Reproductive Health Information Privacy in a Post-Roe World

Kristen Rosati and Melissa Soliz, Coppersmith Brockelman PLC
July 26, 2022

On June 24, 2022, the Supreme Court issued its decision in *Dobbs v. Jackson Women's Health Organization*, overruling *Roe v. Wade* and *Planned Parenthood v. Casey* and concluding that women no longer have a constitutional right to obtain an abortion. There are volumes we could say about this decision, but we have limited this Coppersmith Brief to the data privacy issues presented by the onslaught of new state laws to prohibit abortion, including statutes that criminalize providing abortion care.

Specifically, this Brief discusses when the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. Parts 160 and 164) permits disclosure of protected health information (PHI) to state attorneys general, law enforcement, medical boards and other regulatory authorities that may be involved in enforcing these new state laws. We do not discuss the application of other federal privacy laws, including the federal regulations governing substance use disorder treatment information at 42 C.F.R. Part 2, Title X or the Federal Privacy Act, and do not discuss state health information confidentiality laws that may provide greater protection than HIPAA.

This Brief also discusses how the Information Blocking Rule may affect the production of electronic PHI by health care providers to state authorities.

Finally, we make a number of practical suggestions on how to protect the privacy of patients who have had an abortion or who present with complications relating to abortion or miscarriage.

HIPAA and the Release of PHI to Governmental Authorities

As an initial matter, the HIPAA Privacy Rule does not *require* release of PHI to governmental authorities. Instead, the Privacy Rule has many provisions that *permit* disclosure of PHI in certain defined circumstances. The Department of Health and Human Services Office for Civil Rights (OCR) made that point forcefully in its guidance document released on June 29, 2022: HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care.

The Privacy Rule *permits* HIPAA covered entities to disclose PHI (including reproductive health information) to governmental authorities in the following circumstances:

- **With patient authorization:** HIPAA covered entities may disclose PHI with a valid, written authorization signed by the patient (or the patient's health care decision maker if the patient is not competent). 45 C.F.R. § 164.508. We anticipate that most governmental authorities' request for reproductive health information will not be done with patient authorization.

- **As required by law:** Covered entities may disclose PHI if required to do so by federal or state law. 45 C.F.R. § 164.512(a). We recommend caution in ensuring that a disclosure is actually required. The definition of "required by law" at 45 C.F.R. §164.103 is:

  > Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

  Before responding to a request, a covered entity should confirm the reporting requirements are applicable to the entity (which might be an issue as states try to extend long-arm jurisdiction to facilities in other states that care for patients who reside in other states), and that the mandate is *enforceable*. Also, any production of PHI must be limited to what is required by the law.

- **In response to a court order:** A covered entity may release patient information when ordered to do so by a court. 45 C.F.R. § 164.512(a), (e), and (f)(1). The entity should confirm that the court has jurisdiction over the provider (so it is enforceable) and the entity should provide only the patient information specifically set forth in the court order.

- **In response to a search warrant:** A covered entity may release patient information if a law enforcement officer presents a court-ordered search warrant for that information. 45 C.F.R. § 164.512(f)(1)(ii)(A). The entity should confirm that the issuing court has jurisdiction over the entity and should provide only the patient information specifically listed in the search warrant.

- **In response to an "administrative request" by law enforcement:** HIPAA permits release of PHI pursuant to an "administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that: (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." Given the sensitivity of reproductive health information—particularly if sought in a criminal investigation—we do not recommend relying on this exception. If the presenting governmental authority can demonstrate that the request is enforceable under state law, it would be a "required by law" disclosure.

- **In response to a grand jury subpoena:** A covered entity may release patient information when presented with a subpoena issued by a grand jury. 45 C.F.R. § 164.512(f)(1)(ii)(B). Grand jury subpoenas are not subject to the requirements for "regular" subpoenas discussed in the next paragraph. Again, as with any release of information, an entity must be careful to provide only the patient information specifically authorized by the grand jury subpoena.

  In response to a subpoena <u>not</u> issued by a grand jury: If a covered entity receives a subpoena for patient information, the entity may produce that information under HIPAA only if the entity receives documentation from the party seeking the information – or itself obtains documentation—that: (1) reasonable efforts were made to ensure that the patient has been given notice of the request, the notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the patient to object, and the patient has not objected to production during the time permitted (or those objections were resolved in favor of producing the PHI); or (2) reasonable efforts were made to secure a "qualified protective order." A qualified protective order is an order of the court (or stipulation of the parties) that: (1) limits the use of the PHI to the litigation; and (2) requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding. 45 C.F.R. § 164.512(e). Many states have more stringent laws related to production of patient information pursuant to a subpoena.

- **Related to a crime on premises:** Covered entities may disclose PHI where the entity "believes in good faith [the PHI] constitutes evidence of criminal conduct that occurred on the premises of the covered entity." 45 C.F.R. § 164.512(f)(5). We anticipate that this exception will be met only if an abortion was performed at the entity in violation of state law. Where a patient presents with complications from a medication abortion or a surgical abortion initiated or performed elsewhere, we do not anticipate that OCR, under its current guidance, would treat this as a "crime on premises."

- **Related to decedents:** A covered entity may disclose PHI about a patient who has died, for the purpose of alerting law enforcement of the death of the patient, if the covered entity has a suspicion that such death may have resulted from criminal conduct. 45 C.F.R. § 164.512(f)(4).

- **To the coroner or medical examiner:** A covered entity may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. 45 C.F.R. § 164.512(g).

- **To avert a serious and imminent threat to health or safety**: A covered entity may release PHI if the covered entity—"consistent with applicable law and standards of ethical conduct"—in good faith believes disclosure is "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public" and the disclosure is "to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat." 45 C.F.R. § 164.512(j)(1)(i).

  This rule also permits release of PHI where it is "necessary for law enforcement authorities to identify or apprehend an individual" where the patient has admitted "participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim." 45 C.F.R. § 164.512(j)(1)(ii). The type of PHI that may be released is limited to the patient's statement concerning participation in the crime and the patient's name, address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death (if applicable), and a description of distinguishing physical characteristics (such as height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos).

  We recommend consultation with counsel before using this exception.

- **For health oversight activities**: A covered entity may disclose patient information to a "health oversight agency." A health oversight agency is a government agency (federal, state, county, local, or tribal) that is authorized by law to oversee the health care system (whether public or private), or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. 45 C.F.R. § 164.501. Typical health oversight agencies include state departments of health services and medical boards. If a law enforcement officer justifies a request for records under the "health oversight agency" rule, rather than one of the law enforcement disclosure rules, we recommend asking for an explanation in writing and seeking advice of counsel.

  Health oversight agencies may obtain patient information for oversight activities authorized by law. 45 C.F.R. § 164.512(d). This includes audits, civil, criminal or administrative investigations, inspections, licensure or disciplinary actions, and civil, criminal and administrative proceedings. It also includes other activities necessary for the oversight of the health care system, of government benefits programs (as necessary), or to determine compliance with government regulatory programs or civil rights laws.

One exception, however, is that a provider may not disclose PHI under this exception for a government investigation of a patient, unless it relates directly to the patient's receipt of health care, claim for public health benefits, or qualification for or receipt of public health benefits when the patient's health is integral to the claim for services. We thus exercise caution in responding to health oversight agency request for PHI related to reproductive health.

- **For other purposes**: There are other HIPAA rules related to disclosures of PHI to law enforcement, such as disclosures of limited information to identify or locate a suspect, fugitive, material witness or missing person, and disclosure of crime victim PHI (see 45 C.F.R. § 164.512(f)(2)-(3)), release of PHI to correctional personnel (see 45 C.F.R. § 164.512(k)(5)), release of PHI related to crimes committed against personnel (see 45 C.F.R. § 164.502(j(2)), and for emergency service providers (see 45 C.F.R. § 164.512(f)(6)). We do not anticipate those rules applying where reproductive health information is sought.

The Information Blocking Rule

The Information Blocking Rule or IBR (42 U.S.C. § 300jj-52 and 45 C.F.R. Part 171) prohibits certain actors, including health care providers, from engaging in practices that are likely to interfere with the access, exchange or use of electronic health information (EHI), unless the practice is specifically required by law or falls into a regulatory exception. There are currently eight regulatory exceptions, including the IBR Privacy Exception, which protects actors if they engage in practices that are reasonable and necessary to comply with privacy laws, like HIPAA. The IBR is an intent-based law. To violate it, a provider must have actual knowledge that a practice is likely to interfere with the access, exchange or use of EHI and that the practice was unreasonable. Enforcement of the IBR is delayed pending finalization of the IBR enforcement rules.

The IBR requires providers (and other actors) to assess whether it is lawful to not share EHI in response to an otherwise authorized EHI request. While HIPAA is permissive and does not require covered entities to disclose PHI, the IBR may require a provider to release EHI about reproductive health care in response to a lawful request. For example, if a health care provider receives a subpoena for reproductive health records, and that subpoena meets the requirements of HIPAA and other applicable law, not producing those records could give rise to an IBR complaint.

However, it is not information blocking if a provider demonstrates that the provider's practice meets an IBR exception. For example, one of the IBR Privacy Exceptions (45 C.F.R. § 171.202(e)) permits a provider to deny an EHI request if the patient requests the provider not to provide the EHI to the requestor. To qualify for this protection, the provider must document the patient's request within a reasonable time after it is made. The provider cannot improperly encourage or induce the person to request such a restriction and must implement this practice in a consistent and non-discriminatory manner. Accordingly, a provider could give all patients the

choice to "opt out" of the release of their reproductive health records (or abortion records specifically) to law enforcement, and would not violate the IBR if all the requirements of this privacy exception are met.

Similarly, some providers may choose to document a more restrictive approach in their HIPAA Notice of Privacy Practices (NPP) and choose not to disclose certain PHI unless required by law or necessary to avert a serious or imminent threat to health or safety. Under HIPAA, a provider must abide by the terms of its NPP, including any voluntary limitations on the provider's disclosure of PHI to third parties. Under a different IBR Privacy Exception (45 C.F.R. § 171.202(b)), a provider may deny an EHI request if a legal precondition has not been satisfied—such as if a limitation in the NPP has not been satisfied. To qualify for this protection, the provider must implement this practice in a consistent and non-discriminatory way, and document the practice in its organizational policies and procedures or on a case-by-case basis. Accordingly, a provider could choose to use a NPP that limits the circumstances in which the provider will release reproductive health records—except when such a disclosure is required by law or necessary to avert a serious or imminent threat to health or safety—and not violate the IBR, if all the requirements of the Privacy Exception are met.

Additionally, some providers may operate in multiple jurisdictions, some of which may provide more stringent privacy protections for reproductive health records. There is a special safe harbor protection in the IBR Privacy Exception (45 C.F.R. § 171.202(b)(3)) that permits such a provider to adopt uniform policies and procedures that apply the more stringent privacy restriction to the provider's entire operation across all jurisdictions.

There are other IBR exceptions that may apply given the facts and circumstances of a particular case. For example, a provider who has (or had) a clinician-relationship with the patient may determine that releasing EHI in response to an otherwise lawful request to state authorities may be reasonably likely to endanger the life or physical safety of the patient or another person under the IBR Preventing Harm Exception (45 C.F.R. § 171.201).

Finally, even if an IBR exception is not available, a provider's decision to not release reproductive health records under certain circumstances might not constitute an IBR violation. The facts and circumstances of a particular case may permit a provider to engage in a practice that interferes with the release of EHI, if the provider did not have actual knowledge that the practice was unreasonable.

Practical Suggestions to Protect Patients

We have a number of practical suggestions for providers to consider:

- Investigate whether women presenting for reproductive care (miscarriages, abortions, *etc.*) can be marked as VIP patients or otherwise have their EHRs accessible only to personnel who "break the glass" for that particular record. Some EHRs have this capability, which is used in handling substance use

disorder treatment information; other EHRs don't have the capacity to segregate records. For compliance with the IBR, providers should further consider whether engaging in such a practice will qualify under one or more IBR exceptions. For example, a provider may choose to offer this as an option to such patients and then document the patient's request for this heightened privacy protection.

- Rigorously audit access to records for women presenting for reproductive care—and let your employees know you are doing so. In the event there is a breach related to an employee who accesses a record to pursue a lawsuit or bounty in states where that is permitted, it would be very helpful in an OCR investigation to show that the organization is aggressively auditing and did employee training around the issue.

- Assess how your organization participates in data sharing networks, such as CommonWell and Carequality. If a particular data sharing network does not have a mechanism for protecting particular types of sensitive data, consider whether your organization can suppress data sharing of reproductive health records through these networks, such as by using sensitive code software (such as how many organizations suppress substance use disorder treatment information or psychotherapy notes). If data suppression is not feasible, providers should consider educating women who present for complications related to abortion or miscarriage on network opt-out options. Again, providers should also carefully consider whether, and how, to structure such practices to qualify for an IBR exception.

This will be a challenging time for patients who seek reproductive care and the providers who care for them. We stand ready to assist!

Kristen Rosati is one of the nation's leading "Big Data" and HIPAA compliance attorneys. She also has deep experience in data sharing for research, development of artificial intelligence, and clinical integration, health information exchange, clinical research compliance, biobanking and genomic privacy, data breaches and OCR investigations. Kristen is a Past President and Fellow of the American Health Law Association.

Melissa (Mel) Soliz is highly sought out for her deep expertise on interoperability issues ranging from the ONC Information Blocking Rule and TEFCA (the Trusted Exchange Framework and Common Agreement) to CMS interoperability mandates. Her practice also focuses on HIPAA and 42 C.F.R. Part 2 compliance, health information exchange and networks, health IT contracting (particularly for social determinants of health and health equity platforms), data breaches and OCR investigations, as well as clinical research compliance and contracting. Mel is President of the Arizona Society of Healthcare Lawyers (AzSHA).