ConnectedHealthInitiative

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

Intro and Executive Summary

The U.S. Supreme Court's June 2022 opinion in *Dobbs v. Jackson Women's Health* creates risks for health organizations, including organizations, and other entities that handle both Protected Health Information (PHI) and personal information relating to reproductive health services, including abortion care.[1] In addition to the more direct impact on reproductive health providers (*i.e.*, government and private actions to enforce restrictions on reproductive health care and abortion care services), *Dobbs* and related state and federal requirements introduce numerous data privacy, security, exchange and use, and availability complexities, among other data-related risks for organizations that deliver, pay for, or provide technology services relating to health care, such as:

1. *Dobbs* and precursor as well as subsequent changes in state law and regulation, in addition to federal regulation and guidance, significantly expand the types of organizations that are likely to receive law enforcement requests or subpoenas related to PHI, reproductive health care data, and other personal information, and significantly increases the likelihood of receiving requests and subpoenas.
2. Existing state and federal laws and regulations (*e.g.,* the Health Insurance Portability and Accountability Act (HIPAA), HIPAA Privacy Rule, California Civil Code §1798.80)[2] in many cases will not provide sufficient privacy protections to stop states from leveraging existing investigative tools, using subpoenas, and/or enacting new laws or rules to obtain reproductive health data.
3. Organizations subject to HIPAA, called covered entities (CEs), will likely increase scrutiny of Business Associate Agreement (BAA) provisions relating to law enforcements, subpoenas, and other similar disclosure pathways, costing more time and resources.
4. Health Information Exchanges ("HIE") and state -operated All-Payer Claims Databases (APCDs) are likely to receive requests for reproductive health data, which could indirectly lead to fewer HIEs operating in certain states, restrictions on the data available from HIEs and APCDs, and/or less HIE and APCD participation and, consequently, negatively impact unrelated care delivery, care coordination, data interoperability, and research or innovation due to decreased data quality and availability.
5. Abortion-friendly states ("Protective States") may enact legislation prohibiting (or at least making it difficult) for Electronic Health Records (EHRs) to be transmitted across state lines (akin to privacy "data localization laws") to prevent EHR systems or providers, APCDs, and

---

[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.

[2] For a comprehensive review of state health care information privacy, see https://www.seyfarth.com/a/web/77459/50-State-Survey-of-Health-Care-Information-Privacy-Laws.pdf. For additional information on HIPAA, see https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html.

HIEs from disclosing abortion-related data when those entities also operate in states that now prohibit or significantly curtail abortion ("Restrictive States").

6. Although the Biden administration is unlikely to leverage the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule*[3] to force abortion-related data sharing, future administrations may and/or states could pass equivalent state laws or finalize new rules to penalize health organizations that resist disclosing data.
7. Organizations are likely to face conflicting pressure related to the U.S. Federal Trade Commission (FTC) and state "unfair and deceptive acts and practices laws," with the FTC and Protective States scrutinizing disclosures organizations may make if required in Restrictive States.
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 organizations that may be targeted) is likely to expand significantly.[4] Many organizations 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.

[3] 85 FR 25642 (May 1, 2020)

[4] 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.

- Official and private litigants can, either directly or with court approval (depending on state-specific rules), issue subpoenas for the same,[5] 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.

Risk 2: Existing law (HIPAA and other state/federal laws and rules) in many cases will not provide sufficient privacy protections to stop states from leveraging existing investigative tools (and/or enacting new laws) to obtain abortion data.

States already have numerous tools (beyond law enforcement powers) to obtain health (including abortion-related) data from HIPAA- covered entities and Business Associates (BAs) and non-HIPAA- regulated entities alike, and *Dobbs* may embolden states to enact even more specific laws mandating proactive abortion data disclosures. For example, some organizations that have health information are not required to follow HIPAA or federal Privacy and Security Rules, including life insurers, workers compensation carriers, many state agencies like child protective services agencies, many municipal offices, and employers (specific to employment records). 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;
- APCDs to which many states require insurers and health care payors to submit health care 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

[5] 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.

knows or suspects a pregnant patient intends to imminently terminate the pregnancy, whether by traveling to another state or otherwise.[6]

HIPAA Permits Disclosures in Numerous Circumstances. Neither HIPAA, current federal Privacy Rules, nor other 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) CEs and their 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;
    - "(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)]."

[6] 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.

Although CEs and BAs are generally prohibited from disclosing PHI without a patient authorization ***in response to informal law enforcement/private investigator requests***, HIPAA is unlikely to provide a basis to resist most law enforcement requests, subpoenas, and other **formal** processes seeking abortion-related data that comply with the standards described above.[7]

Workforce Members May Create Risks by Proactively Disclosing Information. 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, the HHS Office for Civil Rights (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."*

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.[8] 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 Laws Likely Do Not Provide Sufficient Privacy Protections Either. State laws are unlikely to provide sufficient protection because most either already have exceptions that permit complying with subpoenas and court orders, or Restrictive States could easily enact such modifications. The most likely avenue to resist production, however, are state laws that create independent confidentiality obligations to patients and/or privileges against disclosure that are

---

[7] The 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.

[8] 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.

controlled by those individuals.[9] 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 organizations 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.[10]

Risk 3: Organizations 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 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 **HIEs, APCDs,** and **EHRs,** which are BAs to a large number of CEs and may store treasure troves of reproductive health information.

Risk 4: HIEs and APCDs 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

---

[9] 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.

[10] 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.

maintained by HIEs, APCDs, 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.[11]

Risk 5: Protective States may enact legislation prohibiting (or at least making it difficult) for EHR records to be 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 Protective States. Such laws could undermine decades of work and billion of dollars spent promoting EHR technologies to increase data availability and interoperability.

Risk 6: Although the Biden administration is unlikely to leverage the ONC* Information Blocking Rules *to force abortion data sharing, future administrations may and/or states could pass equivalent state laws to penalize health organizations that resist data production.

HIEs, EHRs, and health care providers are also subject to a federal prohibition against information blocking, which the 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 HHS 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

[11] 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.

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* 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: Organizations are likely to face conflicting pressure related to the FTC and state "unfair and deceptive acts and practices" laws, with the FTC and Protective States scrutinizing abortion-related data disclosures in Restrictive States.

The Federal Trade Commission (under Section 5 of the FTC Act) and/or state attorneys general have authority to regulate and enforce "unfair and deceptive acts and practices" (against both HIPAA-regulated and non-regulated entities). Such regulators are likely to closely scrutinize organizations that handle sensitive abortion-related data, including evaluating whether privacy notices are sufficiently transparent, whether company practices comply with public-facing statements, how organizations 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 organizations 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.[12]

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.

[12] 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.**