APRIL 9, 2020

HIPAA Enforcement Discretion During the COVID-19 Public Health Emergency

For more information, contact:

Marcia Augsburger
+1 916 321 4803
maugsburger@kslaw.com

Gina Cavalier
+1 202 626 5519
gcavalier@kslaw.com

Rob Keenan
+1 404 572 3591
rkeenan@kslaw.com

Adam Solander
+1 202 626 5542
asolander@kslaw.com

Igor Gorlach
+1 713 276 7326
igorlach@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

Over the last two months, the U.S. Department of Health and Human Services ("HHS") published guidance regarding the enforcement of HIPAA and its privacy and security requirements in response to the COVID-19 public health emergency ("PHE"). To date, the HHS Office for Civil Rights ("OCR"), which enforces HIPAA, has announced that it would not impose penalties during the PHE for violation of certain HIPAA rules in connection with the following:

I. Providing telehealth services via apps that are not HIPAA compliant;

II. Business Associates' use and disclosure of protected health information ("PHI") for public health and health oversight activities; and

III. Specified privacy rule requirements applicable to hospitals, but only for violations during the first 72 hours after hospitals institute disaster protocols.

The Substance Abuse and Mental Health Services Administration ("SAMHSA") also issued guidance for providers offering telehealth or telephonic consultations to substance use disorder patients during the PHE. SAMHSA advised that providers may disclose or use substance use patient identifying information and records without first obtaining written patient consent. The guidance and announcements are discussed in Part I below.

While covered entities and their business associates are able to take advantage of the enforcement discretion to care for patients and cooperate with public health agencies, caution is warranted. Compliance with HIPAA regulations is still required by law, and entities subject to HIPAA should continue to observe privacy and security procedures as feasible and otherwise work to reduce or contain their compliance risk. We outline below in Part II measures that providers and business associates may consider undertaking to mitigate risk during the PHE.

ENFORCEMENT DISCRETION AND GUIDANCE IN EFFECT DURING THE PHE

Telehealth

On March 17, OCR began exercising its enforcement discretion with respect to the provision of telehealth services, pursuant to guidance published as a notification and a FAQ sheet. OCR stated that it would not enforce penalties for noncompliance with HIPAA regulatory requirements against covered health care providers "in connection with the good faith provision of telehealth during [the PHE]," referring specifically to the technology used to provide services via telehealth. OCR's enforcement discretion applies to services that are related to the diagnosis and treatment of COVID-19 as well as services that are not.

HIPAA security regulations require that video and other transmissions between distant site providers and patients at originating sites be secure in accordance with industry standards. This places telehealth providers at risk of violating HIPAA requirements if they use FaceTime and other popular video conferencing apps that do not have a high level of security and with whose developers healthcare providers cannot enter into business associate agreements. Because the HHS Secretary agreed to permit originating sites to include patients' homes, OCR apparently recognized a need to loosen the required standards and permit transmissions through popular apps that allow one-on-one video conferencing but that may not be HIPAA compliant. Under the guidance, a covered health care provider may use any non-public facing audio or video communication product to provide telehealth services to patients during the PHE. The exercise of enforcement discretion is not limited to telehealth for the treatment and diagnosis of COVID-19.

OCR provided the following as examples of permissible apps for good faith telehealth use during the PHE: Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, and Skype. OCR encouraged providers to use apps provided by vendors who enter into business associate agreements with users and comply with HIPAA standards (such as Microsoft Teams and Doxy.me), but confirmed that it would not penalize providers for "using less secure products in their effort to provide the most timely and accessible care possible to patients during the [PHE]." OCR stated that if PHI is intercepted during the transmission of telehealth services provided in good faith by a health care provider, OCR would not pursue otherwise applicable penalties for breaches.

OCR did not elaborate on what constitutes "good faith." However, OCR's examples of "bad faith" provision of telehealth services include conduct in furtherance of a criminal act (fraud, identity theft, invasion of privacy), further using or disclosing patient data in violation of the HIPAA rules (sale of data, use for marketing without authorization), violating state licensing laws or professional conduct standards in the provision of telehealth services, or using public-facing remote communication products like TikTok, Facebook live, or Twitch to provide telehealth services.

Use and Disclosure by Business Associates for Public Health and Health Oversight Activities

While covered entities are already permitted to use and disclose PHI for public health activities and for health oversight activities, business associates are not authorized to do so absent express delegation from the covered entity. This delegation is not commonly included in business associate agreements. Recognizing this limitation, OCR published an enforcement discretion notice aimed at business associates' actions. Pursuant to the notice, OCR will not impose penalties against a business associate or covered entity under certain regulatory provisions if:

- the business associate makes a good faith use or disclosure of the covered entity's PHI for public health activities consistent with 45 C.F.R. § 164.512(b), or health oversight activities consistent with 45 C.F.R. § 164.512(d); and
- the business associate informs the covered entity within ten calendar days after the use or disclosure occurs or commences.

The waived requirements covered by the notice are 45 C.F.R. §§ 164.502(a)(3) (prohibiting a business associate from using or disclosing PHI except as authorized by a business associate contract or as required by law), 164.502(e)(2) (requiring written assurances by business associate to covered entity with respect to safeguarding PHI), and 164.504(e)(1) and (5) (pertaining to breaches of business associate agreements, including with subcontractors). Business associates remain responsible for compliance with other requirements, including the implementation of safeguards to maintain the confidentiality, integrity, and availability of PHI, such as by ensuring secure transmission of electronic PHI to the public health authority or health oversight agency.

72-hour Waiver for Hospitals Implementing a Disaster Protocol

As of March 15, OCR waived sanctions and penalties against any hospital that institutes a disaster protocol and that does not comply with the following provisions of the HIPAA Privacy Rule in the 72 hours from the time the hospital implements its disaster protocol:

- The requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care (45 C.F.R. § 164.510(b));
- The requirement to honor a request to opt out of the facility directory (45 C.F.R. § 164.510(a));
- The requirement to distribute a notice of privacy practices (45 C.F.R. § 164.520);
- The patient's right to request privacy restrictions (45 C.F.R. § 164.522(a)); and
- The patient's right to request confidential communications (45 C.F.R. § 164.522(b)).

Substance Use Disorder Patient Records

SAMHSA issued an announcement on March 19 that the medical emergency exception set forth in 42 C.F.R. § 2.51 permits providers offering telehealth or telephonic consultations to substance use disorder patients during the PHE to disclose or use patient identifying information and records without first obtaining written patient consent for disclosure. Following the disclosure, the disclosing provider must document in the records the name of recipient, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency.

MEASURES TO MINIMIZE RISK

During the PHE and despite the waivers and enforcement relief HHS is extending, covered entities and business associates should make sure they are continuing to follow HIPAA and its implementing Rules, as well as entity-specific compliance processes to minimize their risk as possible under the circumstances. It is important to remember during this PHE that OCR's enforcement discretion is not a broad waiver of HIPAA or its implementing Rules. It also does not affect the application of other federal laws and of state laws (such as state privacy and consumer protection laws) and the waivers and guidance they are issuing will not preclude all civil lawsuits. The following are examples of measures that are particularly important during the PHE to ensure compliance and/or that will help minimize risk:

- When health care providers obtain authorization from their patients to proceed with the services via telehealth, they should fully inform their patients of the potential for interception and security issues and that the app being used is not or may not be compliant with HIPAA regulations and standards;
- Providers should document the patients' consent to proceed despite the risks;
- Providers should ensure that all devices used to deliver telehealth are password-protected;
- Providers should use HIPAA-compliant devices and software when available;

- Any patient information remaining on any device or software following a telehealth session should be removed as soon as possible after documenting the encounter for medical record purposes as required under the circumstances;
- Telehealth transmissions should be through private Wi-Fi networks;
- Telehealth services should be provided in a private location, with reasonable precautions to reduce the possibility that the information may be overheard;
- Covered entities and business associates should revise or create interim privacy and security policies and notices of privacy practices ("NPPs") to ensure that they reflect the use and disclosure of information during the PHE;
- Health care providers should continue providing NPPs to new patients and new NPPs to all patients when doing so does not cause a burden or delay in treatment, or at a minimum make sure NPPs are posted;
- Health care providers should ensure compliance with medical record requirements;
- Business associates should ensure safeguards are in place and effective to ensure secure transmission of electronic PHI to public health authorities or health oversight agencies; and
- Covered entities and business associates should continue to comply with federal and state laws that are not affected by HHS's guidance.

OCR also compiled and provided guidance on the relevant provisions of the HIPAA Privacy Rule pertaining to the use and disclosure of patient information during an emergency situation such as an outbreak of infectious disease. Covered entities should review this compilation and guidance, which covers the sharing of patient information for treatment, public health activities, and to prevent a serious and imminent threat to patients and their family, friends, and others. The guidance provides helpful examples of the applicability of HIPAA standards to factual scenarios during the PHE, such as the disclosure by a covered entity to the Centers of Disease Control and Prevention PHI on an ongoing basis as needed to report all prior and prospective cases of patients confirmed to have COVID-19.