GROOM LAW GROUP

Publications

Reproductive Health Care: New HIPAA Restrictions & Compliance Checklist

ATTORNEYS & PROFESSIONALS

Katelyn Davis
kdavis@groom.com
202-861-6632

Elizabeth LaPaugh
elapaugh@groom.com
202-861-6606

Christy Tinnes
ctinnes@groom.com
202-861-6603

Viv Hunter Turner
vturner@groom.com
202-861-6324

Joel Wood
jwood@groom.com
202-861-6656

PUBLISHED

09/09/2024

SOURCE

Groom Publication

SERVICES

Health Services

Privacy & Security

Earlier this year, the Department of Health & Human Services Office of Civil Rights ("HHS") published a final "HIPAA Privacy Rule to Support Reproductive Health Care Privacy" that imposes new restrictions on disclosure of protected health information ("PHI") related to lawfully provided "reproductive health care" services. The new rule is applicable December 23, 2024. The rule defines "reproductive health care" broadly as health care that affects the health of an individual in all matters relating to the reproductive system and its functions and processes.

HIPAA covered entity health plans and business associates will have several "to do" items to prepare for the new rule.

- The primary "to do" items – updates to HIPAA procedures, training, and (in some cases) business associate agreements – must be in place by **December 23, 2024**.
- The final "to do" item – update and issue a revised HIPAA Privacy Notice – is due **February 16, 2026**.

Below we provide an overview of the new rules with Groom Insights, along with a detailed Compliance Checklist with practical tips.

BREAKING NEWS

On September 4, 2024, the State of Texas brought a legal challenge in the Northern District of Texas to the new HIPAA rule, along with the validity of the original HIPAA privacy rules. *Complaint State of Texas v. Dep't. of Health & Human Servs. (N.D. Tex. 2024) (E.C.F. 5:24-cv-00204-H).* Among other claims, Texas asserts that HHS exceeded its statutory authority in adopting both sets of rules and that covered entities already have cited to both when refusing to disclose reproductive health care information pursuant to a Texas subpoena. Texas further states that the term "reproductive health care" is "clearly meant to encompass abortion, hormone and drug therapy for gender dysphoria, surgical procedures related to gender dysphoria, and gender experimentation." We note that, although commenters to the proposed rule asked HHS to provide greater clarification on the types of care, services, or supplies that should be included within the scope of "reproductive health care" (including gender affirming care), HHS said it declined to do so to "avoid the impression of creating a complete list." The new rule turns on the underlying condition that is being treated (rather than the type of service provided), and HHS acknowledged that it may be challenging to identify the full scope of services that would be covered by the new rule. Texas asks that the court vacate both the new HIPAA reproductive health care final rule, as well as the entire original HIPAA privacy rules issued in 2000, and enjoin HHS from enforcing these rules. The Northern District of Texas may sound familiar, as this is the court that has overturned a number of health-related mandates, including, recently, the app tracking guidance that HHS issued under the HIPAA privacy rules (*American Hospital Association v. Becerra*) and much of the ACA preventive care rule (*Braidwood v. Becerra*).

Background

The HIPAA Privacy Rules apply to HIPAA covered entities, which include health care providers and health plans that access an individual's protected health information ("PHI"). A health plan is defined to include an employer group health plan, as well as a health insurance issuer offering individual or group coverage. HIPAA also applies to a business associate, which is a service provider that performs functions on behalf of a covered entity involving PHI. Under HIPAA, a covered entity and business associate may not use or disclose PHI without an individual's HIPAA authorization, except for purposes of treatment, payment, or health care operations, or under an express exception listed in the HIPAA Privacy Rules.

The new final reproductive health care rule addresses questions HIPAA covered entities and business associates have had regarding whether and when HIPAA prohibits the disclosure of PHI as part of an investigation into an individual's receipt of reproductive health care services, such as abortion-related treatment. In particular, HIPAA covered entities and business associates have had concerns that a state or other third party might seek information from a health care provider, employer group health plan, or health insurer about the provision of, facilitation of, or payment for reproductive health care services as part of a law enforcement investigation or judicial subpoena.

As discussed below, the final rule includes two key elements: (1) a general prohibition against using or disclosing PHI as part of an investigation into or to impose liability related to reproductive health care services that were lawfully provided; and (2) a requirement to obtain an attestation for requests for PHI potentially related to reproductive health care under certain HIPAA exceptions. The final rule also requires HIPAA covered entities to update their HIPAA privacy notices to alert individuals of these new rules, along with other rules HHS issued earlier this year related to substance use disorder information under 42 C.F.R. Part 2.

How is "Reproductive Health Care" ("RHC") defined?

The final rule defines "reproductive health care" as health care that affects the health of an individual in all matters relating to the reproductive system and its functions and processes. The preamble to the final rule clarifies that RHC includes the "full range of health care related to an individual's reproductive health" and provides a "non-exclusive list" of examples that HHS says fits within the definition, including:

- contraception;
- pre-conception screening and counseling;
- management of pregnancy and pregnancy-related conditions, including pregnancy screening, prenatal care, miscarriage management, treatment for preeclampsia, hypertension during pregnancy, gestational diabetes, molar or ectopic pregnancy, and pregnancy termination;
- fertility and infertility diagnoses and treatment, including assisted reproductive technology and its components (e.g., IVF);
- diagnosis and treatment of conditions that affect the reproductive system (e.g., perimenopause, menopause, endometriosis, and adenomyosis); and
- other types of care related to the reproductive system, (e.g., mammography, pregnancy-related nutrition services, and postpartum care products).

> **Groom Insight**: The final rule extends beyond requests for information about abortion-related treatment. Covered entities and business associates should carefully review any request for PHI that may be related to the diagnosis and/or treatment of conditions that affect the reproductive system, which may include a wide range of services.

Step #1: General Prohibition on Disclosing RHC Information

The final rule prohibits HIPAA covered entities and business associates from using or disclosing an individual's PHI to conduct a criminal, civil, or administrative investigation against, to impose liability against, or seek to identify a person for the "mere act of seeking, obtaining, providing, or facilitating" RHC that was lawfully provided ("General Prohibition").

Breaking this new rule down, the General Prohibition applies to a request for PHI: (1) that is related to a criminal, civil, or administrative investigation against a person; (2) where the person is being investigated for the "mere act" of seeking, obtaining, providing, or facilitating RHC; and (3) where the RHC was lawfully provided (as described below).

> **Groom Insight:** The General Prohibition applies to both HIPAA covered entities and business associates. So, a business associate is directly liable under these rules, not just contractually liable under the business associate agreement.

The final rule explains the scope of the General Prohibition by providing examples of activities that fall under the "mere act of seeking, obtaining, providing, or facilitating" RHC.

The final rule says these activities include, but are not 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 RHC.

> **Groom Insight:** The preamble clarifies that the General Prohibition only applies where a person is being investigated for the "mere act" of seeking, obtaining, providing, or facilitating RHC. The preamble states that the prohibition does not apply in other circumstances, such as an investigation into a participant's fraudulent claim or a covered entity's violation of federal nondiscrimination laws. These types of investigations would not be for the "mere act" of seeking, obtaining, providing, or facilitating RHC. The General Prohibition also would not apply to the routine processing of claims.

When is RHC considered to be lawfully provided?

The General Prohibition only applies where the HIPAA covered entity or business associate that receives the request for PHI reasonably determines that the RHC: (1) was lawful under the state in which the care was provided under the circumstances in which it was provided; or (2) was protected, required, or authorized by federal law under the circumstances under which it was provided. The preamble provides that whether a determination is "reasonable" is based on facts and circumstances.

Under the final rule, RHC will be *presumed to be lawfully provided* unless the covered entity or business associate has:

- "actual knowledge" that care was not lawful under the circumstances in which it was provided; or
- factual information supplied by the requesting party that demonstrates a "substantial factual basis" that the RHC was not lawful under the specific circumstances in which was provided.

> **Groom Insight:** The preamble states that covered entities and business associates may rely on the presumption that RHC was lawfully provided unless they have actual knowledge otherwise, such as the requesting party providing a "substantial factual basis" that the RHC was not lawful. However, the preamble expressly states that covered entities are "not expected to conduct research or perform an analysis of an individual's PHI" to determine whether RHC was lawful under the circumstances in which it was provided.
>
> Note that the presumption does not apply to the party that actually provides the care, although the underlying "reasonableness" determination as to whether the provision of care was lawful would continue to apply.

Step #2: Additional Attestation Requirement for Certain Exceptions

In addition to the General Prohibition discussed above, if the request for PHI falls under one of the four exceptions below ("Attestation-Required Exceptions"), and the request potentially relates to RHC information, the requesting party must provide an attestation that it is not using the PHI for a prohibited purpose. In other words, the requesting party must attest that it is not using the PHI to investigate the provision of RHC, or if it is making such an investigation, that the investigation relates to RHC that was not lawfully provided.

The Attestation-Required Exceptions are:

- disclosures for health care oversight (45 CFR 164.512(d));
- disclosures for judicial or administrative proceedings, including subpoenas (45 CFR 164.512(e));
- disclosures for law enforcement purposes (45 CFR 164.512(f)); and
- disclosures to a coroner or medical examiner about a deceased individual (45 CFR 164.512(g)(1)).

The final rule provides that the attestation must be stand-alone with certain content and signed by the requesting party. If a HIPAA covered entity or business associate discovers information reasonably showing that a representation made in the attestation is materially false, leading to a prohibited disclosure, the covered entity or business associate must cease using or disclosing the PHI for the purpose requested in the attestation.

HHS has issued a model attestation.

Note that covered entities and business associates may disclose PHI related to RHC services without an attestation under the other exceptions allowed by HIPAA, but the General Prohibition analysis still would apply. For example, under the "required by law" exception (45 CFR 164.512(a)), a covered entity or business associate may disclose PHI if the law: (1) mandates such use or disclosure of PHI; and (2) is enforceable in a court of law, provided the PHI disclosed is limited to the relevant requirements of such law and the General Prohibition does not preclude the disclosure.

> **Groom Insight:** The attestation requirement is on top of the General Prohibition outlined in Step #1. If a request falls under one of the above Attestation-Required Exceptions, the HIPAA covered entity or business associate also must analyze whether the General Prohibition applies. If the General Prohibition applies, the requested PHI cannot be disclosed, *even if an attestation has been provided*.
>
> The preamble is clear that a covered entity or business associate cannot rely solely on the attestation, but may need additional information – separate and distinct from the attestation itself – to determine that the disclosure is permitted under the General Prohibition as well. For example, this could be additional evidence from the requesting party that the RHC was not lawfully provided so does not trigger the General Prohibition.

What other HIPAA considerations apply?

A covered entity's or business associate's determination that the General Prohibition does not apply does not mean that it necessarily is free to disclose the PHI. Other HIPAA restrictions may still apply. For example, the disclosure still must fall under treatment, payment, health care operations, or an allowed exception. The covered entity or business associate needs to review the specific requirements of these definitions or exceptions to make sure they fit.

In addition:

- If the request falls under the four Attestation-Required Exceptions for health care oversight, judicial or administrative proceedings, law enforcement, or to a coroner or medical examiner, the covered entity or business associate must make sure that attestation requirement is met.
- If the request falls under any of the HIPAA allowed exceptions (including the four Attestation-Required Exceptions), the covered entity or business associate must keep an accounting of the disclosure – the individual has a right to request an accounting of disclosures outside of treatment, payment, and health care operations disclosures.
- The general rule that a covered entity only disclose the "minimum necessary" amount of PHI necessary to accomplish the intended purpose still applies to all of these disclosures, so the covered entity and business associate should be careful how much PHI it is disclosing.

Groom Insight: Even if the General Prohibition does not apply, HIPAA does not necessarily require that the covered entity or business associate must disclose the requested PHI. HIPAA only mandates that a covered entity or business associate must disclose PHI if to the Secretary of HHS as part of an investigation or to the individual under the individual's right to access request. The covered entity or business associate could decide not to disclose the requested PHI for other reasons, such as to protect enrollees' information that it promised would remain confidential. While there may be other legal considerations for not disclosing the PHI, such as an enforcement action for failing to comply with a subpoena, it would be another law, not HIPAA, that would require that disclosure.

Updates to HIPAA Privacy Notices

The final rule requires HIPAA covered entities to update their HIPAA privacy notices to inform individuals about these new restrictions, including:

- A description and example of the types of uses and disclosures where the new prohibition applies;
- A description and example of the types of uses and disclosures where attestation will be required; and
- Additional requirements and restrictions specifically related to substance use disorder patient records that were adopted in final rules issued earlier this year under 42 CFR Part 2.

The final rule includes a checklist of the content of the updated HIPAA privacy notice, including re-stating the existing requirements and adding the new requirements. HHS has not indicated whether it will issue sample language.

The applicability date to issue updated HPAA privacy notices is February 16, 2026.

Groom Insight: The delayed applicability date for the HIPAA privacy notice update is because the update includes information about new requirements under the Part 2 rules related to substance use disorder information. The changes to the Part 2 rules are not applicable until February 16, 2026, and HHS decided to only make one required update for both rules.

Health plans should think through when to issue the updated notice. A lot can happen between now and 2026 – including legal challenges, an election, and possible additional guidance or sample language – so health plans may want to hold off until closer to 2026 to draft or issue their updated notices to avoid having to send a second update with clarifications or retractions.

Compliance Checklist

Due Date	To Do	Explanation & Groom Practical Tips
12/23/24	HIPAA Privacy Procedures	The General Prohibition and attestation requirements apply as of 12/23/24. Covered entities and business associates should implement procedures to comply with the final rule and update their HIPAA Privacy & Security Procedures accordingly, as required under HIPAA. 45 CFR 164.530(i)(3). <u>Groom Practical Tips</u>: *We have been helping clients update their HIPAA Privacy & Security Procedures to add these new requirements. This includes discussions about whether it will be the health plan or business associate that will field these requests, make determinations regarding whether RHC was lawfully provided, and obtain attestations.* *Since there is some uncertainty whether there could be changes to the rule due to legal challenges and the November election, health plans and business associates may want to add the new procedures as a "snap-on" section or appendix that can be easily updated if needed.*

12/23/24	Business Associate Agreement (BAA)	The final rule does not expressly require that the BAA be updated, and BAAs generally require that the business associate comply with HIPAA, which would include the new rule. So, whether a BAA update is required will depend on the terms of the current BAA and the decisions made by the parties. Health plans and business associates may want to update their BAAs to include the new rule and clarify which party will be responsible for making a determination as to whether a disclosure is permitted or prohibited, which party will obtain attestations, and whether the health plan wants to be notified of or have the right to prior approval of a disclosure of RHC information. <u>*Groom Practical Tips*</u>*: We have been helping health plans and business associates facilitate discussions about the new requirements so each of them knows which party has what responsibility and when to involve each other in decision- making. Also, not every business associate may understand how these rules could apply to them, so the health plan may use this opportunity to make sure the business associate realizes its role.* *Since a BAA update is not expressly required, the health plan and business associate could at least make sure they have the same understanding as to which party will be taking on which responsibilities under the new rule. The parties could document these responsibilities when they next renew their BAA or when they enter into a new BAA.*
12/23/24	HIPAA Privacy Training	HIPAA requires that a covered entity provide training to each member of its workforce whose functions are affected by a material change in the HIPAA policies or procedures within a reasonable time after the material change becomes effective. 45 CFR 164.530(b)(2)(C). Business associates also should update their HIPAA training to reflect the new rule. If a health plan or business associate discloses PHI in violation of these requirements, that could be considered a HIPAA breach, so it would be important to ensure that workforce members are trained on these new procedures. <u>*Groom Practical Tips*</u>*: We have been helping health plans and business associates add slides to their existing training to make workforce members aware of these new rules and/or draft more robust one-time training updates to address the new rule. How detailed the training is generally depends on how involved the health plan or business associate is in the decision-making and analysis related to the new rule.* *At the least, workforce members should be able to identify a request for PHI related to RHC so that they can make sure it is flagged and forwarded to the Privacy Officer or other party with responsibility to analyze and act on these requests.*

2/16/26	HIPAA Privacy Notice	Covered entities will need to update their HIPAA Privacy Notices to reflect the new RHC rules, along with the Part 2 rules. The final rule has a checklist of the content that must be included in the update. *Groom Practical Tips: Only health plans that currently issue a HIPAA Privacy Notice must send the update. Under existing rules, group health plans that are fully insured and that do not access PHI may rely on the insurer to provide the HIPAA Privacy Notice. 45 CFR 164.520(a)(3)(iii). That rule has not changed, so these fully insured group health plans can continue to rely on their health insurer to send the updated HIPAA Privacy Notice. These insurers must send the updated HIPAA Privacy Notice by 2/16/26. For self- funded health plans or fully insured plans that do not fall under the exception allowing the insurer to send the Notice, the health plan must send the updated HIPAA Privacy Notice by 2/16/26.* *Many health plans include the HIPAA Privacy Notice in enrollment materials, their SPD, or other annual mailings. Health plans that issue these materials during Open Enrollment for a calendar year would need to have their updated HIPAA Privacy Notice ready in the fall of 2025 to be included in the enrollment materials for the 2026 plan year. Health plans with non- calendar years should consider whether they can include their updated HIPAA Privacy Notice in their annual mailings or if they may need an additional delivery method prior to 2/16/26.*

If you have questions or need assistance in any of these “to do” items, please reach out to one of the authors or your regular Groom attorney.