COSMOS
Navigate the Compliance Universe

Compliance Today - October 2020
OCR's COVID-19 regulatory relief: Changing how we deliver care

By Jessica Quinn, Esq. and Vladimir Edmondson, MPAff, CHC

Jessica Quinn (jessica.quinn@ohiohealth.com) is Senior Vice President, Chief Ethics and Compliance Officer, and **Vladimir I. Edmondson** (vlad.edmondson@ohiohealth.com) is Senior Compliance Director and Chief Privacy Officer at OhioHealth in Columbus, OH.

Almost 25 years ago, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), establishing a national framework for patient privacy.[1] To ensure an appropriate balance between individual privacy rights and public health needs, Congress included the following statutory language: "Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention."[2] Consistent with this congressional intent, when drafting the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule),[3] the secretary of the U.S. Department of Health & Human Services (HHS) incorporated a savings clause to exempt state public health laws from preemption and a number of important exceptions for public health activities.[4]

As the COVID-19 pandemic has unfolded, healthcare providers have proven to be critical players in the fight against the pandemic through preventing, treating, and recovering from COVID-19 in, at times, nontraditional ways not necessarily contemplated by privacy laws. To ensure that those engaged in the COVID-19 fight are not unnecessarily restricted under the Privacy Rule, the HHS Office for Civil Rights (OCR) began to issue a rapid-fire series of regulatory relief documents providing covered entities the relief they needed to fight a pandemic of this magnitude. To date, OCR has issued three notifications of enforcement discretion, four separate guidance documents, and two bulletins focused on the COVID-19 response. OCR's early efforts to address the not-yet-declared pandemic began in early February when it issued, without fanfare, the "BULLETIN: HIPAA Privacy and Novel Coronavirus."[5] While not yet extending regulatory relief, the February bulletin highlighted ways in which covered entities and their business associates could continue to permissibly share patient information and put them on notice that they must continue to implement and apply reasonable, as well as administrative, physical, and technical, safeguards to protect patient information. This regulatory relief is not without limitations, however, and a careful understanding of the guardrails for these temporary regulatory changes is critical to help navigate through these changes without inadvertently crossing the line into noncompliance.

Telehealth regulatory relief guardrails

The first series of regulatory relief applies to telehealth, arguably one of the most important tools for the healthcare industry during this public health emergency.[6] Pre-public health emergency application of HIPAA would have required, among other things, covered healthcare providers to satisfy requirements set out in the HIPAA Privacy, Security, and Breach Notification rules, including:

- Providing the covered entity's Notice of Privacy Practices no later than the date of the first service delivery and, if the first service delivery to an individual is delivered electronically, the covered healthcare provider must provide electronic notice automatically and contemporaneously in response to the individual's first

request for such service;[7]

- Obtaining satisfactory assurances from the engaged telehealth technology vendor (i.e., the business associate) that the vendor will appropriately safeguard protected health information (PHI) prior to any disclosure of PHI made by the covered healthcare provider to the business associate, in the form of a written contract or other written agreement or arrangement with the business associate (e.g., business associate agreement);[8] and
- Performing third-party security reviews of potential telehealth technology vendors to reasonably determine their ability to comply with the HIPAA Privacy and Security rules.[9]

In this series, OCR relieved covered entities from HIPAA-related penalties for the *good-faith* provisioning of telehealth, thereby significantly expanding the available vendors and vendor tools a covered healthcare provider may use to deliver telehealth. A thorough understanding of what OCR considers "good faith" in this context is critical, however, to avoid noncompliance.

March 17 telehealth notification

On March 17, when 7,038 COVID-19 cases in the United States were reported by the U.S. Centers for Disease Control and Prevention,[10] OCR issued its first Notification of Enforcement Discretion.[11] In its March 17 telehealth notification, OCR feverishly removed one of the telehealth hurdles that had been arguably blocking many covered healthcare providers from fully switching to telecommunication technologies that support and promote the delivery of healthcare in the living rooms, bedrooms, and kitchen tables across our country. In one regulatory swoop, OCR paved the way for covered healthcare providers to make technologically delivered house calls in response to the pandemic through nonpublic-facing remote audio/video communication platforms and products (e.g., Apple FaceTime, Facebook Messenger, Google Hangouts, WhatsApp, Zoom, Skype, Signal, Jabber) that are not necessarily compliant with HIPAA.[12]

Roger Severino, OCR director, announced at that time that this initial exercise of enforcement discretion was being made in an effort to empower "medical providers to serve patients wherever they are during this national public health emergency."[13] To carry this through, OCR declared that it would "not impose penalties for noncompliance with the regulatory requirements under the HIPAA rules against covered health care providers in connection with the good faith provision of telehealth during the COVID–19 nationwide public health emergency."[14]

But what exactly does the good-faith provisioning of telehealth look like to OCR? In its March 17 telehealth notification, OCR hinted at what covered healthcare providers—those healthcare providers who conduct one or more covered healthcare transactions electronically, such as transmitting healthcare claims to a health plan[15]—could do that one might reasonably believe demonstrates the good-faith provisioning of telehealth, such as (a) notifying their patients that third-party telehealth applications potentially introduce privacy risks, (b) enabling all available encryption and privacy modes when using such applications, (c) engaging telehealth services through technology vendors who represent that they are compliant with HIPAA, and (d) entering into HIPAA business associate agreements with such vendors.

March 20 FAQs

On March 20, three days and just over 11,000 additional COVID-19 cases later;[16] OCR provided important insight into what would be considered good-faith provisioning of telehealth when posting its "FAQs on Telehealth and

HIPAA during the COVID-19 nationwide public health emergency" (March 20 FAQs).[17] OCR noted that when determining what constitutes the good-faith provision of telehealth services, it would reserve the right to consider all facts and circumstances, including "[f]or example, if a provider follows the terms of the Notification and *any applicable OCR guidance*" (emphasis added). In the March 20 FAQs, OCR also provided the other guardrail by setting out in the alternative what OCR would consider *bad faith*, including:

- "Conduct or furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy;
- "Further uses or disclosures of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (*e.g.*, sale of the data, or use of the data for marketing without authorization);
- "Violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth (*i.e.*, based on documented findings of a health care licensing or professional ethics board); or
- "Use of public-facing remote communication products, such as TikTok, Facebook Live, Twitch, or a public chat room, which OCR has identified in the [March 17 telehealth notification] as unacceptable forms of remote communication for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communication."

March 28 bulletin

Eight days and more than 100,000 new COVID-19 cases later,[18] OCR provided an additional guardrail for our vulnerable populations in its "BULLETIN: Civil Rights, HIPAA, and the Coronavirus Disease 2019 (COVID-19)" (March 28 bulletin).[19] It must be noted first though that on both March 17[20] and March 20,[21] Director Severino cautioned that OCR is "especially concerned about reaching those most at risk, including older persons and persons with disabilities." Further, on March 28, Director Severino committed that "[p]ersons with disabilities, with limited English skills, and older persons should not be put at the end of the line for health care during emergencies."[22] To that end, the March 28 bulletin[23] warned that "as resources allow, government officials, health care providers, and covered entities should not overlook their obligations under federal civil rights laws to help ensure all segments of the community are served by:

- "Providing effective communication with individuals who are deaf, hard of hearing, blind, have low vision, or have speech disabilities through the use of qualified interpreters, picture boards, and other means;
- "Providing meaningful access to programs and information to individuals with limited English proficiency through the use of qualified interpreters and through other means."