

Understanding the 2024 HIPAA Privacy Rule Revision for Reproductive Healthcare

Revisions to the HIPAA Privacy Rule for reproductive healthcare and key information for implementing these changes

JESSICA PAYNE, BS, MANAGEMENT INFORMATION SYSTEMS,
SECURITY+ | CYSA+ | CC | CCSA

Table of contents

Introduction 2

The history and evolution of the HIPAA Privacy Rule 2

Key provisions in the 2024 HIPAA Privacy Rule.....3

 Reproductive healthcare: a new definition 3

 Key changes of the Final Rule.....3

 Presumption of lawfulness.....4

 Notice of Privacy Practices updates 5

Implications for healthcare providers and covered entities 5

 A roadmap for implementation.....6

Conclusion.....7

Appendix: Acronyms 8

Legal disclaimer 9

Introduction

On April 26, 2024, the U.S. Department of Health and Human Services (HHS) published a final rule in the Federal Register revising the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to enhance protections for individuals seeking reproductive healthcare. This 2024 HIPAA Privacy Rule Final Rule (the “Final Rule”) enhances safeguards to patient privacy in consideration of recent developments in reproductive rights. The changes seek to address growing concerns about the potential misuse of personal health information in legal actions related to reproductive healthcare services, such as abortion, contraception, and fertility treatments. The rule is part of a broader effort by the federal government to maintain and protect privacy in the face of rapidly changing state laws and legal challenges.

The Final Rule amends existing regulations under HIPAA, with an emphasis on prohibiting the disclosure of protected health information (PHI) for certain activities involving reproductive healthcare. The regulations took effect on June 25, 2024, with a compliance deadline of December 23, 2024. However, specific requirements related to the Notice of Privacy Practices (NPP) have a later compliance deadline of February 16, 2026.

The history and evolution of the HIPAA Privacy Rule

HIPAA, enacted in 1996, was initially designed to enhance the efficiency of the healthcare system, combat fraud, and ensure health insurance coverage portability. However, as electronic health records (EHRs) became more common, protecting the confidentiality of health data became a pressing concern. This led to the introduction of the HIPAA Privacy Rule in 2000, which became enforceable in 2001. The HIPAA Privacy Rule established foundational safeguards for PHI, limiting its use and disclosure without patient authorization. It also granted individuals the right to access and amend their health records. Over time, further legislative updates, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, strengthened enforcement measures and expanded compliance requirements.

The 2024 HIPAA Privacy Rule to Support Reproductive Health Care Privacy revisions represent the latest effort to address evolving privacy concerns, particularly in the realm of reproductive healthcare. This update prohibits the disclosure of PHI related to lawful reproductive healthcare to ensure that individuals seeking such reproductive health services, including abortion, can access care without fear that their health information will be used to penalize them.

Figure 1 illustrates the trends in complaints filed under the HHS Privacy Rule from April 2023 to October 2024, highlighting the growing awareness and concerns surrounding health care privacy. As the new HIPAA Privacy Rule revisions take effect, this data may reflect the importance of safeguarding personal health information in the context of reproductive services.

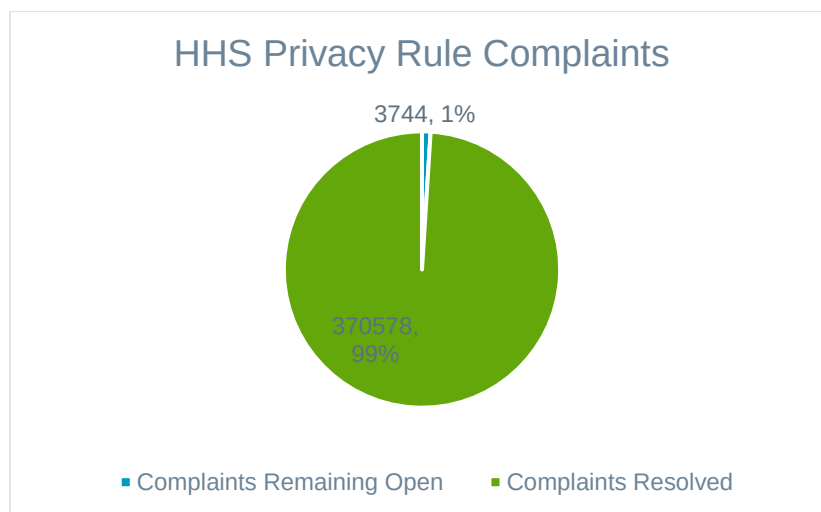


Figure 1: HHS Privacy Rule complaints from April 2023 to October 2024

Key provisions in the 2024 HIPAA Privacy Rule

Reproductive healthcare: a new definition

One of the most critical aspects of this rule is the establishment of a new, clear definition of “reproductive healthcare.” This term is used throughout the rule to describe healthcare services that affect the reproductive system, including, but not limited to, services such as abortion, contraception, prenatal care, and infertility treatments. The Final Rule specifically clarifies that this definition is not intended to dictate the standard of care or regulate what is considered appropriate reproductive healthcare. Instead, it aims to ensure that individuals’ privacy regarding reproductive healthcare is protected under the same standards as other medical services.

By defining “reproductive healthcare” in this way, the rule underscores the importance of privacy when it comes to sensitive health decisions while also avoiding interference with clinical judgment or practice standards. This ensures that any individual seeking these services is entitled to confidentiality protections under HIPAA.

Key changes of the Final Rule

The most notable change introduced by the Final Rule is the prohibition of the use or disclosure of PHI for investigations related to seeking, obtaining, providing, or facilitating reproductive healthcare. This prohibition is particularly relevant in the context of civil, criminal, or administrative investigations which may have previously involved the disclosure of PHI to pursue legal actions against individuals seeking reproductive healthcare services that are lawful under state or federal law.

Under the new rule, PHI may not be used or disclosed to investigate or impose liability on individuals involved in reproductive healthcare unless the regulated entity (such as a healthcare provider or insurer) has actual knowledge that the care in question was unlawful or there is substantial information supporting the conclusion that the healthcare provided was unlawful under the specific circumstances.

According to the [HHS HIPAA Privacy Rule Final Rule Fact Sheet](#), the Final Rule strengthens privacy protections by prohibiting the use or disclosure of PHI by a [covered entity](#) (i.e., healthcare provider, health plan, or healthcare clearinghouse) or their [business associate](#) (collectively, “regulated entities”) for either of the following activities:

- To conduct a criminal, civil, or administrative investigation into or to impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare, where such healthcare is lawful under the circumstances in which it is provided
- The identification of any person for the purpose of conducting such investigation or imposing such liability

Under the Final Rule, the prohibition applies where a regulated entity has reasonably determined that one or more of the following conditions exists:

- Reproductive healthcare is lawful under the law of the state in which such healthcare is provided and under the circumstances in which it is provided.
- The reproductive healthcare is protected, required, or authorized by federal law, including the U.S. Constitution, regardless of the state in which such healthcare is provided.
- The reproductive healthcare was provided by a person other than the covered regulated entity that receives the request for PHI and the presumption described below applies.

The Final Rule continues to permit regulated entities to use or disclose PHI for purposes otherwise permitted under the Privacy Rule where the request for the use or disclosure of PHI is not made to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare. For example:

- A covered healthcare provider could continue to use or disclose PHI to defend themselves in an investigation or proceeding related to professional misconduct or negligence where the alleged professional misconduct or negligence involved the provision of reproductive healthcare.
- A covered regulated entity could continue to use or disclose PHI to defend any person in a criminal, civil, or administrative proceeding where liability could be imposed on that person for providing reproductive healthcare.
- A covered regulated entity could continue to use or disclose PHI to an Inspector General where the PHI is sought to conduct an audit for health oversight purposes.

To enforce the prohibition on the use or disclosure of PHI for prohibited purposes related to reproductive healthcare, the Final Rule mandates that covered regulated entities must obtain a signed attestation when they receive requests for PHI that could be related to reproductive care. The signed attestation serves as a written representation from those requesting PHI that confirms that their request is not intended for a prohibited purpose. This requirement applies to requests for PHI in the contexts of health oversight activities, judicial and administrative proceedings, law enforcement, and disclosures to coroners or medical examiners. This measure ensures that covered entities have a way of verifying that PHI is being requested for lawful reasons. The attestation requirement also alerts requesters to the potential criminal penalties under HIPAA for knowingly obtaining or disclosing individually identifiable health information (IIHI) in violation of the regulations.

Presumption of lawfulness

An important component of this rule is the presumption of lawfulness regarding reproductive healthcare. The Final Rule establishes a presumption that reproductive healthcare provided by someone other than the covered regulated entity receiving the request for PHI is lawful under the circumstances in which it was provided. This presumption holds unless the covered regulated entity has actual knowledge of, or receives sufficient evidence indicating that, the reproductive healthcare was not lawful. The presumption aims to protect individuals by ensuring that the disclosure of PHI related to reproductive healthcare is not used to investigate lawful activities.

The rule provides specific conditions under which the presumption of lawfulness can be overridden. If the covered regulated entity has actual knowledge that the reproductive healthcare was unlawful, such as when an individual discloses that they obtained care from an unlicensed provider and the healthcare provider knows that the care should have been

provided by a licensed professional, then the presumption does not apply. In such cases, the covered regulated entity may be required to disclose PHI related to the investigation of unlawful conduct.

Alternatively, the presumption can also be challenged if the covered entity receives factual information from the person requesting PHI that demonstrates a strong factual basis for the claim that the reproductive healthcare was unlawful. For example, if a law enforcement official provides evidence that the healthcare was provided by an unlicensed individual where licensing is required, the presumption of lawfulness is no longer applicable. This ensures that PHI is only disclosed in situations where there is clear and substantiated evidence of unlawful conduct.

Notice of Privacy Practices updates

Another significant requirement of the Final Rule is the obligation for covered entities to update their NPP. The NPP must include updated provisions that reflect the new protections for reproductive healthcare privacy, along with other changes in regulations such as those associated with the [Confidentiality of Substance Use Disorder Patient Records regulations at 42 CFR part 2 \("Part 2"\)](#). This ensures that individuals are clearly informed about their privacy rights and the protections available to them regarding reproductive healthcare.

The updated NPP must be compliant with the revised rule by February 16, 2026, which aligns with the compliance deadline for changes to the Part 2 regulation. This provides covered entities sufficient time to ensure that their NPPs reflect the new legal requirements, offering transparency about how patient information is managed in relation to reproductive healthcare.

Implications for healthcare providers and covered entities

The 2024 modifications to the HIPAA Privacy Rule have significant implications for healthcare providers, insurers, and other entities covered by HIPAA. These organizations must carefully assess their current policies and procedures to ensure they align with the new protections for reproductive healthcare. The rule requires that organizations update their protocols to reflect the prohibition of disclosing PHI in connection with reproductive healthcare investigations, as well as revise their NPPs to incorporate the updated privacy protections. According to the [HHS](#), 67% of the complaints investigated between April 2023 and October 2024 were found in violation of the Privacy Rule and required subsequent corrective action (Figure 2).

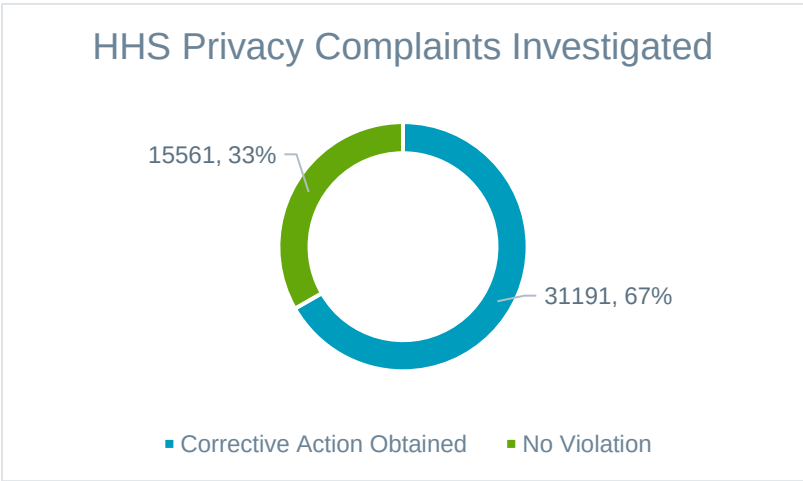


Figure 2: HHS Privacy Rule complaints investigated from April 2023 to October 2024

Healthcare providers must also implement training programs to educate staff on the changes to the HIPAA Privacy Rule, ensuring that all employees understand their responsibilities in protecting patients’ privacy regarding reproductive healthcare. Training should focus on the new prohibitions on PHI disclosures, the presumption of lawfulness for reproductive healthcare, and the steps involved in complying with the new NPP requirements.

A roadmap for implementation

To implement the 2024 HIPAA Privacy Rule revisions effectively, organizations should follow a structured approach that ensures compliance while minimizing disruption. The first step is to assess current policies and procedures to identify gaps in compliance. This process should focus on areas where reproductive health PHI is most likely to be managed, such as patient intake, records management, and disclosure workflows.

Once gaps have been identified, organizations must then (1) update their NPP to reflect the new protections for reproductive health information and (2) revise their disclosure protocols. The NPP should clearly inform patients about their rights under the revised rule and outline the organization’s responsibilities in safeguarding sensitive data. This update must be completed by the compliance deadline of February 2026. Revising disclosure protocols involves establishing processes for managing requests involving reproductive health PHI, including the use of attestation forms, where applicable. These processes should be integrated into existing workflows to ensure consistency and efficiency.

Enhanced safeguards are also necessary to protect reproductive health data. Organizations should update administrative, technical, and physical measures to align with the new requirements. For example, EHR systems can be configured to flag reproductive health data for special handling, ensuring it is not disclosed inappropriately.

Training is also key to successful implementation, as staff members must be trained in the new rules, with a focus on real-world scenarios involving reproductive health PHI. Role-specific training can address the unique responsibilities of different teams, from front-line staff to compliance officers.

Finally, organizations should establish a robust system for monitoring and auditing compliance. Regular reviews of disclosure logs and attestation forms can help identify potential issues early, while comprehensive documentation ensures the organization can demonstrate compliance if audited.

Conclusion

The 2024 revisions to the HIPAA Privacy Rule represent a significant step in ensuring the privacy and confidentiality of individuals seeking reproductive healthcare services. By prohibiting the disclosure of PHI in connection with investigations into lawful reproductive healthcare, the rule aims to protect patients from discrimination, legal jeopardy, or unnecessary scrutiny. Healthcare organizations must take proactive steps to comply with the updated regulations by revising their policies, procedures, and training programs, as well as ensuring that their NPPs are fully updated by February 2026.

With the Final Rule, HHS has strengthened privacy protections for reproductive healthcare, helping to ensure that individuals can seek care with the confidence that their personal health information will remain protected from misuse. Compliance with the new rule is critical for healthcare organizations to maintain trust with patients and adhere to evolving legal and regulatory standards. As compliance experts, Coalfire has a deep understanding of the regulatory landscape and offers a range of services to help organizations not only comply with the necessary regulatory requirements and strengthen their security posture but to also meet the expectations of their clients when it comes to data privacy.

For more information on the 2024 HIPAA Privacy Final Rule, visit: [The Federal Register](#) and [HHS Final Rule Fact Sheet](#).

Appendix: Acronyms

Acronym	Term
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
EHR	Electronic health record
EMR	Electronic medical records
IIHI	Individually identifiable health information
NPP	Notice of Privacy Practice
PHI	Protected health information
PII	Personally identifiable information

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the author

Jessica Payne, *Consultant – GRC Healthcare*

Jessica Payne, BS in Management Information Systems with a focus on Information Assurance, is a certified cybersecurity professional holding CompTIA Security+, CompTIA CySA+, ISC2 Certified in Cybersecurity (CC), and Certified Cyber Security Architect (CCSA) credentials. Since joining Coalfire in 2024, she has brought over five years of cybersecurity consulting experience, specializing in healthcare risk management and compliance. Jessica works closely with healthcare clients to strengthen their security postures using industry frameworks such as NIST 800-53, NIST CSF, HIPAA, and ISO 27001.

Her expertise includes conducting comprehensive security assessments, developing tailored cybersecurity programs, and ensuring regulatory compliance for healthcare organizations. Jessica has led initiatives in incident response, vulnerability management, and policy development, helping clients mitigate risks and safeguard sensitive data. Dedicated to ongoing professional growth, she stays at the forefront of cybersecurity trends to provide innovative, effective solutions that address evolving security challenges.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit [Coalfire.com](https://coalfire.com).

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_UnderstandingThe2024HIPAARuleUpdatesToReproductiveHealthCare_01022025