ConnectedHealthInitiative

June 16, 2023

Honorable Xavier Becerra
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW
Washington, District of Columbia 20201

RE: HIPAA Privacy Rule to Support Reproductive Health Care Privacy (HHS-OCR-2023-0006; 88 FR 23506)

Dear Secretary Becerra:

The Connected Health Initiative (CHI) appreciates the opportunity to respond to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) on its proposal to modify the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) to limit uses and disclosures of protected health information (PHI) by prohibiting uses and disclosures of PHI for criminal, civil, or administrative investigations or proceedings against individuals, covered entities or their business associates, or other persons for seeking, obtaining, providing, or facilitating reproductive health care that is lawful under the circumstances in which it is provided.[1]

I. Introduction & Statement of Interest

CHI is the leading effort by stakeholders across the connected health ecosystem to enable the responsible deployment and use of digital health tools throughout the continuum of care, supporting an environment in which patients and consumers can see improvements in their health. Across a range of touchpoints in the healthcare ecosystem, we seek essential policy changes that will enable all Americans to realize the benefits of an information and communications technology-enabled American healthcare system. For more information, see www.connectedhi.com.

[1] 88 FR 23506.

II. The Connected Health Initiative's Commitment to Protecting Sensitive Health Data and the Need for Clarity Under HIPAA

No data is more personal to Americans than their own health data, particularly for sensitive areas such as reproductive health. CHI members acknowledge and respect the significant threats to Americans' most sensitive data and put extensive resources into ensuring the security and privacy of health data to earn the trust of consumers, hospital systems, and providers.

The HIPAA privacy and security rules provide a set of minimum standards for protecting all electronic PHI that a covered entity and business associate create, receive, maintain, or transmit.[2] The concerns addressed by these laws are taken seriously by CHI members, who in turn work to meet the letter and spirit of the law. However, HIPAA privacy and security rules and guidance applicable to basic modern technology modalities, such as mobile apps, have fallen woefully out of touch with today's technology, and the persistent lack of clarity around HIPAA applicability in a mobile environment prevents many patients from benefiting from these services. As a result, many providers and patients find themselves discouraged from leveraging basic technologies. While OCR has developed a limited audit program in sub-regulatory guidance for assessing covered entities' controls and processes,[3] and HHS has issued guidance with specific scenarios which may be helpful in a narrow range of circumstances,[4] regulatory relief, or, at minimum, more guidance, is needed to address the use of new innovative modalities and software app-powered products and services that facilitate the flow of PHI.

CHI believes that as OCR continues to work to improve the HIPAA rules to meet the needs of our changing industry and standards of care, it is imperative that OCR continues to work to ensure that the HIPAA rules do not unduly restrict the ability of covered entities and their business associates to use the most efficient and secure technologies in their operations. CHI has detailed many ways that OCR can improve HIPAA rules to advance connected care while protecting patient privacy in previous public comments,[5] which we urge OCR to consider acting consistent with in this matter and its general efforts to improve HIPAA.

---

[2] 45 CFR Part 160; 45 CFR Part 164 Subparts A and C.

[3] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.

[4] http://hipaaqsportal.hhs.gov/a/pages/helpful-links.

[5] CHI comments to OCR detailing the range of ways that HIPAA regulations should be updated to protect patients while enabling the use of new technologies can be found at https://www.regulations.gov/comment/HHS-OCR-2018-0028-1188.

III. Connected Health Initiative Input on Proposed HIPAA Privacy Rule Changes to Support Reproductive Health Care Privacy

Increased collection and use of patient-generated health data (PGHD) is positively transforming, and will continue to positively transform, the U.S. healthcare ecosystem. A well-established and growing evidence base demonstrates that the collection of PGHD through a range of modalities and its use for timely healthcare decisions advances the Quadruple Aim. Yet, the potential for sensitive PGHD being leveraged against patients for civil or criminal proceedings is undoubtedly a theme that has concerned the entire ecosystem, and for this reason CHI supports OCR's general goals in this matter. Already, CHI has worked to inform the digital health ecosystem's consideration of the unique challenges arising from the *Dobbs v. Jackson Women's Health Org.* decision, which has given rise to a range of challenges, including but not limited to those which are privacy related.[6]

In the wake of the *Dobbs* decision, some state policymakers are responding with updates to health-related policies. In addition, federal and state consumer protection enforcement agencies have recently prioritized the investigation of the collection, use, and transfer of reproductive information—including health data—occurring under existing law outside the scope of the HIPAA.[7] Further, alongside federal and state consumer privacy laws, several states will have or already have comprehensive privacy laws to enforce.[8] OCR's timely action in light of the *Dobbs* decision is a critical step in addressing significant new HIPAA questions that have arisen.

Noting our general support for OCR's goals, we offer the following recommendations on its proposals:

- *OCR's Attestation Requirements Should Be Refined to Make Compliance Objective and Reasonable:* OCR's proposed attestation requirements in 42 CFR §164.509(a) would obligate covered entities and the business associates to obtain signed attestations from specified PHI requesters (health oversight activities, judicial and administrative proceedings, law enforcement purposes, or disclosures to coroners and medical examiners) that the use or disclosure will not be used against an individual for seeking, obtaining, providing or facilitating reproductive healthcare when that request for PHI is "potentially

[6] CHI's detailed memo addressing issues for digital health raised by the *Dobbs* decision is included in this filing as **Appendix A**.

[7] Fed. Trade Comm'n, *Flo Health Inc.*, FTC Matter No. 192 3113, settlement (Jun. 22, 2021), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc; Fed. Trade Comm'n, *BetterHelp*, proposed settlement (Mar. 2, 2023), *available at* https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook; Office of the Atty. Gen., State of Calif., "Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information," (May 26, 2022), *available at* https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect.

[8] States with comprehensive privacy statutes include Virginia, Colorado, California, Utah, Connecticut, and Iowa.

related to reproductive healthcare." CHI urges OCR to take steps to avoid placing covered entities and their business associates in the unworkable position of deciding what is "potentially related" to reproductive health. Alternatively, CHI urges OCR to leverage approach taken in 42 CFR Part 2 to protect substance use disorder (SUD) patient privacy, which places the restriction on the data rather than specifying particular entities, and simply require attestations from a requester. Taking this approach would also further OCR's goal of harmonizing HIPAA and Part 2. Combined with CHI's recommended approach to general attestations, healthcare providers can incorporate an attestation feature into their workflows to efficiently meet OCR's requirements and protect patient safety. In addition, CHI notes that any attestation or paper form requirement makes it more difficult for patients to access health care remotely, is inherently less secure, and increases the burden on clinicians providing these services.

- *OCR Should Resolve the Unintended Creation of New Liabilities in its Proposed New Category of Prohibited Uses and Disclosures:* CHI is supportive of OCR's intent in its proposal to prevent a covered entity from using or disclosing PHI for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive healthcare in §164.502(a)(5)(iii). However, OCR's proposal would hold a provider responsible for a HIPAA violation when a recipient of PHI, unbeknownst to the provider, later chooses to use the data in a civil or criminal action using the data. In addition, under OCR's §164.502(a)(5)(iii)(C), providers would be required to determine whether previous care was lawfully provided in order to determine whether or not the PHI at issue must be protected by them.

  OCR can take needed steps to avoid exposing providers to liability for intent and actions of third parties by allowing a provider to ask a PHI requester for an attestation that the PHI will not be used against an individual for seeking, obtaining, providing or facilitating reproductive healthcare, and to be able to decline the request should that attestation be refused (and such a refusal should be protected from claims of illegal information blocking by ONC); and by clearly indicating that a provider will only face liability for a prohibited disclosure when the covered entity had actual knowledge that the PHI request is being made for the purpose of investigating or imposing civil or criminal liability on a person for seeking, obtaining, providing, or facilitating reproductive healthcare. These steps would ensure that covered entities and their business associates are not held responsible for requester's actions (or a requester's intent that may not even be revealed).

- *OCR Should Enhance Coordination with the National Coordinator for Health IT:* We also urge OCR to consider the impact of the *Dobbs* decision on the state of interoperability today and the barriers to interoperability (both related and unrelated to the *Dobbs* decision), as well as the status of related regulations being advanced by other agencies (e.g., ONC). CHI continues to push for the finalization and enforcement of much-needed information blocking rules. As new requirements phase in under this proposal from OCR, we urge for close coordination with ONC to ensure maximum alignment and that HHS' approach is coordinated. For example, as explained above, to resolve any ambiguities that may arise from this approach in the context of compliance with ONC information blocking rules, HHS should also clarify that, in the event of a requester refusing to provide an attestation, that refusal to provide the requested data does not constitute illegal information blocking.

IV. Conclusion

CHI appreciates the opportunity to submit comments to OCR and urges its thoughtful consideration of the above input.

Sincerely,

Brian Scarpelli
Executive Director

Leanna Wade
Regulatory Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005

APPENDIX A

ConnectedHealthInitiative

Data Privacy, Data Availability, and Other Risks for Health Tech in a Post-Dobbs World

Intro and Executive Summary

The Supreme Court's *Dobbs v. Jackson Women's Health* decision creates risks for health organizations and other entities that handle personal information relating to reproductive health services, including abortion.[1] In addition to the more direct impact on reproductive health providers (*i.e.*, government and private actions to enforce laws that limit abortion services in various circumstances), *Dobbs* also creates numerous data privacy, data availability, and other data-related risks, particularly for health technology companies. Many of these issues arise from the conflicting approaches states and federal agencies are likely to take as they seek to either more heavily restrict abortion services or expand or protect access to abortion—policy approaches that inevitably reach across state lines and will likely create conflicting obligations with respect to data management and privacy practices. These risks include:

1. *Dobbs* and resulting changes in state law significantly expand the types of organizations that are likely to receive law enforcement requests related to reproductive health care and significantly increases the likelihood of receiving such requests.
2. Existing law (HIPAA and other state/federal laws) in many cases does not shield entities subject to HIPAA from state law access requests for abortion-related data.
3. Covered entities under HIPAA will likely increase scrutiny of Business Associate Agreement provisions relating to law enforcements, subpoenas, and other similar disclosure pathways, costing more time and resources.
4. Health Information Exchanges ("HIE") are likely to receive requests for abortion-related data, which could indirectly lead to depressed HIE participation and, consequently, negatively impact unrelated care delivery due to decreased data quality and availability.
5. Abortion-friendly states may enact legislation prohibiting (or at least making it difficult for) Electronic Health Records ("EHR") to be transmitted across state lines (akin to privacy "data localization laws") to prevent EHRs and HIEs from disclosing abortion-related data when those entities also operate in states that now or may soon restrict abortion ("Restrictive States").
6. Organizations may leverage the ONC Information Blocking Rules to force abortion-related data sharing to ultimately make it available for state enforcement agencies.
7. Companies are likely to face conflicting pressure related to the FTC and state "unfair and deceptive acts and practices laws" with the FTC and states seeking to limit anti-abortion enforcement scrutinizing disclosures companies may make if required in states that restrict abortion services.

---

[1] For ease of reading, this paper will use the term "abortion" and "reproductive health" interchangeably to broadly encompass all reproductive health procedures and situations that might potentially be implicated in a post-*Dobbs* investigation, prosecution, licensure action, or other litigation. The boundaries of what constitute a potentially-unlawful abortion vary from state to state and are subject to rapid change. See Appendix A for a more detailed background on such laws.

8. Organizations may face private individual and class action litigation by consumers, providers, and other data subjects (both by individuals negatively impacted when organizations disclose abortion-related data and by individuals in states that permit private causes of action against entities that provide "abortion assistance").

The remainder of this white paper explores such data-related risks (both intended and unintended)**.** This paper is intended to be a starting point for organizations seeking to understand and manage such risks but is not a substitute for direct consultations with knowledgeable legal counsel to address organization- and jurisdiction-specific issues. Please see Appendix A for more detailed background on the post-*Dobbs* legal landscape, if desired.

Risk 1: Dobbs and resulting changes in state law significantly expand the types of organizations that are likely to receive law enforcement requests related to reproductive health information and significantly increases the likelihood of receiving such requests.

Organizations that handle any kind of reproductive health-related data are now more likely to be targeted by government officials and private litigants pursuing enforcement actions against those they perceive to have participated in unlawful abortions. The scope of data that state authorities and private actors may seek (and, consequently, the types of companies that may be targeted) is likely to expand significantly.[2] Many companies that previously may have received few, if any, requests for health information will now need to prepare for, navigate, and defend the myriad ways states and individuals might seek to access sensitive data. For example:

- Prosecutors can issue grand jury subpoenas and civil investigative demands for records and/or witness testimony, and now are more likely to do so with respect to reproductive health data.
- Official and private litigants can, either directly or with court approval (depending on state-specific rules), issue subpoenas for the same,[3] as can licensing boards/agencies involved in disciplinary investigations in many cases.
- Although far less frequent, law enforcement authorities can obtain and execute search warrants.
- Law enforcement officers or private investigators can also seek documents or information informally—either directly through "knock and talks" and the like or by sending in confidential informants posing as patients or other interested parties.

[2] As examples, consider: (1) paper and electronic medical records; (2) prescription data; (3) provider productivity/competency tracking data; (4) employee/insurance benefits data; (5) location data that may indicate presence at a women's health-focused provider and/or travel into and out of a Restrictive State; (6) period tracker application data; (7) online search data related to reproductive health services. Those are just a few among many.

[3] Generally speaking, most/all jurisdictions have statutes, rules, and/or caselaw that limit the scope of subpoenas based on factors such as the potential relevance of the information requested and the reasonableness of the burden associated with identifying, collecting, and producing it. Both HIPAA-regulated and non-HIPAA regulated entities should work with their legal counsel to identify collected data that could be subject to subpoena and brainstorm relevant strategies for contesting any such subpoenas.

Risk 2: Existing law (HIPAA and other state/federal laws) often does not shield entities subject to HIPAA from state law access requests for abortion-related data.

States already have numerous tools (beyond law enforcement powers) to obtain health (including abortion-related) data from entities HIPAA-regulated and non-regulated entities alike, and *Dobbs* may embolden states to enact even more specific laws mandating proactive abortion data disclosures. In addition to law enforcement powers (discussed further below), states can already obtain data through:

- Requests for, or direct access to, patient data by state boards of health and other health regulatory/licensure authorities;
- All-payer claims databases to which that many states require insurers to submit claims and other information; and
- Mandatory reporting requirements in situations where providers and others may be required to report suspected child abuse/neglect and/or of imminent threats of harm to the patient or others (often called *Tarasoff* or "duty to warn" requirements).

Restrictive States are likely to continue passing and amending their laws to specifically require disclosure of abortion-related data in these and other circumstances, especially as they encounter barriers to investigation and enforcement under current laws. For example, Restrictive States that view abortion as homicide of an "unborn child" may extend the "duty to warn" (through new legislation or evolving case law interpretation) to explicitly cover situations in which a provider knows or suspects a pregnant patient intends to imminently terminate the pregnancy, whether by traveling to another state or otherwise.[4]

HIPAA Permits Disclosures in Numerous Circumstances. Neither HIPAA nor existing laws provide sufficient mechanisms for entities to resist state attempts to obtain abortion-related data. To the contrary, HIPAA generally permits (but does not require) covered entities ("CEs") and their business associates ("BAs") to disclose PHI without patient notice/authorization in several specific circumstances:

- Disclosures to law enforcement officials:
    - To the extent required by an enforceable "court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer" (45 CFR § 164.512(f)(1)(ii)(A);
    - To the extent required by an enforceable grand jury subpoena (45 CFR § 164.512(f)(1)(ii)(B))
    - To the extent required by an enforceable "administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law" but only if three things are true:
        - "(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

[4] In Tennessee, for example, certain mental health professionals are required to "take reasonable care to predict, warn of, or take precautions to protect the identified victim" in situations when a patient/client " has communicated to a qualified mental health professional or behavior analyst an actual threat of bodily harm against a clearly identified victim" and the professional "has determined or reasonably should have determined that the service recipient has the apparent ability to commit such an act and is likely to carry out the threat unless prevented from doing so." TN Code § 33-3-206.

        - "(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
        - "(3) De-identified information could not reasonably be used." (45 CFR § 164.512(f)(1)(ii)(C))
    - Information about deceased individuals to the extent the death "may have resulted from criminal conduct" (45 CFR § 164.512 (f)(4))

- Disclosures otherwise in the course of any judicial or administrative proceeding:
    - To the extent required by "an order of a court or administrative tribunal"; and/or
    - "In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal," but only if the CE/BA "receives satisfactory assurance … from the party seeking the information" that "reasonable efforts have been made by such party" to either:
        - "ensure that the individual who is the subject of the [requested PHI] has been given notice of the request;" or
        - "secure a qualified protective order that meets the requirements of [45 CFR § 164.512(e)(1)(v)]."

Although CEs and BAs are generally prohibited from disclosing PHI without a patient authorization ***in response to <u>informal</u> law enforcement/private investigator requests***, HIPAA is unlikely to provide a basis to resist most law enforcement requests, subpoenas, and other **<u>formal</u>** processes seeking abortion-related data that comply with the standards described above.[5]

<u>Workforce Members May Create Risks by Proactively Disclosing Information</u>. Another risk organizations face is that CE/BA workforce members may make unsanctioned proactive disclosures to prevent perceived imminent harm to fetuses or alleged abortion-related wrongdoing. In recent guidance, HHS-OCR opined that:

> *"In the absence of a mandate enforceable in a court of law, the [HIPAA] Privacy Rule's permission to disclose PHI for law enforcement purposes does not permit a disclosure to law enforcement where a hospital or other health care provider's workforce member chose to report an individual's abortion or other reproductive health care. That is true whether the workforce member initiated the disclosure to law enforcement or others or the workforce member disclosed PHI at the request of law enforcement. This is because, generally, state laws do not require doctors or other health care providers to report an individual who self-managed the loss of a pregnancy to law enforcement."*

[5] The U.S. Department of Health and Human Services, Office for Civil Rights ("HHS-OCR") may engage in further rulemaking to modify its HIPAA Privacy Rule to tighten or eliminate such disclosures, but any such effort would require months or even years to complete and has not been announced to date.

Restrictive State law enforcement officials, private litigants, and judges are likely to take a different view of their state law "imminent harm" reporting obligations than HHS-OCR expressed. As noted above, states could also enact laws that expressly require reporting in such circumstances. ***In the absence of such explicit state reporting laws relating to abortion, the OCR guidance raises the specter that a CE/BA may find itself caught between a rock and a hard place: with Restrictive State courts/officials treating workforce member disclosures of abortion-related PHI to authorities as protected whistleblowing (or even mandated reporting of imminent harm to an "unborn child") while OCR investigates the same disclosures as potential HIPAA violations***. The potential sanctions under Restrictive State laws and HIPAA both could be substantial.[6] The most effective way for organizations to mitigate the risks from "freelance disclosure by workforce/partners" is through data minimization strategies and careful control of internal access to sensitive data.

State Privacy Laws Differ and are Likely to Shift. Most state laws are unlikely to affect reproductive health privacy post-*Dobbs* because most either already have exceptions that permit complying with subpoenas and court orders, or Restrictive States could easily enact such modifications. However, state laws that create independent confidentiality obligations to patients and/or privileges against disclosure that are controlled by those individuals may play a role.[7] There are also five "generally applicable" privacy laws taking effect in 2023 (in CA, CO, CT, UT, and VA) that may provide incremental protection by requiring companies to obtain "opt in" consent (in VA, CO, and CT) or giving consumers a right to "opt out" (in CA and UT) from the processing of "sensitive personal information," which includes health information (though such laws largely do not apply to HIPAA-regulated entities). It is likely that additional states will pass privacy legislation in the next year, which could provide further protections.[8] Notably, states seeking to further restrict abortion services may conform their privacy approach to one that paves a path for investigative requests for reproductive health information, while pro-abortion states may bar compliance with such requests or otherwise impose limitations on related access or disclosure. ***Federal legislation that would preempt state laws like the American Data Privacy and Protection Act (H.R. 8152), meanwhile, would subject a broad swath of health data to opt-in consent for collection or transfer of such data. Such an approach would eliminate some privacy compliance ambiguities while enhancing privacy protections for***

---

[6] Note that HIPAA-regulated and non-HIPAA-regulated organizations will need to consider employment law and, in many states, "freedom of conscience" law risks in considering how to respond to such workforce member disclosures that are not authorized by organizational leadership.

[7] On the other hand, many states have already enacted legislation, announced executive orders, or proposed legislation to shield residents of those states from inbound Restrictive State enforcement efforts (including, as of mid-July 2022, California, Colorado, Connecticut, Delaware, Maine, Massachusetts, Minnesota, Nevada, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, and Washington). Although most states have adopted the Uniform Interstate Depositions and Discovery Act to ease enforcement of subpoenas across state lines, these new state shield laws would do the opposite—generally prohibiting Protective State authorities from providing information or assistance to their counterparts in Restrictive States related to investigation/prosecution/litigation concerning reproductive health conduct that is legal in the Protective State. It remains to be seen whether such laws will have much practical effect, particularly where a subpoena recipient is subject directly to the jurisdiction of the Restrictive State's courts.

[8] Indeed, dozens of similar state privacy bills were proposed but failed in the last year alone, but *Dobbs* may push more states to enact similar state laws (or, conversely, deter states from enacting similar provisions). Federal privacy legislation has also been proposed (both to implement general privacy requirements as well as more specific laws targeting the privacy of location and health data), but has yet to be enacted.

patients against potential abuse that may emanate from enforcement or investigations under abortion restriction laws. For example, H.R 8152's opt-in requirement would effectively limit the creation and onward transfer of detailed profiles / digital footprints of patients' non-HIPAA covered data without their express, affirmative consent. Those profiles take on additional sensitivity given the uncertain—and in some states, shifting—legality of abortion services, especially if some states authorize private litigant "bounty hunting."

Risk 3: Companies subject to HIPAA will likely increase scrutiny of Business Associate Agreement provisions relating to law enforcement requests, subpoenas, and other similar disclosure pathways, costing more time and resources.

In a post-*Dobbs* world, CEs and BAs may undertake more extensive negotiation of Business Associate Agreements ("BAAs"). For example, CEs will likely want to exercise greater oversight and control over, and be able to assert defenses against, the disclosure of reproductive health information by their BAs in response to subpoenas and other such requests from authorities/litigants in Restrictive States. Organizations may also face increasing scrutiny and potentially even litigation/termination efforts from their contracting partners if disclosures made under existing BAAs play roles in Restrictive State enforcement efforts.

This becomes particularly acute in the context of **Health Information Exchanges ("HIEs"**) and **Electronic Health Records ("EHRs")** which are BAs to a large number of CEs and may store treasure troves of reproductive health information.

Risk 4: Health Information Exchanges ("HIE") are likely to receive requests for abortion-related data, which could indirectly lead to fewer HIEs operating in certain states and/or less HIE participation and, consequently, negatively impact unrelated care delivery due to decreased data quality and availability.

Some privacy advocates have rightly expressed concerns that HIEs, which are already closely tied to state health agencies in some instances, may become the target of law enforcement requests and enforcement litigation subpoenas in Restrictive States. Ultimately the PHI maintained by HIEs or EHRs remains that of the individual CE that provided the PHI to the HIE or EHR (unless the information is incorporated into the medical record of another HIE participant). As a result, some HIEs or EHRs may seek to defer law enforcement requests for reproductive health data to the applicable CE participants within the HIE or EHR. Other HIEs and EHRs may implement data minimization strategies to limit centralized access to sensitive reproductive health information – much like some HIEs and EHRs currently protect against access to substance use disorder information.

A more extreme possibility is that HIEs in Restrictive States may shut down entirely to avoid receiving and having to respond to such requests. A slightly less extreme result could also be that providers become less willing to participate in HIEs because they can't sufficiently control

response efforts to such requests made to the HIE, which would negatively impact quality and availability of data and results in worse care outcomes.[9]

Risk 5: Abortion-friendly states may enact legislation prohibiting (or at least making it difficult) EHR records from being transmitted across state lines (akin to privacy "data localization laws") to prevent EHRs and HIEs from disclosing abortion-related data, which could create stymie years of work designed to increase health data availability and interoperability.

EHRs and HIEs that operate across state lines may find themselves forced to disclose abortion-related data in Restrictive States. This could lead to a number of significant, unintended consequences for the broader EHR system, such as the possibility of future state laws requiring stricter EHR data localization and/or patient requests to ensure that their own data is localized or otherwise restricted to access by users within one or more pro-abortion states. Such laws could undermine decades of work and billion of dollars spent promoting EHR technologies to increase data availability and interoperability.

Risk 6: Organizations may leverage the ONC Information Blocking Rules to force abortion-related data sharing to ultimately make it available for state enforcement agencies.

HIEs, EHRs and health care providers are also subject to a federal prohibition against information blocking, which the Office of the National Coordinator for Health IT ("ONC") implemented under the 21st Century Cures Act. HIEs and EHRs will potentially be subject to $1 million civil monetary penalties for violations after the Office for Inspector General ("OIG") completes rulemaking, while health care providers will be subject to yet-to-be-determined "appropriate disincentives." Some stakeholders have expressed concern that an aggressive regulator could use this information blocking prohibition authority to penalize HIEs, EHRs and health care providers that fail to cooperate with state agencies and law enforcement officials in Restrictive States. Others have focused on the possibility that health care providers could, under the guise of information blocking compliance, be required to disclose patient reproductive health information to an EHR or HIE, from which that information could be more easily accessible by enforcement authorities or bounty-hunting private litigants.

Some of these concerns may be overblown, at least for now. As long as the Biden Administration is in power, it is highly unlikely that ONC would use its information blocking authority to aid Restrictive States in abortion-related investigations. Indeed, all post-*Dobbs*

[9] Another possibility that some have suggested is for providers simply to avoid submitting abortion-related data into EHRs and, in turn, cease the flow of such data to HIEs. In practice, however, this would be difficult to do because of how EHRs are built to be interoperable with and automatically pull data from EHRs. Moreover, data in EHRs is often not structured in a manner that makes it easy to carve out specific data points. To the contrary, some of the most important data is located in "notes" and other open text fields rather than structured data fields that could make it infeasible to segregate or exclude abortion-related data.

public statements by the administration have pointed in the exact opposite direction. However, that obviously could change if a new administration takes over in January 2025.

Additionally, the Privacy Exception of the information blocking regulation permits regulated actors, such as HIEs and health care providers, to honor requests made by patients to not disclose their PHI. As most HIEs are required under state law or by common agreement with other HIEs to offer patients the opportunity to opt-in or opt-out of HIE participation, health care providers could point to the Privacy Exception when they withhold patient information from HIEs pursuant to a patient's wishes.

The information blocking regulation also does not preclude HIEs or health care providers from arguing that other laws – such as provider-patient privilege provisions of various state laws – prohibit disclosure to the government agency. The definition of "information blocking" explicitly considers that covered actors may in some cases be precluded by law from responding to a request for electronic health information. HIEs could point to this language to argue that any law enforcement requests should be directed to applicable CEs – as HIEs and EHRs are arguably precluded by law from disclosing another entity's PHI. Even with these defenses, however, it is not hard to imagine the *Dobbs* decision having a chilling effect on HIE participation as noted above – particularly in Restrictive States.

Risk 7: Companies are likely to face conflicting pressure related to the FTC and state "unfair and deceptive acts or practices" laws, with the FTC and states seeking to protect abortion services scrutinizing abortion-related data disclosures in Restrictive States.

The Federal Trade Commission (FTC, under Section 5 of the FTC Act) and/or state attorneys general have authority to regulate and enforce "unfair or deceptive acts and practices" (against both HIPAA-regulated and non-regulated entities). Such regulators are likely to closely scrutinize companies that handle sensitive abortion-related data, including evaluating whether privacy notices are sufficiently transparent, whether company practices comply with public-facing statements, how companies secure such data, and whether more affirmative notice and choice is necessary. Indeed, the FTC's Acting Associate Director of Privacy & Identity Protection indicated in a July 11 blog post that the FTC will "vigorously enforce the law if [the FTC] uncover[s] illegal conduct that exploits Americans' location, health or other sensitive data", and specifically called out data related to sexual activity or reproductive health as sensitive information that "may subject people to discrimination, stigma, mental anguish, or other serious harms."

Based on the examples in the blog post, the FTC may focus enforcement actions on application developers that unnecessarily (and contrary to publicly posted privacy policies) collect and store information that would allow third parties to infer or prove that individual sought or received abortion care. Consequences from an FTC enforcement action can be severe; although most cases settle, typical consent decrees often last for ***twenty years*** and impose myriad burdensome reporting requirements. Application developers and other companies will need to

(1) ensure their privacy notices are transparent about how data is collected, used, and disclosed; and (2) ensure they comply with the representations in those privacy policies.[10]

Risk 8: Organizations may face private class action and individual litigation by consumers, providers, and other data subjects (both by individuals negatively impacted when organizations disclose abortion-related data and by individuals in Restrictive States that permit private causes of action against entities that provide "abortion assistance").

Organizations should also consider the risk of individual/class action litigation by patients, providers, and other data subjects. To the extent data held by an organization gives rise to criminal prosecution or civil litigation against an individual or another organization, the latter may seek to recover damages from the source organization on a theory that the data should not have been collected, maintained, and/or produced/disclosed in the manner that it was. The potential for negative media coverage and other reputational harm amplifies such risks.

[10] Restrictive State courts and law enforcement authorities are unlikely to view voluntarily undertaken contractual/consumer protection commitments within a privacy policy as bases on which subpoenas or equivalent processes can be resisted. This means that application developers will need to evaluate the risks associated with collecting reproductive health data concerning users that live in Restrictive States, consider strategies for minimizing the collection and storage of data that could be used to prove a user sought or had an abortion and develop potential defenses against producing sensitive information that the developer must collect and store to provide its services.

APPENDIX A: Overview of post-*Dobbs* Legal Landscape

For nearly fifty years, Supreme Court jurisprudence under *Roe v. Wade*, *Planned Parenthood v. Casey*, and other decisions had recognized a federal constitutional right for a person to obtain an abortion—at least early in a pregnancy. In simple terms, the existence of that federal constitutional right prevented federal, state, and local governments from enforcing any laws (pre-existing or new) whose purpose or effect was to place "substantial obstacles" in the path of a person seeking an abortion before the fetus was sufficiently developed to be viable outside of the womb. *Dobbs* overruled those prior decisions, leaving federal, state, and local governments free to regulate abortion—or even prohibit it—as they see fit, subject only to: (1) any other federal constitutional rights, such as with respect to speech, interstate travel, etc.; (2) any applicable state constitutional rights; and (3) any direct conflicts with federal statutes that may preempt contrary state law in such circumstances. What federal and (more immediately) state and local governments choose to do with that newfound freedom to act creates several risk vectors for organizations.

Primarily, government (and sometimes private) actors are now allowed to enforce anti-abortion laws that they were restrained by federal law from enforcing until *Dobbs*. While the specifics vary state to state and are changing in real-time as state legislatures continue to act, that generally includes the following:

- State and local law enforcement authorities can **criminally investigate and prosecute** individuals alleged to have performed, induced, attempted, aided, abetted, solicited, or conspired to accomplish an unlawful abortion. They can criminally investigate and prosecute organizations whose personnel (employees or other agents) allegedly did any of those things, with the approval of organizational leaders. Successful criminal prosecution generally leads to incarceration (for convicted individuals) and/or imposition of monetary fines/forfeiture (for convicted individuals or organizations). Criminal conviction can also collaterally impact ongoing qualification to do business—especially with respect to federal or state government contracts and/or reimbursement from government programs—and/or individual professional licensure.
- State and local law enforcement authorities in some states are also empowered to conduct **civil investigations and enforcement lawsuits—seeking court judgments for civil monetary penalties** (e.g., at least $100,000 per abortion, plus reimbursement of litigation costs and attorneys' fees) from individuals or organizations alleged to have performed, induced, or attempted (sometimes also aided/abetted, etc.) an unlawful abortion.
- In at least two states—Texas and Oklahoma—private individuals are empowered by law to commence **civil bounty-hunting lawsuits** against individuals or organizations that allegedly performed, induced, attempted, or aided/abetted (including providing funding for) seeking court judgments for civil damages of at least $10,000 per unlawful abortion, plus reimbursement of litigation costs and attorneys' fees.
- The patient who underwent an allegedly unlawful abortion, plus the father of the fetus and potentially other family members, have increased ability to **sue civilly, for compensatory damages**, those who performed, induced, or otherwise participated in an allegedly unlawful abortion.
- State licensing boards (e.g., boards of medicine or nursing, etc.) are increasingly empowered and sometimes required by state law to **suspend, revoke, or take other disciplinary action against licensees** for participation in an allegedly unlawful abortion.

Importantly, the boundaries of what constitutes an unlawful abortion for these purposes are not clear or consistent. Many Restrictive State laws define "abortion" broadly—to include any medical, surgical, or other means intended to terminate a pregnancy, starting either from the point of conception (sperm fertilization of egg), from the point of identifiable cardiac activity (around six weeks of gestation), or from another specified gestational milestone. They generally exempt procedures that are necessary to save the pregnant patient's life (including to end ectopic pregnancies), and some also extend such exemptions to other medical emergencies (such as where necessary to prevent a significant physical health impairment)—but often with specific documentation requirements. Many current state laws do **not** exempt cases of rape or incest. Some states' laws are written in ways that expressly exempt contraception measures and/or *in vitro* fertilization activities (or other reproductive health activities that may result in the termination of an embryo) from their abortion prohibitions, but many states' laws are not clear on those issues.

There are many nuances of the specific nature of challenged conduct, the specific language of potentially applicable laws, the limits of state territorial jurisdiction over conduct that crosses state lines, potential federal preemption, etc. that will dictate the boundaries of risk in each case. The initial investigative and enforcement decisions will be made by dozens of state attorneys general and licensing boards, hundreds of county/local prosecutors and police agencies, and thousands of private actors. Courts—especially state courts in Restrictive States—will define the boundaries of unlawful conduct over time, and legislation will continue to try to change those boundaries further**. As a general rule, the stronger an individual's or organization's ties to a Restrictive State, and the more closely involved the individual's or organization's conduct is to an allegedly unlawful abortion procedure, the greater the risk of prosecution and/or civil enforcement will be. Political factors (e.g., targeting high profile individuals/organizations for enforcement) are also likely to come into play.**