Health Information Privacy after *Dobbs*

Deven McGraw & Andrew Crawford

Introduction

The unprecedented overturning of *Roe v. Wade*[1] removed federal constitutional protections on access to abortion. Specifically, in June 2022, the Supreme Court decided *Dobbs v. Jackson Women's Health Organization,*[2] reversing decades of prior court precedent under *Roe* and its progeny. As a result of *Dobbs,* states may protect, ban, or severely limit access to abortion and other types of reproductive health care that might involve pregnancy termination, unless their enactments violate state constitutional protections or another, supervening law. Currently 22 states criminalize abortions or have placed more stringent restrictions on the procedure than were permissible pre-*Dobbs*.[3]

Dobbs has also upended privacy expectations. Although abortion has long been subject to some state restrictions, before *Dobbs* patients may have had confidence that their health data—for instance, data associated with researching, accessing, traveling to, and receiving reproductive health care—generally stayed private. *Dobbs* opened the floodgates not only to greater restrictions on reproductive health care but also to increased enforcement of those restrictions, which may involve invasion of patient privacy.

Much of the data that reveals an individual has received reproductive health care is covered by the privacy, security, and breach notification regulations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[4] Although HIPAA's regulations provide protections for personally identifiable medical records, as well as health plan claims records (collectively known as protected health information or PHI), those rules have always included some exceptions by which law enforcement agencies could obtain access. In response to the changes in the legal landscape for reproductive health care post *Dobbs*, the US Department of Health and Human Services (HHS) recently finalized changes to HIPAA's privacy regulations—known as the Privacy Rule—to limit access to data generated by the delivery of legal reproductive health care, if it is being sought by law enforcement or other persons seeking to use that data to penalize a patient or his or her medical provider for the delivery of that care (hereinafter, the "Privacy Rule Reproductive Data Protections").[5] How well will those protections work to protect health data and what are the gaps that remain?

■

***Deven McGraw** is the Chief Regulatory and Privacy Officer at Citizen Health, a company that helps individuals gather, organize, and share their medical records. She was previously the Deputy Director for Health Information Privacy at the HHS Office for Civil Rights.*

***Andrew Crawford** is a Senior Counsel with CDT's Data and Privacy Project. In addition to advocating for comprehensive federal privacy legislation, Andrew's work focuses on the intersection of technology, health data, and privacy.*

1 Roe v. Wade, 410 U.S. 113 (1973).

2 Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

3 Allison McCann & Amy Schoenfeld Walker, *Tracking Abortion Bans Across the Country,* N.Y. Times (Aug. 1, 2024), https://www.nytimes.com/interactive/2024/us/abortion-laws-roe-v-wade.html.

4 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 20, 1996).

5 HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 89 Fed. Reg. 32976 (Apr. 26, 2024) ("Privacy Rule Reproductive Data Protections").

State law restrictions on reproductive health care in the wake of *Dobbs*

In the wake of *Dobbs*, states have generally taken one of two opposing strategies around access to reproductive health care and privacy. The first approach, taken by nearly a quarter of states, is to ban or severely restrict abortions, either through new laws or resuming enforcement of old, pre-*Roe* laws. Some of these new laws permit the prosecution of people who provide, or otherwise aid in the procurement of, abortions with few to no exceptions,[6] even in cases of abuse and incest.[7] Some states explicitly criminalize self-managed abortions.[8] A few states also allow private citizens to bring civil actions against abortion providers.[9] With these laws in place, and the removal of *Roe* as a barrier, state-level law enforcement agencies in states opposed to abortion rights have new opportunities to seek PHI to conduct investigations and for criminal prosecutions and civil actions against people seeking, providing, or assisting with reproductive health care, including abortions.

By implementing these shield laws, states aim to protect the data of patients and providers within their jurisdiction, regardless of whether the patient is a state resident.

A second approach, taken by twenty states plus the District of Columbia, has been to pass new laws that shore up access to reproductive care, and, recognizing that people may travel to seek abortions, some states limit the circumstances and manner in which in-state entities and providers may share patient information with entities from states that restrict access to care.[10] Such state actions include governor-issued executive orders, and some states, including California[11] and Maryland,[12] have enacted "shield laws" that restrict the sharing of data related to reproductive health care in various forms, such as in response to an out-of-state investigation. By implementing these shield laws, states aim to protect the data of patients and providers within their jurisdiction, regardless of whether the patient is a state resident. For example, under these newer "shield laws", state court judges could be prohibited from domesticating an out-of-state subpoena seeking location data showing that an individual visited an abortion clinic. Additionally, some state shield laws also restricted the activities of communication service providers, like social media companies, headquartered within their borders to preclude their cooperation with surveillance demands relating to reproductive health activities that occur outside the state.

Additional risks to the privacy of reproductive health information

In the wake of new, more restrictive laws, and increased focus on enforcing pre-existing restrictions, law enforcement and civil litigants may turn to entities that collect and store health information

---

[6] *See, e.g.*, Idaho Code §§ 18-605, -606; La. Stat. Ann. §§ 14:87.7, 40:1061(D), 40:1061.29; S.D. Codified Laws § 22-17-5.1 (2023); Tex. Health & Safety Code § 170A.004; Wyo. Stat. Ann. § 35-6-125 (2023).

[7] *See, e.g.*, Tex. Health & Safety Code § 170A.002; Daniel Breen, *Lawmakers reject child rape, incest exceptions to Arkansas abortion ban*, NPR (Mar. 30, 2023), perma.cc/6ZE4-GG4D (reporting on H.B. 1670, 94th Gen. Assemb., Reg. Sess. (Ark. 2023)).

[8] South Carolina, Idaho, Oklahoma, and Nevada. S.C. Code Ann. § 44-41-80(b) (2023); Idaho Code § 18-606(2); Okla. Stat. tit. 63, § 1-733 (2023); Nev. Rev. Stat. Ann. § 200.220 (LexisNexis 2023); *see* Lyn Riddle & Poppy Noor, *South Carolina woman arrested for allegedly using pills to end pregnancy*, Guardian (Mar. 3, 2023), perma.cc/YNX8-XRM2. Of note, between 2000 and 2020, twenty-six states had already investigated or arrested people for self-managed abortions. Laura Huss, Farah Diaz-Tello & Goleen Samari, *Self-Care, Criminalized: August 2022 Preliminary Findings*, If/When/How (Aug. 2022), perma.cc/U6UA-T5MP.

[9] Idaho Code §§ 18-613, 618; Tex. Health & Safety Code § 171.208; *see* Alan Feuer, *The Texas Abortion Law Creates a Kind of Bounty Hunter. Here's How It Works.*, N.Y. Times (Sept. 10, 2021), perma.cc/HS52-YH2N.

[10] For a full list of state actions post-*Dobbs*, see Jake Laperruque, *Two Years After Dobbs: An Analysis Of State Laws To Protect Reproductive Healthcare Information From Interstate Investigations and Prosecutions*, Ctr. For Democracy & Tech. (June 2024), https://cdt.org/insights/report-two-years-after-dobbs-an-analysis-of-state-laws-to-protect-reproductive-healthcare-information-from-interstate-investigations-and-prosecutions/.

[11] Assemb. B. 1242, 2021–2022 Reg. Sess. (Cal. 2022) (codified in scattered sections of the Cal. Penal. Code).

[12] The Reproductive Health Protection Act, Senate B. 859, 2023 Reg. Sess. (Md. 2023) (codified in scattered sections of the Md. Code).

to gain access to data that could help prove that a person sought, received, aided, or provided an abortion.[13] The risks of disclosure of reproductive health care information for law enforcement or civil litigation purposes are not hypothetical. Even prior to *Dobbs*, state-level criminal investigators charged individuals with pregnancy-related offenses, and sought and utilized health information (including PHI covered by the Privacy Rule) as evidence in pregnancy-related prosecutions.[14] In 2010, a woman was arrested for attempted feticide after she fell down the stairs, went to the hospital to check on her fetus, and confessed to a nurse that she had been considering adoption or abortion—the nurse reported her statements to a doctor who called the police.[15] In 2019, the Missouri State Health Director testified at a hearing that he tracked Planned Parenthood patients' menstrual cycles with a spreadsheet that was compiled by the State's main inspector to help identify patients who had undergone failed abortions after the state became concerned they were not receiving complication reports for all failed surgical abortions.[16] The Director later denied tracking menstrual cycles but admitted that officials had the data and a spreadsheet did exist.[17] In 2021, a woman gave birth to a healthy baby but provided her obstetrician a list of prescriptions she took during pregnancy, triggering an investigation and, months later, an armed raid of her house.[18] She was charged with felony possession involving prescription fraud because she failed to inform her prescribing doctor that she was pregnant before refilling her lawful hydrocodone prescription—the charges were dropped but not until 2022.[19]

The expectation is that legal action against medical providers who provide abortions, patients seeking and obtaining abortion care, and the individuals who assist them, will increase, and that health and health-related data will be sought to support these legal actions.[20] The mere threat of potential prosecution or investigation under some of these abortion restrictions has suppressed the delivery of reproductive health care because it causes fear and uncertainty among medical professionals regarding whether the performance of certain health care procedures or administration

---

[13] Andrew Crawford, *Report—Data After Dobbs: Best Practices for Protecting Reproductive Health Data,* CENTER FOR DEMOCRACY & TECHNOLOGY (May 31, 2023), https://cdt.org/insights/report-data-after-dobbs-best-practices-for-protecting-reproductive-health-data/; Christine Henneberg, *The Trade-Offs for Privacy in a Post-*Dobbs *Era*, Wired (June 5, 2023), perma.cc/V5LA-HAZX. *See, e.g.*, Lauren Rankin, *How an online search for abortion pills landed this woman in jail*, Fast Co. (Feb. 26, 2020), perma.cc/3DLV-4924.

[14] *See* Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. Baltimore L. REV. 3 (2020); Sandhya Dirks, *Criminalization of pregnancy has already been happening to the poor and women of color*, NPR (Aug. 3, 2022), perma.cc/RF92-8RUN.

[15] Dirks, *Criminalization of pregnancy has already been happening to the poor and women of color*, NPR (Aug. 3, 2022), perma.cc/RF92-8RUN; Amie Newman, *Pregnant? Don't Fall Down the Stairs*, Rewire News Group (Feb. 15, 2010), perma.cc/4QKZ-CBA8.

[16] Darran Simon, *Missouri says health director didn't track Planned Parenthood patients' periods. But officials did have a spreadsheet*, CNN (Oct. 31, 2019), perma.cc/MSY9-4UYY.

[17] Yasmeen Abutaleb & Emily Wax-Thibodeaux, *Missouri reviewed data about Planned Parenthood's patients, including their periods, to identify failed abortions*, Wash. Post (Oct. 30, 2019), perma.cc/5K7F-T2XC.

[18] Moira Donegan, *Alabama is prosecuting a mom for taking prescribed medication while pregnant*, Guardian (July 27, 2021), perma.cc/YA8M-FPA3.

[19] *Felony Charge Dropped Against Alabama Mother Who Renewed Valid Prescription to Manage Chronic Pain During Pregnancy*, Pregnancy Justice (Feb. 23, 2022), perma.cc/4277-U8NZ.

[20] Caroline Kitchener, *Texas man files legal action to probe ex-partner's out-of-state abortion,* Wash. Post (May 3, 2024), https://www.washingtonpost.com/investigations/2024/05/03/texas-abortion-investigations/?utm_campaign=morning_rounds&utm_medium=e-mail&_hsmi=305565684&utm_content=305565684&utm_source=hs_email.

of certain drugs that have an impact on the fetus could put the medical provider or the provider—or both—in legal jeopardy.[21]

Consequently, in April 2024, HHS took a crucial step in protecting sensitive reproductive health data by finalizing the Privacy Rule Reproductive Data Protections.

Changes to the Privacy Rule in response to *Dobbs*

Following *Dobbs*, President Biden issued a series of Executive Orders directing federal agencies like HHS and the Department of Justice (DOJ), as well as the Federal Trade Commission (FTC) to: safeguard access to reproductive health care services, including abortion and contraception; protect the privacy of patients and their access to accurate information; promote the safety and security of patients, providers, and clinics; and coordinate the implementation of Federal efforts to protect reproductive rights and access to health care. Consequently, in April 2024, HHS took a crucial step in protecting sensitive reproductive health data by finalizing the Privacy Rule Reproductive Data Protections.[22]

HIPAA Background

Grasping the impact of Privacy Rule Reproductive Data Protections requires an understanding of the limitations in HIPAA's scope and the Privacy Rule's general approach to protecting health care system data.

The Privacy Rule does not cover all health information; instead, it governs PHI collected, used, and shared by physicians and hospitals and health plans. The Privacy Rule grew out of provisions in the original HIPAA statute that called for standardization and digitization of the claims for payment submitted by health care providers to health plans.[23] As a result, the HIPAA privacy provisions govern only the entities involved in those types of transactions.

These health system entities—referred to in HIPAA as "covered entities"—collect vast amounts of health information in the form of medical and claims records that provide intimate details about an individual's health. HIPAA also covers the contractors that receive sensitive data from these entities to perform services on their behalf (known as "business associates"). (This article will refer to both collectively as "regulated entities.") HHS wrote the Privacy Rule to accommodate the transfer and sharing of PHI that customarily occurs through the delivery of and payment for health care. For example, the prior consent of a patient is not required in order for doctors and hospitals to share information with one another for treatment purposes, or to review data for quality assurance purposes.[24] Covered entities are permitted to disclose the minimum necessary amount of PHI to public health authorities for public health purposes,[25] or to health plans to be paid or process payments for health care services.[26] Each permitted use and disclosure typically comes with some conditions that must be satisfied in order for lawful use or disclosure to occur under the Privacy Rule. Table A below provides examples of permitted uses and disclosures under the Privacy Rule

---

[21] Ariana Eunjung Cha, *Physicians face confusion and fear in post-Roe world*, Wash. Post (June 28, 2022), https://www.washingtonpost.com/health/2022/06/28/abortion-ban-roe-doctors-confusion/; Selena Simmons Duffin, *For doctors, abortion restrictions create an "impossible choice" when providing care*, NPR (June 24, 2022), https://www.npr.org/sections/health-shots/2022/06/24/1107316711/doctors-ethical-bind-abortion.

[22] Privacy Rule Reproductive Data Protections, *supra* note 5.

[23] The Inst. Of Med., Beyond The HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research (2009), at 63 https://www.ncbi.nlm.nih.gov/books/NBK9578/.

[24] 45 C.F.R. §§ 164.502, .506.

[25] 45 C.F.R. § 164.512(b).

[26] 45 C.F.R. § 164.506.

that do not require patient consent or authorization. Uses and disclosures that are not expressly permitted by the Privacy Rule require the prior written authorization of the patient.

Table A

Permitted Uses and Disclosures under the Privacy Rule[27]

- Treatment
- Payment
- Health care operations
- Reporting to public health authorities
- To contractors (business associates)
- Where required by law
- For reporting of potential abuse and neglect
- For health oversight purposes
- For medical product safety surveillance
- In response to a court order or subpoena
- To coroners and medical examiners
- For national security purposes
- To avert a serious threat to health or safety
- Although all regulated entities are required to comply with the Privacy Rule, business associates may be further limited in their use and disclosure of PHI by their agreements with covered entities, referred to in the Privacy Rule as business associate agreements

The Privacy Rule permits regulated entities to internally use or externally disclose PHI meaning the regulated entity has discretion under the Privacy Rule with respect to whether they will use and/or disclose PHI for a permitted purpose—with two exceptions: covered entities must provide a copy of medical records to patients up on their request[28] and regulated entities must make records available to HHS pursuant to an investigation of alleged HIPAA noncompliance.[29] Indeed, the Privacy Rule contains only a few outright prohibitions with respect to the use and disclosure of PHI—sales of PHI are prohibited, unless the patient has authorized the sale,[30] and identifiable genetic health information cannot be used by health insurers to determine health insurance coverage or to decline to pay for care due to a genetic condition, consistent with the Genetic Information Non-Discrimination Act.[31]

The Privacy Rule has always permitted –but does not require—regulated entities to disclose PHI to public officials for certain purposes, including law enforcement in some circumstances.[32] Table B below provides examples of permitted disclosures for law enforcement purposes. Similarly, the Privacy Rule permits disclosures to public health officials seeking information to perform

[27] 45 C.F.R. §§ 164.500–.534.

[28] 45 C.F.R. § 164.524. Business Associates are only required to respond to patient requests for PHI if required by their business associate agreement to do so.

[29] 45 C.F.R. § 160.310(a),(c).

[30] 45 C.F.R. § 164.502(a)(5)(ii).

[31] 45 C.F.R. § 164.502(a)(5)(i).

[32] 45 C.F.R. §§ 164.512 et seq.

their public health functions,[33] and to "health oversight agencies" for oversight activities, including administrative or criminal investigations.[34] The Privacy Rule also expressly permits the reporting of suspected child abuse to relevant authorities.[35]

Table B

Examples of Permitted Disclosures for Law Enforcement Purposes under the Privacy Rule

- In response to a court order or an administrative request.[36]
- To help locate a suspect or witness to a crime (only some identifying demographic and medical information may be disclosed for this purpose).[37]
- If the entities believe in good faith that the information is evidence of criminal conduct occurring on facility premises or to report commission of a crime that did not occur on facility premises.[38]
- To avert a serious threat to health or safety to a person or the public.[39]
- By workforce members if they believe in good faith that the entity for whom they work has engaged in unlawful conduct or the care the entity provides is a danger to a patient.[40]

The Dobbs decision has now inserted tension and ambiguity into situations when law enforcement seeks PHI about reproductive health care.

At the time when HHS enacted the Privacy Rule it was seeking to establish clear rules for when identifiable health information could be used and disclosed to allow for the functioning of the healthcare system, while still preserving privacy rights for patients. With increased adoption by healthcare providers of electronic medical record systems, PHI is increasingly digital, which is even easier to share. Law enforcement possesses a host of tools to seek evidence for legitimate investigations, including procedures outlined in the Privacy Rule for obtaining PHI. For example, the Privacy Rule permits entities to share information with law enforcement about a crime committed on the premises of a health care facility.[41] The *Dobbs* decision has now inserted tension and ambiguity into situations when law enforcement seeks PHI about reproductive health care. This tension and ambiguity are especially heightened when law enforcement seeks reproductive health PHI for treatments and procedures that are legal in the jurisdiction in which they are provided and received.

Actions to Strengthen the Privacy Rule post-*Dobbs*

The Privacy Rule doesn't *require* data sharing with public officials, including law enforcement. However, the Privacy Rule's permissive sharing provisions mean that the Privacy Rule does not provide much of a shield. State laws that provide greater protections for health data are not preempted by HIPAA;[42] but absent specific state law protections for reproductive health data, PHI

[33] 45 C.F.R. § 164.512(b).

[34] 45 C.F.R. § 164.512(d).

[35] 45 C.F.R. § 164.512(c).

[36] 45 C.F.R. § 164.512(f)(1)(ii).

[37] 45 C.F.R. § 164.512(f)(2).

[38] 45 C.F.R. §§ 164.512(f)(5)–(f)(6)(i).

[39] 45 C.F.R. § 164.512(j).

[40] 45 C.F.R. § 164.502(j).

[41] 45 C.F.R. § 164.512(f)(5).

[42] U.S. Dep't of Health and Human Serv., Does The Privacy Rule Preempt State Laws (March 12, 2003), https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html.

generated out of the delivery of lawful reproductive care could be vulnerable to being disclosed to advance legal actions taken in states with abortion bans or significant restrictions.

In the aftermath of the *Dobbs* decision, HHS initially issued guidance on June 19, 2022 suggesting that disclosures of reproductive health PHI could only occur where required by law or by court order.[43] However, the guidance could not on its own change the more expansive permissions in the regulation; regulatory changes can only occur through processes set forth in the Administrative Procedures Act.

Consequently, on April 17, 2023, the HHS Office for Civil Rights (OCR), which oversees policy and enforcement of HIPAA privacy-related regulations, published a set of proposed modifications to the Privacy Rule intended to strengthen protections for reproductive health data.[44] Those modifications, the Privacy Rule Reproductive Data Protections, were finalized on April 26, 2024 and went into effect on June 25, 2024.[45] Most aspects of the Protections are subject to enforcement by December 23, 2024.[46]

In proposing the Privacy Rule Reproductive Data Protections, OCR recognized that the *Dobbs* decision "makes it more likely than before that individuals' PHI may be disclosed in ways that cause harm to the interests that HIPAA seeks to protect," emphasizing in particular the impact of the decision on "access to lawful health care and full communication between individuals and health care providers."[47] Consequently, HHS chose to preserve the ability of regulated entities to still share reproductive health data to treat patients, to be paid for the delivery of reproductive health care, to facilitate public health reporting, and for all other legitimate functions of the health care system informed by patient medical records. Instead, HHS sought to directly address the problem—use of health information *against* a patient or their medical provider merely for the delivery of a lawful health care service.

Specifically, the Privacy Rule Reproductive Data Protections now prohibit regulated entities from using or disclosing PHI for either:

- Criminal, civil, or administrative investigations—or the imposition of criminal, civil, or administrative liability—of any person "for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided," or
- the identification of a person for the above purposes.[48]

For example, if a patient lives in a state that restricts abortion care and travels to another state to obtain a legal abortion, the reproductive health data generated from that care episode could not be used or disclosed for any of the prohibited purposes. The prohibition also prevents the use or disclosure of records related to care that is protected, required, or authorized by federal law,

---

[43] Press Release, Dep't of Health and Human Serv., HHS Issues Guidance to Protect Patient Privacy in wake of Supreme Court Decision on Roe (June 29, 2022), https://www.hhs.gov/about/news/2022/06/29/hhs-issues-guidance-to-protect-patient-privacy-in-wake-of-supreme-court-decision-on-roe.html.

[44] HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (proposed April 17, 2022) ("Proposed Reproductive Data Protections").

[45] Privacy Rule Reproductive Data Protections, *supra* note 5.

[46] *Id.*

[47] *See* Proposed Reproductive Data Protections, *supra* note 44, at 23507.

[48] 45 C.F.R. § 164.502(a)(5)(iii).

Since 2009, billions of taxpayer dollars have been spent, and policies have been enacted, promoting the interoperability of health information, to break down the silos of patient data to enable patients to receive quality care wherever they need services and facilitate uses of data across the health care system to improve population and public health.

including the U.S. Constitution, regardless of the state where the care is provided. This would include contraceptive care, which is protected by the Constitution under *Griswold v. Connecticut*.[49]

The Privacy Rule still permits PHI to be used or disclosed for the permitted purposes in the Rule so long as the use or disclosure is not to investigate or bring an action against (either criminal, civil or administrative) a person for the "mere act" of performing, receiving, or helping to facilitate a lawful service. For example, a covered entity provider could still access PHI for defense of a malpractice action or to seek reimbursement for care, or where PHI is sought by a regulator seeking to substantiate that services were delivered consistent with program requirements.

The use or disclosure prohibition applies even if the reproductive health data was not created by the regulated entity. Since 2009, billions of taxpayer dollars have been spent, and policies have been enacted, promoting the interoperability of health information, to break down the silos of patient data to enable patients to receive quality care wherever they need services and facilitate uses of data across the health care system to improve population and public health.[50] Consequently, PHI generated from a lawful service delivered in one state could travel for legitimate purposes to a state where that care is illegal—but the regulated entities in that state would still be prohibited from using or disclosing that data for criminal, civil or administrative proceedings that relate to the mere act of seeking or receiving that care. The Privacy Rule Reproductive Data Protections create a presumption that reproductive health care was lawfully delivered unless the regulated entity receiving the request for use or disclosure of data has actual knowledge that the care delivered was not lawful, or receives sufficient factual information from the requester that "demonstrates a substantial factual basis" that the care was not lawful[51] (for example, the entity has knowledge that the service was required to be provided by a licensed professional and the person providing the care did not have the required license).

To operationalize these prohibitions, the Privacy Rule requires regulated entities, when they receive a request for PHI "potentially related to reproductive health care," to obtain a signed attestation that the use or disclosure is *not* for a prohibited purpose.[52] This attestation requirement applies only to requests for, or access to, PHI for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, and for disclosure to or use by coroners or medical examiners. The signed attestations must be in plain English, must include specific provisions—for example, a description of the information requested, the names of individuals (or the class of individuals) whose information is being sought; the name(s) of the requesting person(s), and a clear statement that the use or disclosure is not for a prohibited purpose. The attestation cannot be combined with any other document or contain extraneous information. The attestation must also include a statement that access to information from a regulated entity in violation of this prohibition could be subject to criminal penalties.[53]

---

[49] Privacy Rule Reproductive Data Protections, *supra* note 5, at 33010 (referencing *Griswold v. Connecticut*, 381 U.S. 479 (1965)).

[50] Robert O'Harrow, Jr., *The Machinery Behind Health-Care Reform*, Wash. Post (May 16, 2009), https://www.washingtonpost.com/wp-dyn/content/article/2009/05/15/AR2009051503667.html; Sara Turbow, Julie R. Hollberg, & Mohammed K. Ali, *Electronic Health Record Interoperability: How Did We Get Here and How Do We Move Forward,* JAMA Health Forum (March 17, 2021), https://jamanetwork.com/journals/jama-health-forum/fullarticle/2777782.

[51] 45 C.F.R. § 164.502(a)(5)(C)(2).

[52] 45 C.F.R. § 164.509(a).

[53] 45 C.F.R. § 164.509(b)(1), (c).

The Privacy Rule also provides that regulated entities are not in compliance with the new rule if they use or disclose reproductive health data in reliance on a defective attestation.[54] An attestation is considered to be defective if it lacks a required element, contains additional information that is not a required element, or the regulated entity has actual knowledge that the attestation is false or a "reasonable" regulated entity in the same position would not believe the attestation is true that the use or disclosure is not for a prohibited purpose. HHS has created a model attestation form that regulated entities may choose to use; entities are also welcome to use their own forms.[55]

The HIPAA Privacy Rule has always required covered entities to provide a notice of privacy practices ("NPP") to patients (in the case of health care providers) and beneficiaries (in the case of health plans).[56] The Privacy Rule Reproductive Data Protections now require covered entities to include a provision in their NPPs that describes and includes at least one example of the types of uses and disclosures under the new prohibition "in sufficient detail for an individual to understand [the privacy practices]".[57] Entities do not have to comply with this particular change to the Privacy Rule until February 16, 2026; HHS also had recently finalized changes to the NPP provisions regarding data covered by federal protections for substance abuse treatment data, and wanted to give covered entities more time to make all of the required changes and comply with distribution requirements.

HHS took further steps to help assure that the permissive provisions of the Privacy Rule could not be further leveraged for investigations or pursuit of penalties for the mere act of delivering or receiving reproductive health care services. For example, they modified the definition of "person" to make clear that it refers to a "natural person (meaning a human being who is born alive)."[58] This is intended to assure that language in the Privacy Rule permitting reports to relevant authorities for purposes of preventing harm to a "person" could not be interpreted to permit the release of reproductive health data in violation of the Privacy Rule Reproductive Data Protections' prohibitions. They also made clear that the prohibitions apply even to access to PHI by public health agencies or entities acting on their behalf, even when acting within the scope of their authority.[59]

Finally, the new rule does not change the penalties that can be levied for violations of the Privacy Rule. Regulated entities can be subject to a corrective action order (which is typically imposed in settlement of an enforcement case) or civil monetary penalties of between $100—$50,000 per violation, depending on the level of culpability, with a maximum of $1.5 million annual cap for repeated violations of the same provision.[60] But only regulated entities can be penalized under HIPAA's civil penalty provisions; requesters of reproductive health data who are not also regulated entities are beyond the reach of the civil penalty provisions. Although most state public health departments are not HIPAA covered entities, as explained in more detail below, persons outside of HIPAA coverage can be held *criminally* responsible for obtaining PHI in violation of HIPAA.

---

[54] 45 C.F.R. § 164.509(b)(2).

[55] Dep't of Health and Human Serv., Model Attestation For A Requested Use Or Disclosure Of Protected Health Information Potentially Related To Reproductive Health Care, https://www.hhs.gov/sites/default/files/model-attestation.pdf.

[56] 45 C.F.R. § 164.520.

[57] 45 C.F.R. § 164.520(a)(2).

[58] 45 C.F.R. § 160.103.

[59] *Id.*

[60] 45 C.F.R. § 160.404.

Concerns about the Privacy Rule Reproductive Data Protections

In the Privacy Rule Reproductive Data Protections, HHS promulgated a targeted rule intended, on the one hand, to better protect reproductive health data from being used to investigate or bring an action against an individual or a medical provider or health plan, while, on the other, still allowing that data to be shared to provide care to the individual or to facilitate the functioning of the health care system. Nonetheless the rule will still be challenging to implement, and its protections will have some limits.

Broad definition of "reproductive health data"

A regulated entity is required to obtain an attestation that the requested PHI will not be used for a prohibited purpose before disclosing PHI that is "potentially related to" reproductive health data. The definition of reproductive health data is purposefully broad and is "health care . . . that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes."[61] Because this definition is not limited to abortion, contraception, or pregnancy-related care, and is not defined solely with respect to individuals with female reproductive organs, regulated entities have expressed concerns about inadvertently disclosing PHI that meets this definition without first requesting the attestation. Consequently, entities are considering requiring submission of attestations for all types of requests that would trigger an attestation requirement if reproductive health data were involved, regardless of whether such data is contained in the records. The breadth of the definition also makes it difficult to segment the data falling into the definition of "reproductive health data" from other data that might be lawful to share (although segmentation of sensitive data from non-sensitive data has always been a technical and policy challenge).[62]

The protections do not follow the data, so if a regulated entity legitimately discloses data to an entity not regulated by HIPAA, HIPAA's rules would not apply.

Limitations on reach due to HIPAA's coverage limitations

Traditionally, and as noted above, one of the shortcomings of HIPAA's privacy protections is that only regulated entities are required to comply with the rules. The protections do not follow the data, so if a regulated entity legitimately discloses data to an entity not regulated by HIPAA, HIPAA's rules would not apply. As an example, if a regulated entity shares reproductive health data with a researcher who has received a waiver of consent from an Institutional Review Board (which is permitted by the Privacy Rule), and that researcher then uses or discloses this data to facilitate a prohibited purpose, the civil penalty provisions of HIPAA could not be leveraged to hold the researcher accountable (and the regulated entity would not have been required by HIPAA to have obtained an attestation prior to disclosing the data).

The criminal penalty provisions initially enacted as part of HIPAA[63] and amended by Congress in the Health Information Technology for Economic and Clinical Health Act in 2009[64] may help close this gap. A "person" who knowingly and in violation of HIPAA obtains any individually identifiable health information from a covered entity relating to an individual or discloses individually identifiable health information to another person could be subject to criminal penalties, which

---

[61] 45 C.F.R. § 160.103.

[62] Rebecca Pifer, *ONC advisory committee finalizes interoperability rule recommendations,* Healthcare Dive (May 23, 2019), https://www.healthcaredive.com/news/onc-advisory-committee-finalizes-interoperability-rule-recommendations/555381/.

[63] 42 U.S.C. § 1320d-6.

[64] American Recovery and Reinvestment Act of 2009, Pub. L. No.111-5 (2009), tit. 7 § 13409.

vary by level of culpability.[65] A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment.[66] The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain, or malicious harm.[67] These provisions apply to the Privacy Rule Reproductive Data Protections as well. The Department of Justice is responsible for criminal prosecutions under the Privacy Rule.

Potential Penalties for Accepting a Deficient Attestation

Regulated entities are concerned about their potential liability under the Privacy Rule for making a disclosure based on an attestation that turns out to be defective. An attestation is defective if the regulated entity has "actual knowledge" that material information in the attestation is false, or, of greater concern, a "reasonable covered entity or business associate in the same position would not believe that the attestation is true with respect to" whether the requested use or disclosure is for a purpose that is not prohibited by the new rule. What constitutes a "reasonable covered entity or business associate in the same position" requires subjective judgment, leaving regulated entities concerned about getting it wrong in the eyes of regulators. The Privacy Rule Reproductive Data Protections also require regulated entities to cease any use or disclosure if they discover information showing that any information in the facially valid attestation they relied on to make the use or disclose was materially false, and failure to do so would constitute a HIPAA violation.[68]

Limit on Types of Requests Requiring the Attestation

Regulated entities are required to obtain attestations only when requests for PHI potentially containing reproductive health data are submitted for purposes of health oversight, for judicial and administrative proceedings, for law enforcement, and for disclosures to coroners and medical examiners. But reproductive health data could be released for other purposes—such as for treatment, or research, or any of the other permitted purposes—and the recipient, if the recipient is not a regulated entity would not be subject to the prohibition in terms of its further use and disclosure of the information. For example, a covered entity physician may disclose PHI to a medical researcher pursuant to the research provisions of the Privacy Rule, but many researchers are not regulated entities (for example, researchers working in private research institutions or for pharmaceutical companies). However, the requestor could face criminal liability under the provisions discussed previously. Nevertheless, some regulated entities have discussed requesting attestations in any circumstance where reproductive health data could potentially be used or disclosed as a way of assuring protections for this data. At the same time, regulated entities that are also covered by the federal Information Blocking Rules, promulgated by the HHS Office of the National Coordinator for Health IT pursuant to the 21st Century Cures Act[69], could be subject to penalties for creating obstacles to the sharing of electronic health information in circumstances where it is otherwise

---

[65] 42 U.S.C. § 1320d-6(a)(3), (b)(1)-(3).

[66] 42 U.S.C. § 1320d-6(b)(1).

[67] 42 U.S.C. § 1320d-6(b)(2)-(3).

[68] 45 C.F.R. § 164.509(d). The regulated entity could still make disclosure of PHI which would not be otherwise prohibited by the Privacy Rules as amended by the Privacy Rule Reproductive Data Protections.

[69] 21st Century Cures Act, Pub. L. No. 114-255 (2016), tit. 4 § 4004.

lawful to share. The concern of these dual-regulated entities is that they could be penalized under the Information Blocking Rules for requiring attestations for the sharing of data for purposes for which an attestation is not required.

Of note, regulated entities are still permitted to disclose reproductive health data for public health purposes, and there is no requirement for an attestation for public health requests. However, under the new provisions, it is not a legitimate public health activity if the reproductive health data is to be used for one of the prohibited purposes. But public health agencies are typically not HIPAA regulated entities; consequently, if they receive reproductive health data within the scope of their authority and then subsequently use or disclose that data for a purpose that would be prohibited if they were a regulated entity, it is not clear that the disclosing would be in violation of HIPAA for having made that disclosure.

Some advocates for comprehensive reproductive health care have expressed concerns that HHS didn't go far enough in protecting reproductive health data.

Rule Doesn't Preempt State Laws Requiring Disclosure of Abortion Data

Some advocates for comprehensive reproductive health care have expressed concerns that HHS didn't go far enough in protecting reproductive health data. In the HIPAA statute, Congress gave HHS broad authority to enact privacy protections for individually identifiable health information transmitted among health care providers and health plans (i.e., covered entities), and provided that these standards, largely adopted through regulation, would preempt state laws that were less stringent—i.e., provided fewer privacy protections.[70] Should HHS have utilized these preemption provisions to go further—for example, by enacting new HIPAA privacy provisions that restricted the use or disclosure of reproductive health data for purposes of pursuing *any* civil, criminal or administration action for the mere act of receiving a health care service, even if that service was not lawful in the setting in which it was delivered? For reasons that are not shared in the regulatory materials, HHS instead chose to focus only on protecting the privacy of data generated out of lawfully delivered care and not to test the strength of this broad preemption authority against the plethora of abortion restrictions and new penalties in the post-*Dobbs* era.

HIPAA Doesn't Apply to De-Identified Data

HIPAA covers only identifiable health information; consequently, HHS's authority to promulgate privacy rules extends only to identifiable health information (i.e., PHI). The Privacy Rule establishes a legal standard for de-identification—no reasonable basis to believe the information can be re-identified—and two acceptable methodologies for de-identifying PHI: a safe harbor method requiring the removal of 18 categories of identifiers and no actual knowledge on the part of the disclosing entity that the data can be re-identified; or an expert or statistical methodology requiring a trained statistician, applying statistical techniques, to certify/attest that the data, in the hands of an anticipated recipient(s), would have a very low probability of being re-identified.[71] Although there are few published instances of HIPAA de-identified data having been successfully re-identified, much has been written about the vulnerability of PHI de-identified under HHS's safe harbor methodology, given the increasing amounts of data available for re-identification.[72] Nonetheless, de-identified reproductive health data is not covered by the rules. Further, there is no federal prohibition against re-identifying HIPAA-deidentified data, although any de-identified data collected by a regulated

[70] 42 U.S.C. § 1320d-7.

[71] 45 C.F.R. § 164.514.

[72] *See, e.g.*, Brittany Kryzanowski & Steven M. Manson, *Twenty Years of the Health Insurance Portability and Accountability Act Safe Harbor Provision: Unsolved Challenges and Ways Forward*, JMIR Med. Inform. (Aug. 2022), https://medinform.jmir.org/2022/8/e37756/.

entity would be subject to HIPAA's rules, including the new prohibitions once it meets the definition of PHI. As a result, a recipient of HIPAA de-identified reproductive health data who is not covered by HIPAA and who re-identifies the data—and subsequently uses it for a purpose that otherwise would have been prohibited by the new rules—likely cannot be found to have violated HIPAA, either civilly or criminally. The vulnerability of PHI to re-identification leaves a hole in the protections otherwise extended by this new rule.

Prospects of Legal Challenge

The State of Texas has already filed a legal challenge to block the Privacy Rule Reproductive Data Protections,[73] and it is likely there will be more. While it is too soon to know how many and which challenges may or may not have merit, several rationales could be advanced as possible challenges. For example, states with laws that penalize individuals for seeking or facilitating abortion care *outside* of the state could challenge the law as posing a barrier to enforcement of their duly enacted laws. However, this rationale runs against the long-recognized federal right to travel between states under the Privileges and Immunities Clause of the U.S. Constitution.

Another core consideration underlying many potential legal challenges to the Privacy Rule Reproductive Data Protections is standing. Specifically, who has suffered an injury such that they would have standing to challenge the Protections? Any potential litigant seeking to challenge the rule would need to show that elements of injury, causation, and redressability existed at the outset of the lawsuit, and continue to exist, for each claim and for each form of relief sought.[74] Depending on the specifics of each case, it may be difficult for states to establish all the elements of standing to successfully challenge the rule.[75]

Additionally, the Supreme Court's recent decision in *Loper Bright Enterprises v. Raimondo*[76] overturning the *Chevron* doctrine and possibly the Court's 2022 decision in *West Virginia v. EPA*[77] addressing the Major Questions Doctrine[78] may add to the likelihood of legal challenges. Specifically, in the absence of *Chevron* deference, agency actions, especially those that address divisive issues like abortion, may prove to be priority targets for litigants seeking to challenge executive agency rulemaking under a theory that agency rules exceed Congress' statutory direction to a federal agency. The Privacy Rule Reproductive Data Protections may be vulnerable to such a challenge. Although an Administrative Procedure Act challenge to the original HIPAA regulations was rejected in 2003 by the 4th Circuit in *S.C. Med. Ass'n v. Thompson*,[79] a more recent District Court case[80] rejecting previous HHS amendments to HIPAA that relied on the original grant of HIPAA

---

[73] Brendan Pierson, *Texas sues to block Biden rule protecting privacy for women who get abortions,* Reuters (Sept. 5, 2024), https://www.reuters.com/legal/texas-sues-block-biden-rule-protecting-privacy-women-who-get-abortions-2024-09-05/.

[74] U.S. Const. art. III, § 2, cl. 1; U.S. Congress, *ArtIII.S2.C1.6.1: Overview of Standing,* Constitution Annotated, https://constitution.congress.gov/browse/essay/artIII-S2-C1-6-1/ALDE_00012992/.

[75] In the Texas suit, *supra* note 68, Texas filed suit against HHS seeking to block the new HIPAA privacy protections from going into effect later this year. In its filing, Texas claims, among other things, that it is entitled to a response to its administrative subpoena and is therefore harmed by the 2024 Privacy Rule. Texas cites at least one instance when a covered entity cited the 2024 Privacy Rule as a reason it cannot comply with the state's subpoena. Complaint, *Texas v. U.S. Dep't of Health and Human Serv.*, No 5:24-cv-00204-H (N.D. Tex. Sep. 4, 2024), ECF No. 1.

[76] 144 S.Ct. 2244 (U.S. 2024).

[77] No. 20-1530, slip op. (U.S. Jun. 30, 2022).

[78] Congressional Research Services, *The Major Questions Doctrine* (Nov. 2, 2022), https://crsreports.congress.gov/product/pdf/IF/IF12077.

[79] 327 F. 3d 346 (4th Cir 2003).

[80] Ciox Health, LLC v. Azar, 435 F. Supp. 3d 30 (D.D.C. 2020).

rulemaking authority from 1996 reasoned, in dicta, that the original grant of authority was now "too old" for HHS to rely on in making further amendments to HIPAA.

In sum, there are a lot of unknowns when it comes to weighing the merits of potential challenges to the new HIPAA rule. Recent Supreme Court actions have dramatically impacted agency litigation and action and until there is further case law in the post-*Chevron* era, it is difficult to predict whether HHS authority to promulgate this rule would be upheld, or whether a different Administration would spend the resources to vigorously defend HHS' actions. Moreover, additional federalism and standing questions are likely to persist until they have worked their way through the courts. And of course, changing political winds in either the Administration or Congress could result in overturning or paring back these rules.

Search queries, browsing history, the contents of communications, and a person's location data can all reveal private health-related information, despite not typically being thought of as sources of "medical" or health-related data.

Health Data Privacy Threats Outside of HIPAA

Health data enjoy fewer privacy protections when held by entities outside of the scope of HIPAA. This article has focused on the threats of new and existing state laws banning or restricting abortion care on the privacy of health information governed by HIPAA and actions being taken by HHS to change the Privacy Rule to try to mitigate those threats. However, vast amounts of individuals' health data (indeed in some instances the same records) exist and are held by entities beyond HIPAA's limited scope and jurisdiction.

Search queries, browsing history, the contents of communications, and a person's location data can all reveal private health-related information, despite not typically being thought of as sources of "medical" or health-related data. These types of data can reveal sensitive information about a person's health and healthcare choices, regardless of whether the company collecting it provides health-related services. People's online searches and browsing history have already been used in abortion-related prosecutions,[81] and investigative reporters have shown that location data can be purchased revealing where visitors to an abortion clinic went immediately before and after their visits, which can be highly revealing of a person's identity—those locations are likely either their workplace or home.

In our digitally connected world, given the growing prevalence of medication abortion—and ability to receive reproductive health services from telemedicine—enforcement of anti-abortion laws may increasingly rely on digital and electronic information. Moreover, the popularity of health tracking apps and IoT (internet of things) devices create ever-growing stores of health data that can be very insightful, revealing health conditions, including reproductive status, care, and treatments. For example, a connected scale tracks weight gain and loss over time, and a connected refrigerator can detect items added to its shelves that were purchased at the grocery store.

At the federal level, the FTC has authority to regulate and protect health data not covered by HIPAA. The FTC has and continues to utilize existing rulemaking and enforcement authorities to address health privacy concerns for non-HIPAA covered entities. For example, on May 30, 2024, the FTC published the final version of changes to the Health Breach Notification Rule (HBNR), which sets forth the protocol in the case of a breach of health data.[82] Specifically, the HBNR requires vendors of personal health records (PHR) and related entities that are not covered by

---

[81] John Yang, Kaisha Young, & Marconjia Zor, C*ourt Cases Targeting Abortion Highlight Digital Privacy Concerns*, PBS News (Aug. 5, 2023), https://www.pbs.org/newshour/show/court-cases-targeting-abortion-highlight-digital-privacy-concerns; Cat Zakrzewski, Pranshu Verma &Claire ParkerTexts, Web Searches about Abortion Have Been Used to Prosecute Women, Washing. Post (Jul. 3, 2022), https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/.

[82] Health Breach Notification Rule, 89 Fed. Reg. 47028 (May 20, 2024).

HIPAA to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data.[83] It also requires third party service providers to vendors of PHRs and PHR related entities to notify such vendors and PHR related entities following the discovery of a breach.[84] Since the FTC enacted its initial HBNR in 2009, the number of health tracking apps has dramatically increased, and *Dobbs* has created new health privacy risks, motivating the FTC to expand the HBNR to cover newer types of data collection. The final rule requires entities that manage personal health records (but are not subject to HIPAA) to notify the FTC, the consumer, and in some cases the media following a breach of personally identifiable health data. The update of the rule clarifies its applicability to health apps and strengthens the notification mechanisms in this space.

Although to date Congress has failed to enact comprehensive federal privacy protections for health data that sits outside of HIPAA, states including Washington, Connecticut, and California have enacted data privacy protections that either include or specifically address sensitive health data—as well as other forms of sensitive data that may be used to determine health status and activities.

Conclusion

Health information privacy has always been critical to assuring that individuals can receive care for potentially stigmatizing health conditions. The Dobbs decision amplified concerns about the use of health information against individuals (or persons who assist them, including medical providers) and is likely to have far reaching consequences for the delivery of health care for certain conditions or populations. Time will tell whether current efforts by federal and some state regulators to shore up the privacy of reproductive health information will have the desired effect of extending greater protections for this information and, consequently, for access to care. ●

---

[83] Press Release, Fed. Trade. Comm'n, FTC Finalizes Changes to the Health Breach Notification Rule (Apr. 26, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule.

[84] *Id.*