ROPES & GRAY

ALERT ▪ Health Care

July 21, 2022

Privacy of Health Information Post-*Dobbs* and OCR Guidance on the Protections Afforded under HIPAA

Attorneys
Deborah L. Gersh
Cara Dermody
Chandler Gray

Introduction

On June 24, 2022, the Supreme Court issued its opinion in *Dobbs v. Jackson Women's Health Organization*, overturning precedent that protected access to abortion services before the point of fetal viability. Instead, the Supreme Court stated that state legislatures have the authority to regulate abortion, leading several states to enact laws banning the procedure or to enforce previously unenforceable laws banning abortion.[1] In response to the *Dobbs* decision, on June 29, 2022, the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") released guidance materials discussing the role that the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations, as amended (collectively, "HIPAA") plays in safeguarding the protected health information ("PHI") of women.[2]

Additionally, on July 8, 2022, President Biden signed Executive Order 14076 to affirm reproductive health care access in light of the Supreme Court's decision in *Dobbs*.[3] The Executive Order calls on leaders of federal agencies to promote access to reproductive health care, to protect the privacy and safety of those seeking abortion and other reproductive health care, and to coordinate efforts to achieve these goals. In response to this Executive Order, HHS Secretary Xavier Becerra issued guidance on July 11, 2022, explaining the role of the federal Emergency Medical Treatment and Active Labor Act ("EMTALA") in ensuring reproductive health care access.[4]

As the number of restrictive abortion laws rises, and potential criminal liability for those involved in seeking or providing an abortion grows, the protection of patients' health information has taken on an increasingly vital role in the delivery of health care. Women and other patients may feel that their health information, including PHI, is no longer secure and hesitate to engage with the broader health care system, including providers, health plans, pharmacies, and digital health applications. In addition, patients and providers have become more concerned about the use of cookies and similar tracking technologies by health care companies, including health care providers that are considered to be "covered entities" under HIPAA. These technologies may track, for example, certain website searches, location information, and other online behavior, which many fear state officials could attempt to use in prosecuting abortion. For example, a state official in a state that bans abortion may issue a subpoena to a company using such tracking technologies seeking certain personal information relating to a consumer's online activity, including questions about birth control, pregnancy, pharmaceuticals or abortion services.[5] As a result, OCR has increased enforcement activity and reiterated the obligation of covered entities to appropriately safeguard PHI. In line with the need to protect the privacy of all individuals, OCR also has indicated that it is exploring the release of standard "recognized security practices" under the Health Information Technology for Economic and Clinical Health ("HITECH") Act.[6] A new and more discerning light is now being shined on the critical importance of protecting personal health information. As a result, covered entities, business associates and others who provide support services to the health care industry, will be held to stricter scrutiny. In response, covered entities and their business associates must be aware of, and be prepared to meet, more rigorous privacy and security requirements imposed by HIPAA, including when disclosures of PHI are not permitted, training staff on the new requirements, enhancing security, and ensuring that policies and procedures are current and personnel is appropriately trained, and remaining informed about any new guidance documents released by OCR or the applicable state authority. This client alert summarizes OCR's recent guidance in this area and highlights key areas of potential concern for clients.

Protection of Patient Information under the HIPAA Privacy Rule

June 2022 OCR HIPAA Privacy Rule Guidance

In the guidance material titled *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, released on June 29, 2022 (the "HIPAA Privacy Rule Guidance"), OCR clarified the HIPAA Privacy Rule's (the "Privacy Rule") impact on post-*Dobbs* legislation and practices.[7] The Privacy Rule establishes requirements for the use, disclosure and safeguarding of PHI by covered entities and their business associates.[8] The HIPAA Privacy Rule Guidance reiterates that "regulated entities can use or disclose PHI, without an individual's signed authorization, *only* as expressly permitted or required by the Privacy Rule."[9] The HIPAA Privacy Rule Guidance confirms that "permissions for disclosing PHI without an individual's authorization for purposes not related to health care . . . are narrowly tailored to protect the individual's privacy and support their access to health services."[10]

When disclosure of an individual's PHI is required by another law, covered entities are *permitted, but not required*, to comply with the disclosure.[11] Additionally, "[d]isclosures of PHI that do not meet the 'required by law' definition in the HIPAA Rules, or that exceed what is required by such law, do not qualify as permissible disclosures."[12] The HIPAA Privacy Rule Guidance provides the example of an individual who goes to the hospital while experiencing a miscarriage. OCR stated that even if the hospital worker suspects that the individual took medication to end her pregnancy in violation of state law, if the state law does not "expressly require such reporting," the hospital worker *may not report* the individual to law enforcement.[13]

The HIPAA Privacy Rule Guidance also discusses when covered entities are required to disclose an individual's PHI for law enforcement purposes, and again draws a distinction between when a covered entity must disclose PHI versus when a covered entity may disclose PHI.[14] Under the Privacy Rule, a covered entity may disclose PHI when faced with a court order, court-ordered warrant or subpoena as long as the covered entity meets the specific conditions required by the Privacy Rule.[15] For example, a reproductive health care clinic may not provide records of abortions performed at the clinic to a law enforcement officer absent a court order or other mandate enforceable in a court of law (e.g., court-ordered warrant or subpoena)."[16] Importantly, however, even when faced with a court order or other mandate, the reproductive health care clinic is *never* required by HIPAA to disclose the PHI.[17] Further, the HIPAA Privacy Rule Guidance clarifies that the Privacy Rule does not permit a health care provider to report an abortion to law enforcement without an enforceable mandate.[18]

Finally, the HIPAA Privacy Rule Guidance states that the "Privacy Rule permits but does not require a covered entity . . . to disclose PHI if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen" a serious threat to health or safety of a person or the public.[19] Importantly, however, the HIPAA Privacy Rule Guidance, along with major professional societies, maintains that this category of disclosure does not apply in the reproductive health care context, and thus any such disclosure is not permitted by the Privacy Rule.

Implications of HIPAA Privacy Rule Guidance

To ensure compliance with HIPAA and the HIPAA Privacy Rule Guidance, covered entities should update their HIPAA training materials or otherwise engage their provider workforce on the HIPAA Privacy Rule Guidance, emphasizing when the disclosure of PHI is mandated versus permitted. This is especially important in states where health care providers may face requests for information from law enforcement *and* anyone seeking to enforce an abortion ban under a private right of action. As stated above, several states now ban abortion, and some states criminalize those who assist with or perform an abortion.[20] For example, Texas' law grants a private right of action to any person to bring a civil suit against another who performs or induces an abortion or who aids or abets the performance of an abortion.[21] Under this statute, a hospital employee who suspects a physician of performing an abortion or a spouse of bringing a partner to the hospital for an abortion could sue those individuals. However, as the HIPAA Privacy Rule Guidance explains, this action

would violate HIPAA. Additionally, these statutes may have a chilling effect on patients' use of assisted reproductive technology ("ART"), such as in vitro fertilization. Common aspects of ART procedures, such as freezing embryos before use and selective reduction of nonviable embryos, could now be considered a criminal act under new state abortion laws.[22] Although HIPAA protects PHI related to these procedures, patients may worry that an untrained member of the provider's staff might seek to enforce the abortion ban through the private right of action. Covered entities may benefit from establishing clear guidance for their workforce on protecting PHI related to reproductive health, and if not already in place, developing a process or designating an individual or committee to review and approve any disclosure related to reproductive health.

In addition, law enforcement officials could attempt to access information from third-party companies with which covered entities or their business associates share information.[23] While subpoenas to covered entities or business associates must be appropriately tailored to be enforceable under HIPAA, law enforcement may seek to subpoena companies with which a covered entity or business associates has already shared certain information concerning the online activity of its patients (e.g., a patient's search on a provider website for reproductive health services). Thus, covered entities and business associates should reexamine their data collection and destruction policies; communicate across business departments to ensure transparency within companies concerning what information may be stored, tracked, and shared with third parties; and update its data sharing and use practices accordingly.[24]

Relatedly, health care providers must also be mindful of the interaction between EMTALA and state abortion laws. For example, while Texas law generally states that performing or inducing an abortion is unlawful, EMTALA requires a physician to take these actions if needed to stabilize a pregnant woman who came to a hospital emergency department and presented with an emergency medical condition ("EMC").[25] OCR issued guidance on July 11, 2022 that reiterated hospitals' existing obligations under EMTALA (the "EMTALA Guidance").[26] Under EMTALA, hospitals and physicians are required to screen individuals who come to an emergency department to determine if an EMC is present, to stabilize those individuals who have an EMC, and generally not to transfer those with EMCs unless the medical benefits of the transfer outweigh the risks.[27] Thus, EMTALA mandates that hospitals and physicians provide pregnant patients who come to a hospital emergency department, and are determined to have an EMC, with stabilizing treatment. The EMTALA Guidance offers ectopic pregnancy, severe preeclampsia, emergency hypertension disorders and complications of pregnancy loss as examples of EMCs that require emergency reproductive health care, including abortion.[28] The EMTALA Guidance also discusses issues of preemption of state laws. EMTALA preempts all conflicting state laws, regulations and practices, including more restrictive definitions of EMC and prohibitions against providing necessary abortion care.[29]

In addition to complying with federal rules, covered entities and business associates should ensure that they are in compliance with any new state laws. New York, for example, recently passed a law that "shields companies in the state from having to honor a subpoena request from another state if it relates to legally performed abortion services."[30] Connecticut passed a similar law stating that health care providers generally cannot disclose patient information to law enforcement without a patient's written consent.[31] Patients may seek care, through telehealth or otherwise, from providers in states that permit abortion and provide additional protections for health information.[32] Most states require telehealth patients to be physically present in the state where abortion is permitted in order to receive the telehealth appointment and medication.[33] Thus, states that permit abortion are expecting an influx of patients from other states who need medication abortion.[34] As previously mentioned, New York passed its law in part to protect providers who provide abortion care to nonresidents from legal action outside of the state (e.g., preventing the extradition of abortion providers to states where abortion is banned and providing additional legal protections to providers).[35] We expect more regulation in this area in the coming months, as well as challenges to such laws.

Protection of Health Information on Personal Devices

June 2022 OCR HIPAA Personal Device Guidance

On the same day as the HIPAA Privacy Rule Guidance, OCR issued separate guidance materials related to the privacy and security of an individual's health information on their personal devices (the "HIPAA Personal Device Guidance").[36] Whereas OCR primarily addressed the HIPAA Privacy Rule Guidance to covered entities, the HIPAA Personal Device Guidance addresses the activity of individual patients. The HIPAA Personal Device Guidance explains to individuals that HIPAA generally "does not protect the privacy or security of [] health information when it is access[ed] through or stored on" personal devices, such as cell phones or tablets.[37] Specifically, the HIPAA Personal Device Guidance notes that HIPAA does not apply to geographic location information, Internet search history, information voluntarily shared online or data entered into mobile apps (unless a covered entity provides the app).[38] The HIPAA Personal Device Guidance offers several steps individuals can take to limit the amount of personal data shared with apps, such as turning off location services and app tracking of user activity.[39]

Implications of 2022 Privacy Guidance

The 2022 Privacy Guidance may reflect a lack of public trust in the security of personal information in digital health applications. Consumers are increasingly more aware of how companies gather and use their personal information, including how information relating to health services obtained or sought out may be shared with third parties.[40] For example, women who use digital health tools to track their menstrual cycles have started deleting these apps, concerned that their information is not private and secure.[41] In addition, and as further discussed below, hospitals and other entities have seen an increase in successful lawsuits brought by patients, alleging improper disclosure of their personal health information.[42]

Health care-related businesses, including software development companies, creators of digital health tools, and any health care providers with which they contract, may want to consider limiting the use of certain tracking technologies, including location tracing of app users, or providing other protective measures with respect to such data. These tools are installed within websites that send a packet of data to a designated social media platform whenever a person clicks certain buttons on the website.[43] This tool can become problematic when it is embedded with a hospital's website, tracking when patients schedule doctor's appointments, input search terms about medical conditions and request prescriptions.[44] These tracking tools are also sometimes found within a patient's password-protected patient portal, gathering sensitive information and sending the data to a designated social media platform.

Use of third-party marketing tracing technologies on health care related websites has already resulted in class actions. For example, recently, a class action lawsuit was filed against a hospital system, alleging that the system violated state privacy laws, and another alleging that the recipient was aware that it was improperly receiving patient data.[45] As consumers become more aware of the ways that companies can track and share their activity, they may be less likely to utilize digital health tools. However, there are steps that companies can take to reassure consumers that their personal information, including health information, remains private and secure, including efforts to comprehensively understand how websites, apps, and other Internet-enabled technologies collect, store, and share data.

Companies should continue to monitor developments in this area, including new state and federal laws or guidance. Notably, OCR recently released a request for information ("RFI") asking for comments on what constitutes "recognized security practices" of covered entities and business associates and how individuals should be compensated when harmed by a covered entity or business associate's practices.[46] In light of the RFI, companies should consider reviewing existing data privacy policies and procedures to ensure they are aware of their company's practices, and update workforce training as needed. Covered entities and business associates can also take proactive steps to limit their liability, including ceasing use of tracking technologies in certain circumstances, and either turning off or limiting location and tracking

services for patients on personal devices and browsers. For example, Google recently announced that it would "delete abortion clinic visits from the location history of its users."[47]

Conclusion

The guidance materials issued in the wake of *Dobbs* indicate that federal and state governments are prepared to scrutinize actions by health care providers related to the use and disclosure of sensitive health information, particularly information concerning the use of reproductive health services. Health care providers should ensure that their workforce understands when HIPAA does not permit the disclosure of protected health information, even if requested by a law enforcement official. In addition, health care providers must comply with EMTALA, even when doing so conflicts with state statutes and regulations. Last, companies should review their privacy policies and how they are collecting and sharing consumer data, particularly in connection with how such data may relate to a person's health or use of health care services, to ensure compliance with recent legal development and industry best practices.

Ropes & Gray will continue to monitor developments in this area. If you have any questions, please do not hesitate to contact the authors or your usual Ropes & Gray advisor.

---

1. *See* Interactive Map: US Abortion Polices and Access After *Roe*, *Guttmacher Institute* (last accessed July 17, 2022), at https://states.guttmacher.org/policies/?gclid=EAIaIQobChMIpYOIwIOB-QIVUDizAB2Rng-SEAAYASAAEgKCn_D_BwE.
2. *See* OCR, *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care* (June 29, 2022), at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html; OCR, *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet* (June 29, 2022), at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.
3. *See* Exec. Order No. 14,076, 87 Fed. Reg. 42,053 (July 8, 2022).
4. *See* Press Release, U.S. Dep't Health & Hum. Servs., Following President Biden's Executive Order to Protect Access to Reproductive Health Care, HHS Announces Guidance to Clarify that Emergency Medical Care Includes Abortion Services (July 11, 2022).
5. *See* Kashmir Hill, *Deleting Your Period Tracker Won't Protect You*, N.Y. Times (June 30, 2022), at https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html.
6. 87 Fed. Reg. 19,833 (April 6, 2022).
7. *See* OCR, *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care* (June 29, 2022), at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html.
8. *See* 45 CFR 164.502.
9. *See id.*
10. *See id.*
11. *See id.*
12. *See id.*
13. *See id.*
14. *See id.*
15. *See id.*
16. *See* 45 CFR 164.512(a)(1).
17. *See* OCR, *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care* (June 29, 2022), at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html.
18. *See id.*
19. *See id.*
20. *See* New York Times, *Tracking the States Where Abortion Is Now Banned*, N.Y. Times (updated July 18, 2022), at https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html.
21. *See* Tex. Health & Safety Code § 171.208.
22. For example, Texas' trigger law, which is currently in effect, bans any abortion of an unborn child, with a small exception for cases where continuing the pregnancy would place the mother at risk of death or pose a serious risk of substantial impairment. *See* Tex. Health & Safety Code §§ 170A.011 et seq. The Texas law defines an unborn child as beginning

with fertilization and does not require implantation in the uterus; however, the term abortion refers to the death of an unborn child of a pregnant woman. *See* Tex. Health & Safety Code § 245.002. As such, the most direct impact of the trigger law would be potentially criminalizing selective reduction procedures. Scholars have expressed concern that this law gives "personhood" to a fertilized egg, which could put these IVF procedures in a "legal gray zone" and open the door to limitations on their use in future legislation. *See* Salon article; *see also* NPR article. Additionally, health law experts believe that Texas' abortion statutes have already affected IVF procedures in the state by stopping selective reductions in the IVF process, as this procedure arguably falls under the state's definition of abortion. *See* Salon article.

23. Natasha Singer & Brian X. Chen, *In a Post-Roe World, the Future of Data Privacy Looks Even Grimmer*, N.Y. Times (July 13, 2022), at https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html.
24. Allison Grande, *Dobbs Ruling Lays Bare Data Privacy Protection Gaps*, Law360 (June 29, 2022), at https://www.law360.com/articles/1507152/dobbs-ruling-lays-bare-data-privacy-protection-gaps.
25. *See* U.S. Dep't Health & Hum. Servs., Reinforcement of EMTALA Obligations specific to Patients who are Pregnant or are Experiencing Pregnancy Loss (QSO-21-22-Hospitals-Updated July 2022) (July 11, 2022).
26. *See id.*
27. *See id.*
28. *See id.*
29. *See id.*
30. Allison Grande, *Dobbs Ruling Lays Bare Data Privacy Protection Gaps*, Law360 (June 29, 2022), at https://www.law360.com/articles/1507152/dobbs-ruling-lays-bare-data-privacy-protection-gaps; *see also* N.Y. Crim. Proc. Law §§ 140.10, 570.17.
31. Connecticut Public Act No. 22-19 (2022).
32. *See* Ben Leonard, *What's Next for Virtual Abortions Post-Roe*, Politico (June 24, 2022), at https://www.politico.com/news/2022/06/24/whats-next-for-virtual-abortions-post-roe-00038085.
33. *See id.*
34. *See* Celeste Bott, *Illinois to Become Abortion 'Oasis' in Wake of Dobbs Ruling*, Law360 (June 27, 2022), at https://www.law360.com/publicpolicy/articles/1506375/illinois-to-become-abortion-oasis-in-wake-of-dobbs-ruling?nl_pk=d5ecbd33-53e8-44bb-a373-b4cba99b5d3f&utm_source=newsletter&utm_medium=email&utm_campaign=publicpolicy&utm_content=2022-06-28.
35. *See* Greer Donley, Rachel Rebouche & David S. Cohen, *Abortion Pills Will Change a Post-Roe World*, N.Y. Times (June 23, 2022), at https://www.nytimes.com/2022/06/23/opinion/abortion-pills-online-roe-v-wade.html?referringSource=articleShare; Anna Gronewold, *Abortion Protections in New York Fortified Ahead of SCOTUS Ruling*, Politico (June 13, 2022), at https://www.politico.com/news/2022/06/13/abortion-new-york-scotus-00039191.
36. *See* OCR, *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet* (June 29, 2022), at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.
37. *See id.*
38. *See id.*
39. *See id.*
40. *See* Shira Ovide, *Our Data Is a Curse, With or Without Roe*, N.Y. Times (June 29, 2022), at https://www.nytimes.com/2022/06/29/technology/abortion-data-privacy.html.
41. Natasha Singer & Brian X. Chen, *In a Post-Roe World, the Future of Data Privacy Looks Even Grimmer*, N.Y. Times (July 13, 2022), at https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html.
42. *See* Jeff Lagasse, *Patients Increasingly Suing Hospitals Over Data Breaches*, Healthcare Finance (April 13, 2022), at https://www.healthcarefinancenews.com/news/patients-increasingly-suing-hospitals-over-data-breaches; *Solara Medical Supplies $9.76 Million Data Breach Settlement Gets Preliminary Approval*, HIPAA Journal (May 19, 2022), at https://www.hipaajournal.com/solara-medical-supplies-9-76-million-data-breach-settlement-gets-preliminary-approval/.
43. *See* Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
44. *See id.*
45. *See id.*
46. 87 Fed. Reg. 19,833 (April 6, 2022).
47. Nico Grant, *Google Says It Will Delete Location Data When Users Visit Abortion Clinics*, N.Y. Times (July 1, 2022), at https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html.