to determine whether any revisions are necessary to reflect the new protections;<sup>12</sup> and
4. Adopt a compliant attestation form (a copy of the HHS model attestation is attached to this Alert) for use if the plan receives a request for reproductive health care PHI.

Employers should also work with their legal advisors and/or HIPAA subject matter experts to update their HIPAA notices of privacy practices by or before February 16, 2026.<sup>13</sup>

Finally, affected employers may wish to discuss with their legal advisors in advance how to challenge or respond to requests for disclosures of PHI that may violate the final rules. In general, we recommend slowing down and assessing requests for reproductive health care PHI since nothing under the HIPAA Privacy rules compel a group health plan to disclose this information.

## Enforcement

A party, including a state legal authority, who knowingly violates the new HIPAA Privacy protections is subject to criminal penalties, including both financial penalties and potential imprisonment.<sup>14</sup> The U.S. Department of Justice enforces criminal violations of HIPAA on behalf of HHS.

A covered entity (including a group health plan) or business associate that fails to obtain a valid attestation before making a disclosure subject to the attestation rule is subject to potential civil penalties assessable by HHS.<sup>15</sup>

## Legal challenge?

Several states commented that they feel the final rules exceed HHS's authority. For example, does HHS have the authority to enforce violations of the new HIPAA Privacy protections against state authorities? At this time, it is not clear if one or more states will challenge the regulations.

---

<sup>12</sup> The language of an existing business associate agreement may be broad enough that no revision is necessary.

<sup>13</sup> Marsh McLennan Agency is comfortable referring clients to [HIPAA10](#) (also available through [CXC Solutions](#)).

<sup>14</sup> 42 U.S.C. §1320d-6.

<sup>15</sup> 42 U.S.C. §1320d-5.

## About the author



**Christopher Beinecke, J.D., LL.M.** is the Employee Health & Benefits National Compliance Leader for Marsh McLennan Agency.

The information contained herein is for general informational purposes only and does not constitute legal or tax advice regarding any specific situation. Any statements made are based solely on our experience as consultants. Marsh McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. The information provided in this alert is not intended to be, and shall not be construed to be, either the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the agency, our lawyers or our clients. This is not legal advice. No client-lawyer relationship between you and our lawyers is or may be created by your use of this information. Rather, the content is intended as a general overview of the subject matter covered. This agency is not obligated to provide updates on the information presented herein. Those reading this alert are encouraged to seek direct counsel on legal questions. © 2024 Marsh McLennan Agency LLC. All Rights Reserved.

# Model Attestation for a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care

The entire form must be completed for the attestation to be valid.

**Name of person(s) or specific identification of the class of persons to receive the requested PHI.**  
*e.g., name of investigator and/or agency making the request:*

**Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure.**

*e.g., name of covered entity or business associate that maintains the PHI and/or name of their workforce member who handles requests for PHI:*

**Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals, whose protected health information you are requesting.**

*e.g., visit summary for [name of individual] on [date]; list of individuals who obtained [name of prescription medication] between [date range]*

I attest that the use or disclosure of PHI that I am requesting is not for a purpose prohibited by the HIPAA Privacy Rule at 45 CFR 164.502(a)(5)(iii) because of one of the following (check one box):

- The purpose of the use or disclosure of protected health information is not to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes.
- The purpose of the use or disclosure of protected health information is to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was not lawful under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person.

*Signature of the person requesting the PHI:*

Date: \_\_\_\_\_

If you have signed as a representative of the person requesting PHI, provide a description of your authority to act for that person.

*This attestation document may be provided in electronic format, and electronically signed by the person requesting protected health information when the electronic signature is valid under applicable Federal and state law.*