As HIPAA Enforcement Discretion Ends, Telehealth and Other Healthcare Providers Reminded of Health Information Privacy and Security Obligations

August 7, 2023 Jennifer Kreick

PRACTICES Telehealth, Healthcare and Life Sciences

While the healthcare industry has been preparing for, and transitioning through, the end of the COVID-19 public health emergency ("PHE") and the corresponding regulatory and operational changes involved, telehealth and other healthcare providers should increase their focus on their health information privacy and security practices. This comes in light of the end of the United States Department of Health and Human Services Office for Civil Rights' ("OCR") Notifications of Enforcement Discretion on Aug. 9, 2023 and OCR's recent warnings regarding online tracking technologies.

During the PHE, OCR published four Notifications of Enforcement Discretion under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including the Notification of Enforcement Discretion for Telehealth ("Telehealth Notification"). Pursuant to the Telehealth Notification, OCR exercised its enforcement discretion to not impose penalties for HIPAA violations against covered healthcare providers in connection with the good-faith provision of telehealth using a non-public-facing remote technology during the PHE. The foregoing enabled healthcare providers to quickly mobilize and provide necessary care through a remote environment. The PHE expired effective 11:59 p.m. on May 11, 2023. Recognizing that certain regulated entities began using telehealth technologies for the first time during the PHE, OCR provided a 90-calendar day transition period to permit covered healthcare provider to bring their telehealth practices into compliance with HIPAA. This 90-calendar day transition period will expire at 11:59 p.m. on August 9, 2023, and the Telehealth Notification will no longer provide a basis for OCR to exercise enforcement discretion with respect to imposing penalties for violations of HIPAA. For suppliers of telehealth equipment and services and the covered healthcare providers that use such telehealth equipment and services, this highlights the importance of ensuring that such telehealth equipment and services comply with HIPAA. In particular, covered healthcare providers should ensure they have any necessary business associate agreements in place with video chat applications and scheduling applications.

In addition, on July 20, 2023, the OCR and the Federal Trade Commission ("FTC") issued a joint warning to telehealth providers and hospital systems about the privacy and security risks to consumer's sensitive personal health data associated with online tracking technologies. Websites and mobile apps may integrate online tracking technologies that collect and analyze information about how users interact with the website or mobile app, which may include identifiable health information. This information may be sent to the third party that developed the technology. OCR highlighted its concerns with the use of tracking technologies and reminded HIPAA-regulated entities about their compliance obligations in its guidance issued in December 2022, including the need to enter into a business associate agreement or obtain a HIPAA-compliant authorization prior to disclosing protected health information in connection with the use of third-party tracking technology. The FTC, with its regulatory authority to protect the public from deceptive or unfair business practices and from unfair methods of competition, has also focused on the unauthorized

disclosure of personal health information through the use of tracking technologies, which may violate the FTC Act and constitute a breach of security under the FTC's Health Breach Notification Rule. The FTC's recent enforcement actions highlight the risks that telehealth providers and other health technology companies face, particularly those that are not regulated by HIPAA, when they do not closely monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps and do not obtain consumer authorization and or make adequate disclosures in their privacy policies.

The end of enforcement discretion under the Telehealth Notification and the recent emphasis on tracking technology comes as cyber-attacks against the healthcare industry continue to present significant threats to patient safety, hospital operations and personal health information. Recent ransomware attacks against health systems have forced systems offline and affected millions of patients[1]. While hospitals and health systems are often targeted, cyber criminals also exploit perceived security gaps in vendors and suppliers that access health information. These recent events highlight the need for telehealth and other healthcare providers, as well as healthcare technology developers, suppliers, and innovators, to review the flow of health information to third parties and ensure compliance with applicable regulations.

For additional guidance and legal counsel, please contact one of the lawyers listed below.

---

[1]See, *e.g.*, The New York Times, Rebecca Carballo, Ransomware Attack Disrupts Health Care Services in at Least Three States (Aug. 5, 2023), *available at*: https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html.