Battling cyber criminals and protecting patient information during the COVID era, Crain's Chicago Business

Emily A. Johnson | Monday, June 13, 2022

This article originally appeared in Crain's Chicago Business on June 13, 2022.

The world was turned upside down in 2020, and the practice of medicine changed overnight as providers were forced to adapt to the complexities and risks presented by the COVID pandemic. Concern for staff and patient exposure to the virus caused many providers to jump feet first into the telehealth space with little or no previous experience – making them easy targets for cybersecurity attacks.

Telehealth is defined by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration. During COVID, telehealth presented a safe option to offer treatment to patients without requiring them to physically come to an office for a visit.

Evolution of telehealth during the COVID era

Prior to the pandemic, only a small percentage of providers worked in practices that offered telehealth. State laws varied on when and how telehealth could be rendered and what modalities could be used to provide such services.

In response to the pandemic, the Office for Civil Rights (OCR) announced it would exercise enforcement discretion and would waive potential penalties against healthcare providers for violations of the Health

Insurance Portability and Accountability Act (HIPAA). This enforcement discretion applied to widely available, non-public facing communication applications like FaceTime or Skype when used in good faith for the provision of telehealth for any treatment or diagnostic purpose, not just treatment or diagnoses related to COVID. The purpose of this enforcement discretion was to encourage all providers to continue to serve their patients during the public health emergency period, and to protect those patients who were particularly at risk for contracting COVID by offering alternative treatment settings.

Just three days after announcing its enforcement discretion, OCR issued guidance explaining how providers could use video communication tools to offer telehealth to patients responsibly. The guidance clarified that public facing applications like Facebook Live and TikTok were not acceptable forms of remote communication for telehealth because they are designed to be open to the public and created an inherent risk of unauthorized disclosure of patient information. Instead, the guidance stated that non-public facing applications like FaceTime, Facebook Messenger video chat, and Zoom were acceptable.

The enforcement discretion and corresponding guidance caused many providers to pivot from their traditional in-office treatment and into the digital health space. What followed was a large increase in the number of providers practicing via telehealth.

Confusion surrounding HIPAA enforcement discretion

The enforcement discretion created confusion among many providers, who mistakenly believed the requirements of HIPAA were waived during this period, including the requirements to safeguard patient information under the Privacy and Security Rules and the obligations to provide notification under the Breach Notification Rule of any breaches of patient information. The enforcement discretion announced by OCR was simply discretion and not a waiver of HIPAA – and the requirements of the Privacy, Security, and Breach Notification Rules remained in full force and effect.

In addition to the confusion surrounding the status of HIPAA, many providers quickly began offering telehealth services to their patients on the premise that the government had waived the requirements for licensure and establishment of a legitimate patient encounter set forth under state law. Many states issued executive orders that created flexibilities for the provision of telehealth. However, in the absence of any such order, state telehealth rules and regulations remained in effect. The HIPAA enforcement discretion related solely to HIPAA and had no impact on state laws.

Increased cybersecurity attacks against healthcare providers

As providers quickly began to provide telehealth services, they became easy targets for cybersecurity attacks. While the flexibilities afforded by state executive orders and the HIPAA enforcement discretion made it much easier for patients to access virtual care, it also created access for cyber criminals. Many providers had no prior digital presence and therefore had very few technical safeguards in place to prevent cyberattacks and unauthorized use or disclosure of patient information. Providers offered telehealth to patients utilizing less secure technology without advising them of the potential risks associated with such technology. This led to a recognizable increase in the number of cyberattacks and unauthorized disclosures of patient information. One common form attack was known as Zoom bombing, where intruders would enter video conferences without authorization.

When cyberattacks occur involving unauthorized access, use, acquisition, or disclosure of patient information, there is a presumption under HIPAA that a breach occurred and that notification is required to impacted individuals and OCR, unless an exception applies. If the breach involves 500 or more

individuals, OCR will commence an investigation of the incident to determine if the covered entity (or business associate, as applicable) complies with the requirements of HIPAA. If OCR concludes that the provider failed to comply with HIPAA, the provider may be assessed fines or penalties.

Aggressive government investigations

Since the onset of the pandemic, the government has spent an astonishing sum of money to address the complexities caused by COVID. As a result, the government has become particularly aggressive in its attempt to reclaim at least a portion of the money it spent. Government investigations, including those performed by OCR, have become more complex and the risk of fines or penalties being assessed appears to be higher than ever.

As we move toward a hopeful end of the public health emergency period or adjust to this new normal, providers may continue to offer telehealth services. However, state regulations have not quite caught up with the current telehealth landscape that exists under state executive orders and the HIPAA enforcement discretion announced in response to COVID. There is hope that states will revise their regulations, but until that happens, providers are left with the existing regulatory framework. As soon as the public health emergency period ends, the prior regulatory framework will apply and providers must be prepared to revert their practices back to how they operated pre-pandemic, or they will have to adapt their telehealth services to comply with existing state laws and regulations.

Emily A. Johnson