ISSUE BRIEF

Safeguarding Reproductive Health Privacy After the Elimination of Federal Protections: Considerations for States Enacting Shield Laws

Maintaining the privacy of reproductive health information is critical for ensuring access to care, promoting open communication with providers, and preventing harm like stigma, harassment, and criminalization. The risks flowing from privacy violations are heightened for structurally marginalized communities, such as people of color and people with low or no income, who disproportionately experience oversurveillance and barriers to care. In 2024, recognizing the need to safeguard privacy amidst increased hostility to reproductive rights, the U.S. Department of Health and Human Services (HHS) issued a new rule to protect reproductive health privacy under the Health Insurance Portability and Accountability Act (HIPAA). The privacy protections in this HIPAA Privacy Rule to Support Reproductive Health Care Privacy (the 2024 Final Rule) were valuable but short lived; in June 2025, about a year after its effective date, the 2024 Final Rule was invalidated by a federal court.

Now that the 2024 Final Rule is no longer in effect, state laws may play an outsized role in protecting the privacy of reproductive health information. About half of the states have enacted what are known as "shield laws" to protect access to reproductive health care, and most include some level of privacy protections for reproductive health information. Following the 2024 Final Rule's elimination, states may consider revisiting their shield laws and addressing any resultant gaps in the privacy of health information held by entities regulated by HIPAA. This issue brief aims to support policymakers and others considering enactment of additional state-level protections. To that end, it describes the 2024 Final Rule's protections that are no longer in effect and identifies HIPAA provisions that could leave reproductive health information vulnerable to punitive use and disclosure. It then provides a general overview of privacy-related state shield laws, analyzes how they relate to the 2024 Final Rule, and identifies considerations for enactment of additional protections, providing state law examples for others to draw from.

PRIVACY PROTECTIONS UNDER HIPAA

FORMER PROTECTIONS FOR REPRODUCTIVE HEALTH PRIVACY UNDER THE 2024 FINAL RULE

In the spring of 2024, HHS issued the HIPAA Privacy Rule to Support Reproductive Health Care Privacy, which went into effect that June. The 2024 Final Rule applied to HIPAA covered entities (health plans, health care clearinghouses, and most health care providers) and their business associates (entities that perform certain functions or services for or on behalf of covered entities or other business associates) (collectively, "HIPAA regulated entities"). The 2024 Final Rule created additional prohibitions on certain uses and disclosures of protected health information (PHI) for non-health care purposes. Specifically, the 2024 Final Rule prohibited HIPAA regulated entities from using or disclosing PHI to conduct a civil, criminal, or administrative investigation into, or to impose civil, criminal, or administrative liability on, any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that was lawful under the circumstances in which it was provided. The 2024 Final Rule additionally prohibited HIPAA regulated entities from using or disclosing PHI to identify someone for one of these purposes.

If the entity receiving a request for information did not provide the reproductive health care in question, the 2024 Final Rule applied a presumption that the care was provided lawfully. The 2024 Final Rule also created a requirement that HIPAA regulated entities receiving certain requests for PHI potentially related to reproductive health care obtain a signed attestation from the requestor verifying that the PHI would not be used or disclosed for a prohibited purpose. The attestation requirement applied to disclosures of PHI for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, and to coroners and medical examiners.

Additionally, the 2024 Final Rule defined several terms, including "person" and "public health." "Person" was defined to exclude a fertilized egg, embryo, and fetus. This definition clarified that certain uses and disclosures permitted by HIPAA do not serve as avenues for disclosing PHI to investigate or impose liability on someone for providing, seeking, obtaining, or facilitating lawful reproductive health care. For example, under certain circumstances, HIPAA permits a HIPAA regulated entity to disclose an individual's PHI without authorization if it in good faith believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and if the disclosure is to a person reasonably able to prevent or lessen the threat. The new definition of "person" clarified that the person whose health or safety is threatened could not be a fertilized egg, embryo, or fetus.

The 2024 Final Rule defined "public health" as population level activities to prevent disease in and promote the health of populations, specifying that such activities do not include investigating or imposing liability on someone for providing, seeking, obtaining, or facilitating lawful reproductive health care. This definition thus clarified that a HIPAA regulated entity could not circumvent the 2024 Final Rule's prohibitions by sharing PHI pursuant to the HIPAA provision permitting disclosure for public health activities.

The 2024 Final Rule also made changes to narrow law enforcement access to PHI under circumstances where such access would not be barred by the 2024 Final Rule's prohibitions related to reproductive health care. Specifically, for disclosures of PHI pursuant to administrative requests for law enforcement purposes, the 2024 Final Rule clarified that PHI may only be disclosed if the administrative request is one "for which a response is required by law." HHS explained that this had always been the case but that clarification was necessary to dispel longstanding confusion among HIPAA regulated entities about whether disclosures for law enforcement purposes pursuant to administrative requests are permissible even if disclosure is not legally required. This clarification applied to disclosures for all law enforcement purposes, not only those related to reproductive health care.

In June 2025, a federal judge in the U.S. District Court for the Northern District of Texas found the 2024 Final Rule to be unlawful and invalidated almost all of its provisions.[1] That case, *Purl v. Department of Health & Human Services*, thus eliminated the reproductive health privacy protections. Importantly, the *Purl* decision did not eliminate the longstanding general protections for PHI in the HIPAA Privacy Rule.

CURRENT PROTECTIONS AND GAPS UNDER THE HIPAA PRIVACY RULE

State shield laws that cover HIPAA regulated entities build on the baseline federal protections in the HIPAA Privacy Rule, which were not eliminated by the *Purl* decision. Generally, the HIPAA Privacy Rule prohibits HIPAA regulated entities from using or disclosing PHI without an individual's authorization unless one or more of the Privacy Rule's exceptions to this general prohibition apply. Thus, notwithstanding the *Purl* decision, a HIPAA regulated entity cannot disclose reproductive health information that constitutes PHI without individual authorization absent an applicable exception. Unfortunately, the Privacy Rule contains numerous exceptions that could, if certain conditions are met, be exploited by state actors and others seeking to obtain and use PHI to target reproductive health care. The following list identifies several of these gaps in protections. HIPAA regulated entities should note that these provisions, while they may permit disclosure under certain circumstances, **do not by themselves compel disclosure of PHI.** Further, other privacy laws may prohibit

disclosure even when it is permissible under these provisions. HIPAA regulated entities should consult with their legal counsel to determine whether disclosures of PHI in connection with reproductive health care are permissible and obligatory.

- **Disclosures for law enforcement purposes:** 45 C.F.R. 164.512(f) permits HIPAA regulated entities to disclose PHI to a law enforcement official for law enforcement purposes as required by law or in response to a court order, subpoena, summons, or administrative request if certain conditions are met. Additionally, under certain conditions, it permits disclosure of PHI in response to a law enforcement request seeking to identify or locate a suspect, fugitive, material witness, or missing person or in response to a request seeking information about an individual who is or is suspected to be a victim of a crime. Under certain circumstances, HIPAA regulated entities may also disclose PHI to law enforcement to identify a decedent, to report a crime on the premises, and to report a crime in an emergency.
- **Disclosures for judicial and administrative proceedings:** 45 C.F.R. 164.512(e) permits HIPAA regulated entities to disclose PHI in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal or, if certain conditions are met, in response to a subpoena, discovery request, or other lawful process. For example, a HIPAA regulated entity may disclose PHI in response to a subpoena, discovery request, or other lawful process if it receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to obtain a qualified protective order. The qualified protective order must prohibit the use or disclosure of PHI for any purpose other than the litigation or proceeding and require return or destruction of the PHI once the litigation or proceeding ends.
- **Disclosures for public health purposes:** 45 C.F.R. 164.512(b) permits HIPAA regulated entities to disclose PHI for public health activities and purposes, such as public health surveillance, investigations, and interventions, to a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability.[2]
- **Disclosures to report abuse:** 45 C.F.R. 164.512(b) permits HIPAA regulated entities to disclose PHI to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect. Further, under certain circumstances, 45 C.F.R. 164.512(c) permits HIPAA regulated entities to disclose PHI about an individual whom the entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government agency authorized by law to receive reports of such incidents.[3]
- **Disclosures for health oversight activities:** 45 C.F.R. 164.512(d) permits disclosure of PHI to a health oversight agency for oversight activities authorized by law, including but not limited to audits, investigations, inspections, and licensure actions, for oversight of the health care system, government benefit programs, and compliance with regulatory programs and civil rights laws.[4]

PRIVACY-RELATED STATE SHIELD LAWS AND CONSIDERATIONS AFTER *PURL*

State shield laws vary substantially, but, as a general matter, they prohibit conduct that could further out-of-state investigations, enforcement actions, or prosecutions targeting reproductive health care (and, in some states, gender-affirming care[5]) that is lawful under the laws of the shield law state. Such care is often referred to as "legally protected care," "legally protected health care," "legally protected health care activity," or another similar term. Most states with shield laws include some level of privacy protections that seek to reduce the risk of information being shared with individuals or entities in states that penalize the provision or receipt of reproductive health care. Many of these serve purposes that differ from that of the 2024 Final Rule, with its exclusive focus on protecting PHI held by HIPAA regulated entities. But some state protections do apply to

HIPAA regulated entities, building on the floor created by HIPAA, which permits states to implement more stringent privacy standards.

State shield laws, many of which predated the 2024 Final Rule, play a critical role in protecting reproductive health privacy and will continue to do so following the 2024 Final Rule's elimination. But in some shield law states, the 2024 Final Rule may have provided supplementary protections for PHI held by HIPAA regulated entities, the loss of which may leave reproductive health information more vulnerable. As discussed above, the Privacy Rule's general protections for PHI are still in effect, but these are limited and permit disclosure for purposes like law enforcement activities, judicial and administrative proceedings, and public health activities that could be exploited by out-of-state agencies or others targeting reproductive health care. State shield laws thus provide a crucial avenue for reinforcing safeguards in the wake of the *Purl* decision eliminating the 2024 Final Rule.

The following is a non-exhaustive list of types of privacy-related shield laws with analysis of how they may fill the gaps in privacy protections for HIPAA regulated entities resulting from the *Purl* decision. The Center on Reproductive Health, Law, and Policy at UCLA Law maintains a tracker of shield laws that policymakers may find useful for understanding the protections available and potential gaps in their specific state.

RESTRICTIONS ON DISCLOSURE AND USE BY HEALTH CARE PROVIDERS AND OTHER REGULATED ENTITIES

Many shield law states restrict use and disclosure of reproductive health information by health care providers and other HIPAA regulated entities. In general, these shield laws are the most similar to the 2024 Final Rule. However, they vary significantly with respect to the entities that they cover and the types of uses and disclosures that they prohibit. Some provide narrower protections while others include safeguards that go beyond those in the 2024 Final Rule and can serve as examples for states striving for more comprehensive privacy protections.

Delaware's law is an example of a relatively narrow restriction. It applies to health care providers and prohibits disclosure of certain reproductive health information "in any civil action or proceeding," absent authorization from the patient, their guardian, or their legal representative. This prohibition does not apply under certain circumstances, including if the records are requested by a health care licensing board in connection with an investigation of a complaint or if the records are requested by law enforcement or other agencies in connection with an investigation of abuse. 10 Del. Code § 3926A.

As it only applies to health care providers, this law would not protect against uses and disclosures by other kinds of HIPAA regulated entities, like health plans (although Delaware's law may cover more health care providers than HIPAA, which only applies to health care providers that engage in certain kinds of transactions). Additionally, Delaware's law only prohibits a narrow set of disclosures (e.g., disclosures in civil actions or proceedings) and may not protect against uses and disclosures under other circumstances, such as criminal or administrative proceedings. Furthermore, broad exceptions for healthcare oversight activities and reports of abuse could be exploited as a pretext to circumvent prohibitions.

States looking for a more extensive approach might turn to **Vermont** as an example. Vermont's law, which partially predated the 2024 Final Rule, contains certain parallels with the 2024 Final Rule's eliminated prohibitions. It prohibits HIPAA regulated entities from disclosing PHI "that is identifiable or susceptible to reidentification and is related to a legally protected health care activity" to any government entity other than the State of Vermont or its local governments if the HIPAA regulated entity has reason to believe that the PHI will be used to conduct a criminal, civil, administrative or professional investigation into, or to impose criminal, civil, or administrative liability or professional disciplinary action on, "any individual for the mere act of seeking, obtaining, providing or facilitating a legally protected health care activity." The prohibition also applies if the regulated entity has reason to believe the PHI will be used to identify an individual for any of these activities.

Additionally, HIPAA regulated entities must not disclose PHI that is identifiable or susceptible to reidentification and related to a legally protected health care activity "for use in a civil or criminal action; a proceeding preliminary to a civil or criminal action; or a probate, legislative, or administrative proceeding." Vermont law shields HIPAA regulated entities from civil, criminal, or administrative liability or professional discipline for refusal to disclose PHI pursuant to these prohibitions. But disclosure is permitted under specified circumstances, such as with the patient's authorization. Disclosure is also permissible pursuant to a court order under federal or Vermont law but, if the order is issued by a state court, it must include a determination that the PHI will not be used for a prohibited purpose. The law further permits disclosure to specified Vermont state agencies for various purposes, like investigating licensed health care facilities. Vt. Stat. tit. 18, § 1881.

Thus, Vermont's law goes several steps further than the 2024 Final Rule. The reasonable belief standard clarifies that a regulated entity need not know with certainty that the disclosure is for a prohibited purpose. Further, the law includes a prohibition on uses and disclosures in connection with professional disciplinary actions, in addition to criminal, civil, and administrative actions. It also specifies that PHI may not be disclosed in other types of proceedings, like probate and legislative proceedings. And it shields HIPAA regulated entities from liability or disciplinary action for refusal to disclose PHI pursuant to the law's prohibitions. These additional safeguards strengthen the privacy of sensitive information vulnerable to misuse. Furthermore, by identifying specific Vermont agencies that may receive PHI under the law's exceptions, rather than permitting disclosure to governmental agencies or law enforcement agencies generally, Vermont reduces the risk that such exceptions inadvertently serve as avenues for disclosing PHI to out-of-state agencies targeting reproductive health care.

California takes a different approach. One of its shield laws states that "a provider of health care, health care service plan, contractor, or employer shall not release medical information related to an individual seeking or obtaining an abortion in response to a subpoena or request if that subpoena or request is based on either another state's laws that interfere with a person's [reproductive rights under California law] or a foreign penal civil action." Additionally, a health care provider, health care service plan, contractor, or employer must not release medical information that would identify an individual or that is related to an individual seeking or obtaining an abortion to law enforcement for the above purposes.

The law further states that "a provider of health care, health care service plan, contractor, or employer shall not cooperate with any inquiry or investigation by, or provide medical information to, any individual, agency, or department from another state or, to the extent permitted by federal law, to a federal law enforcement agency that would identify an individual and that is related to an individual seeking or obtaining an abortion or abortion-related services that are lawful under the laws of [California]," with certain exceptions. Cal. Civil Code § 56.108.

California has additionally passed measures focused on limiting disclosure of information out of state through electronic information systems. Specifically, it prohibits health care providers, health care service plans, pharmaceutical companies, contractors, and employers from disclosing certain reproductive health information out of state through an electronic health records (EHR) system or a health information exchange (HIE) except if clear written authorization is provided, the disclosure is necessary for payment, or other conditions are satisfied. Cal. Civil Code § 56.110. It further requires that business entities that electronically store or maintain medical information on behalf of health care providers, health care service plans, pharmaceutical companies, contractors, or employers develop capabilities, policies, and procedures to safeguard information related to abortion, abortion-related services, and contraception. Specifically, these business entities must develop system capabilities to limit user access privileges, prevent disclosure of protected information out of state, segregate protected information, and automatically disable access to segregated information by out-of-state individuals or entities. The business entities covered by this part include but are not limited to EHR vendors, HIEs, and health information networks (HIN). Cal. Civil Code § 56.101.

While the structure of California's law differs from that of the 2024 Final Rule, it similarly prohibits disclosures of information that interfere with lawful reproductive health care. However, California's law is broader than the 2024 Final Rule in certain respects. It prohibits disclosures in response to a "request" based on another state's

laws that interfere with a person's reproductive rights, which could be read to cover circumstances beyond the investigations and impositions of liability covered by the 2024 Final Rule. It also broadly prohibits the provision of information to out-of-state individuals, agencies, and departments without focusing on punitive purposes. And it requires entities like HIEs and EHR systems to develop capabilities to prevent disclosure of reproductive health information across state lines. On the other hand, it focuses narrowly on certain subsets of information (e.g., information related to abortion and abortion-related services) while the 2024 Final Rule did not limit its application to specific types of PHI. Purpose-based protections that apply to all PHI used or disclosed for certain purposes can help to ensure that patient privacy is more fully protected and, as HHS explained in the 2024 Final Rule, can help to avoid the imposition of onerous data segmentation requirements on HIPAA regulated entities. Policymakers weighing restrictions based on purpose against those based on information type should consider the technological feasibility of data segmentation in their jurisdictions.

Another important consideration for policymakers analyzing gaps in privacy protections following *Purl* is the limited breadth of shield laws. Unlike the 2024 Final Rule, state shield laws do not apply on a nationwide basis. In the course of treatment or payment, reproductive health information might move from a state with shield laws to a state without them, leaving the information vulnerable to punitive uses. Some states have partially addressed this concern by requiring consent for disclosure of reproductive health information for treatment purposes. **Maryland**, for instance, requires patient consent to disclose certain reproductive health information to treating providers through a HIE or HIN. Md. Code Ann., Health-Gen. § 4-302.5. As discussed above, **California** similarly prohibits certain entities from transmitting reproductive health information out of state through an EHR system or HIE unless authorization is provided or other conditions are met. Cal. Civil Code § 56.110. When designing and implementing such requirements, policymakers and HIPAA regulated entities should consider how to best support patients in making informed consent decisions and how to strike an appropriate balance between sharing information to promote quality treatment and preventing harmful uses and disclosures.

Policymakers may also consider adopting definitions in their shield laws that mirror the 2024 Final Rule's definitions of "person" (to exclude fertilized eggs, embryos, and fetuses) and "public health" (to exclude prohibited purposes). Doing so can help to ensure that any statutory provisions permitting use or disclosure for purposes like reporting suspected abuse, identifying victims, and engaging in public health activities cannot be leveraged as a pretext for targeting reproductive health care.

RESTRICTIONS ON PROVISION OF INFORMATION BY STATE AGENCIES, EMPLOYEES, AND CONTRACTORS

Most states with shield laws restrict the ability of state agencies, employees, contractors, or others acting under the color of state law to share information to advance investigations targeting reproductive health care that is legally protected in the state.

For example, **Illinois** law provides that state and local agencies, officials, and others acting under color of state or local law "shall not provide any information . . . to assist any individual, or out-of-state officer, official, agency, entity, or department seeking to impose civil or criminal liability upon a person or entity for lawful health care activity," unless otherwise necessary to comply with Illinois or federal law. 735 Ill. Comp. Stat. § 40/28-11.

Similarly, **New York** prohibits state and local government employees and entities or persons acting on their behalf from "provid[ing] information to any out-of-state individual or out-of-state agency or department regarding any legally protected health activity . . . in furtherance of any investigation or proceeding that seeks to impose civil or criminal liability, professional sanctions, or any other legal consequences upon a person or entity for any legally protected health activity." This law does permit the commissioner of health to disclose such information for certain public health purposes, but identified information may be disclosed only when strictly necessary and with consent. N.Y. Exec. Law § 837-x.

These shield laws may provide additional protections for PHI held by HIPAA regulated entities that are state or local governmental bodies or their contractors, such as state and local health departments and state- and local-run hospitals. However, because these laws typically leave out HIPAA regulated entities that are not state or local bodies or their contractors, they do not entirely fill the gaps left by the elimination of the 2024 Final Rule. **Colorado** takes an approach that broadens the application of these protections, serving as a potential example for states looking to encompass more HIPAA regulated entities under such laws. In a bill passed in 2025, Colorado revised its law to include not only public entities and those working on their behalf, but also "a person or entity licensed or regulated by the state," thus extending these protections to licensed health care providers regardless of whether they are public entities. Colo. Rev. Stat. §§ 24-116-101, 24-116-102.

RESTRICTION ON ISSUANCE AND ENFORCEMENT OF WARRANTS, SUBPOENAS, AND OTHER JUDICIAL INSTRUMENTS

Another very common type of shield law is a prohibition on courts' issuance or enforcement of warrants, subpoenas, *ex parte* orders, summons, or other instruments of investigation or discovery that could compel the disclosure of reproductive health information.

In **Maryland**, for example, "[a] judge may not order a person within the [s]tate to give testimony or a statement, or produce documents, electronically stored information, or other tangible things" in a pending prosecution or a grand jury investigation "for a violation of a criminal law of another state involving the provision of, receipt of, or assistance with legally protected health care" in Maryland, unless the underlying facts would constitute a crime in Maryland. Md. Code Ann., Cts & Jud. Proc. § 9-302(b)(2). Judges in Maryland are also prohibited from issuing ex parte orders authorizing interception of wire, oral, or electronic communications for the purpose of investigating or recovering evidence of actions related to legally protected health care, unless the underlying facts would constitute a crime in Maryland. Md. Code Ann., Cts. & Jud. Proc. § 10-408(c)(5).

Further, when requesting issuance of a subpoena based on an out-of-state subpoena, the request must "include a sworn, written statement signed under penalty of perjury by the party seeking enforcement, or the party's counsel, that no portion of the subpoena is intended or anticipated to further any investigation or proceeding related to legally protected health care," unless the underlying claim is brought by the patient who received the care or is based on conduct that would be prohibited under Maryland's laws. Md. Code Ann., Cts & Jud. Proc. § 9-402(a)(2)(ii).

These laws create powerful limits on the use of judicial instruments to compel disclosure of reproductive health information, but they generally do not address demands for or disclosures of PHI that are made outside of the judicial process of the shield law state. Many of the Privacy Rule exceptions that could permit disclosure of PHI targeting reproductive health care do not require a court order or other judicial instrument legally compelling disclosure. This is even more true following the elimination of the 2024 Final Rule's clarification that if a HIPAA regulated entity discloses PHI to law enforcement pursuant to an administrative request, that request must be one for which a response is required by law.[6] Furthermore, an out-of-state agency could usurp the restrictions in these shield laws by presenting a HIPAA regulated entity with a request for information pursuant to a judicial instrument issued in the agency's state (rather than the shield law state). Even if this is procedurally improper and the judicial instrument is not enforceable in the shield law state, a regulated entity may not recognize as much.

CONSUMER HEALTH DATA PRIVACY LAWS

In addition to shield laws, a growing number of states are enacting consumer health data privacy laws, some of which include special protections for reproductive health information.

For example, **Washington's** My Health My Data Act prohibits business entities from collecting or sharing consumer health data, including reproductive or sexual health information, except with the consumer's consent or to the extent necessary to provide a product or service that the consumer has requested. RCW 19.373.030.

Among other protections, this law additionally prohibits implementation of "a geofence around an entity that provides in-person health care services where such geofence is used to: (1) Identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services." RCW 19.373.080. The My Health My Data Act expressly does not apply to PHI subject to HIPAA. RCW 19.373.100.

These consumer health data privacy laws apply critical privacy protections to consumer information that could be used to target reproductive health care. But they do not fill the gaps in privacy protections following *Purl* because they typically exclude from their coverage HIPAA regulated entities and/or HIPAA PHI. In fact, these laws generally apply to business entities with the intent of filling privacy gaps resulting from HIPAA's limited application to covered entities and business associates. Washington's law, for example, expressly notes that Washington consumers expect their health data to be protected by privacy laws like HIPAA, and, by creating protections for non-HIPAA regulated entities, the law seeks to better align industry practice with consumer expectations. RCW.19.373.005. However, particularly after *Purl*, HIPAA itself leaves reproductive health information vulnerable to punitive use and disclosure, highlighting the need for more robust protections applicable to HIPAA regulated entities in addition to the business entities covered by these consumer health data privacy laws.

ADDITIONAL PRIVACY-RELATED SHIELD LAWS

Some shield law states have passed other types of privacy protections for reproductive health information, such as exemptions from disclosure under public record laws for reproductive health care-related records,[7] provisions permitting providers to participate in address confidentiality programs,[8] and confidentiality protections on prescription drug labels.[9] While they create important privacy safeguards, these laws serve narrower purposes than the 2024 Final Rule and do not provide robust protection for reproductive health information held by HIPAA regulated entities.

CONCLUSION

In the wake of the 2025 federal court decision eliminating the HIPAA Privacy Rule to Support Reproductive Health Care Privacy, state shield laws can continue to provide critical protections for reproductive health information held by HIPAA regulated entities. These state-level safeguards are paramount given that the HIPAA Privacy Rule contains multiple provisions that could lead to use or disclosure of information to target lawful reproductive health care. With a better understanding of the different types of state-level privacy protections and how they relate to the 2024 Final Rule, states can adjust their safeguards to fill any gaps in the absence of more robust federal protections.

The shield laws that are most similar to the 2024 Final Rule's protections are those that apply to HIPAA regulated entities and restrict uses and disclosures in connection with civil, criminal, and administrative investigations or proceedings targeting reproductive health care. This issue brief highlights how these laws can most effectively protect the privacy of PHI held by HIPAA regulated entities. Other shield laws, like those that limit public employees' disclosure of information in investigations and those that prohibit issuance or enforcement of judicial instruments compelling disclosure, can support the privacy of reproductive health information held by HIPAA regulated entities but are limited in their scope and most effective in combination with other privacy protections.

When considering the potential of new or amended shield laws, policymakers should work with their legal counsel to understand the privacy landscape in their state, including current shield laws as well as other kinds of privacy protections. While, on its own, a shield law may seem limited, acting in conjunction with other privacy laws, it may play a role in effectively protecting the privacy of PHI. Close consultation with legal counsel is critical for understanding potential threats to reproductive health information and for developing privacy safeguards that protect access to care in climates increasingly hostile to reproductive rights.

This document was developed by Emma Kaeser, J.D., Staff Attorney, Network for Public Health Law – Mid-States Region. The Network promotes public health and health equity through non-partisan educational resources and technical assistance. These materials provided are provided solely for educational purposes and do not constitute legal advice. The Network's provision of these materials does not create an attorney-client relationship with you or any other person and is subject to the Network's Disclaimer.

SUPPORTERS
Support for this work is provided by the Robert Wood Johnson Foundation and the Kresge Foundation. The views expressed in this document do not necessarily reflect the views of the Foundation.

[1] The decision left intact several provisions relating to modifications to the Notice of Privacy Practices that do not pertain to reproductive health privacy.

[2] Generally, this public health exception is applied to promote and protect population health. However, some states have recently sought to expand collection and disclosure of reproductive health information for punitive purposes pursuant to laws requiring providers to report abortions to public health authorities.

[3] The 2024 Final Rule reflected concern that the HIPAA provisions permitting disclosure of abuse could be used to target reproductive health care. Such targeting could occur either under the theory that the provision of reproductive health care could constitute abuse of the patient or under the theory that it is abuse of a fetus. The latter theory is a particularly salient threat in jurisdictions that have fetal personhood laws granting fetuses the same legal rights given to humans born alive.

[4] While health oversight activities generally do not target reproductive health care, the 2024 Final Rule noted the risk of an investigation of substandard medical care or other oversight activities being used as a pretext for targeting reproductive health care. This risk is already a reality in the gender-affirming care context; according to a U.S. Senate Finance Committee investigation, some state attorneys general have weaponized health oversight authority to target trans youth and their providers, demanding health records related to gender-affirming care for purported purposes like investigating Medicaid fraud.

[5] This issue brief focuses on the privacy of information related to reproductive health care, but many of the concerns described are relevant for the privacy of information related to gender-affirming care as well, and the considerations raised may likewise guide policymakers exploring more robust privacy protections for gender-affirming care.

[6] In the 2024 Final Rule, HHS takes the position that 45 C.F.R. § 164.512(f)(1), which permits disclosures for law enforcement purposes "[p]ursuant to process and as otherwise required by law," has always required that the disclosure be required by law. Thus, the 2024 Final Rule's specification that an administrative request must be one "for which response is required by law" is simply a clarification of this preexisting position. But HHS recognized in the 2024 Final Rule that some HIPAA regulated entities interpret § 164.512(f)(1) to permit disclosure in response to an administrative request even if a response is not required by law. Thus, even if it has been HHS's intent to only permit disclosures required by law under § 164.512(f)(1), without the 2024 Final Rule's clarification, HIPAA regulated entities may continue to respond to law enforcement demands when not legally compelled to do so.

[7] For example, Maryland law states that a public records custodian must deny inspection of a public record that contains the name or other identifying information of an individual related to a licensed ambulatory surgical facility (with limited exceptions) or a licensed surgical abortion facility. A custodian must also deny inspection of a public record that relates to an investigation of a licensee or certificate holder regarding the provision of legally protected health care, pending a final order. Md. Code Ann., Gen. Provisions § 4-333.

[8] Maine's Address Confidentiality Program is an example of one that permits reproductive health care services practitioners to apply to have a designated address assigned by the Secretary of State to avoid disclosure of their actual address. It does, however, permit disclosure of actual addresses to law enforcement and other agencies under certain circumstances. 5 Me. Rev. Stat. § 90-B.

[9] For example, Massachusetts permits health care providers to request that the label for a controlled substance prescribed for reproductive health care services state the name of the practice, rather than the name of the provider. Mass. Gen. Laws ch. 94C, § 22(d).