# Health Law Daily Wrap Up, STRATEGIC PERSPECTIVES: Telemedicine and HIPAA—a balance of speed and security, (May 17, 2018)

Health Law Daily Wrap Up

Click to open document in a browser

By Bryant Storm, J.D.

As telemedicine expands its influence in the health care industry, telemedicine providers are facing novel privacy and security risks. CMS continues to promise expanded use of telemedicine in the federal health care programs and the Government Accountability Office (GAO) has given telemedicine more than one favorable review—all signs that telemedicine will see increased usage in the coming years (see *Top 5 ways telemedicine improved its connections in 2017*, December 27, 2017). While the growth of telemedicine is a boon for health care access, Kelly A. Thompson cautioned, "the same benefit that makes telemedicine such a convenient option for patients and providers alike" is also "the biggest threat to protecting patient information."

This Strategic Perspective provides expert analysis on the intersections between telemedicine, compliance with the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191), and data protection. For this Strategic Perspective, Wolters Kluwer interviewed Kelly A. Thompson, Ashley Thomas, Chanley T. Howell, and Jayme Matchinski. Thompson is a health care business lawyer with Foley & Lardner LLP; Thomas is a health care attorney at Baker Donelson. Howell is a partner and intellectual property lawyer with Foley & Lardner LLP and Matchinski is an attorney at Greensfelder, Hemker & Gale, P.C.

**Data Protection**

Thompson stressed that "health care providers treating patients via telemedicine have the same obligations to protect patient health information under the HIPAA Privacy and Security Rules as providers that treat patients face to face." She noted, however, that "having a provider at the tip of your fingertips can lead to communication between the provider and patient through unsecure channels, such as text and email, leaving patient health information at risk of being intercepted or shared to unauthorized recipients." Thus, she said, telemedicine providers in particular need to take steps to "preserve the integrity of the patient health information during telemedicine consults." Those steps include the use of secure technology, data encryption, and sound business associate agreements.

**Business Associates.** Thomas noted, "one of challenges of telehealth is the increased number of people, independent of the medical team, who have potential access to a patient health information as a provider will need contract with third parties to provide the capabilities for transmitting, storing, and maintaining health information via telemedicine." Thus, business associates (BAs) are an essential component of telemedicine. "By definition," Howell said, "practitioners conducting telemedicine services are transmitting [protected health information] PHI and storing it in clouds and, therefore, must enter into business associate agreements (BAAs) with a variety of different vendors, including HIPAA compliant cloud hosting companies and HIPAA compliant email or SMS [short message service] providers. Increased risks come with a telemedicine practice so it is important for providers to conduct vendor due diligence on data security practice and controls and enter into a HIPAA compliant BAA."

Matchinski explained that "health care providers who practice telemedicine are not expected to become experts in firewalls, data encryption, or network security. Health care providers are responsible for choosing telemedicine vendors who are experts in these areas. Matchiniski explained, "The HIPAA Privacy Rule allows covered entities, including health care providers, to disclose PHI to their business associates (BAs) as long as the patients' PHI is safeguarded." Additionally, "health care providers who practice telemedicine should have BAAs with each BA to ensure that the BAs do not misuse the information, including the [electronic PHI] ePHI, which results in an authorized disclosure of such ePHI." She recommended "health care providers... take additional

steps to scrutinize BAs regarding the BA's telemedicine background and expertise and the BAAs ...include well drafted indemnification and insurance provisions which specifically address telemedicine and what occurs in the event there is a violation of the HIPAA regulations and the BA is the cause of an unauthorized disclosure of ePHI."

**Exception to the BA rule.** Not every entity involved in the transmission of telemedicine data necessarily qualifies as a BA necessitating a BAA. Howell noted, "Under HIPAA's conduit exception, random access by a data transmission entity does not necessarily make the entity a HIPAA business associate, and this is where it gets confusing. A provider of pure ISP (internet service provider) services typically is a conduit, as [this type of provider] determine[s] whether PHI being transmitted over its network is arriving [at] its intended destination, but do[es] not access or store the data." Further, he said, "the preamble to the [Privacy] Rule explicitly states that the 'mere conduit' exception is intended to include organizations that deal with 'any temporary storage of transmitted data incident to such transmission.' The preamble goes on to define the distinction between transmission (including incidental storage associated with such transmission) and ongoing storage." The key difference between these two situations, he explained, "'is the transient versus persistent nature of' the opportunity to access PHI. If the PHI is transient, a BAA is not required."

**Encryption and devices.** "HIPAA falls short in protecting patient information, specifically ePHI that is transmitted through telemedicine, because ePHI is often being downloaded or stored on unsecured mobile devices," Matchinski noted. She said, "Providers should be cautious with any ePHI that is being stored on their mobile devices. Password protecting the device, installing a remote wipe software on the mobile device to erase ePHI if the mobile device is lost or stolen, and requiring a review of data stored on the devices before the device is thrown away or recycled are a few precautions health care providers can take to protect ePHI that is transmitted through telemedicine and comply with the HIPAA regulations." Matchinski also raised security concerns regarding instances when a "provider communicates with patients outside of a secure portal. While telemedicine can make connecting with patients easy through the use of smartphones, the use of smartphones can also encourage communication via text or email which are unsecure modes of communication and in violation of the HIPAA Security Rule. Any specific identifiable health information, including ePHI, needs to be protected with encryption and should not be sent outside of telemedicine apps or tools that the health care provider knows are secure."

Matchinski also said "data protection mechanisms, including encryption, are essential for the security of telemedicine and compliance with the HIPAA Privacy and Security rules and regulations." She noted, the HIPAA regulations were originally promulgated to secure and protect a patient's PHI from unauthorized disclosure. The HIPAA Privacy and Security Rules required health care providers to establish appropriate administrative, technical, and physical safeguards to protect the privacy of health information."

Thomas echoed these comments, saying "the way to secure the transmission of PHI is through encryption. Patients and providers are becoming increasingly comfortable with communicating via telemedicine and through text messaging, email, [and] video but it is important to keep in mind that these tools are not always HIPAA compliant and encrypted."

**De-identification.** "Risk can be reduced," Thompson explained, "for companies providing telemedicine services if patient data can be de-identified, particularly when sharing PHI with a third party. De-identification can be accomplished though the removal of a list of patient identifiers in a manner that truly makes the information de-identifiable from the patient, or by hiring an expert statistician to de-identify the data. Following the de-identification of data, the information is no longer subject to protections under HIPAA."

**Patient education.** Thomas noted that "a patient may want to have a telemedicine appointment from their home. In such cases, "patient[s] need to consider whether their home Wi-Fi network is secure enough. Not everyone has their home network properly secured. Patients should be educated about these types of risks."

**Medicare Coverage**

Medicare covers 81 distinct telehealth services including: consultations, office visits, and psychiatry services, furnished through a telecommunications system with audio and video equipment permitting two-way, real-time, interactive communication between a patient and a remote provider. Medicare primarily restricts the use of such services to rural areas or regions designated as having a shortage of health professionals. The GAO found that the use of telehealth services in Medicare showed several positives, ranging from improved quality of care, relief from provider shortages, and improved convenience (see High quality is seldom far away with telehealth, April 17, 2017; Factors, potential impact of expanded telehealth services for Medicare patients, July 21, 2017).

Matchinski noted that, "Social Security Act §1834(m) defines the conditions for payment for telehealth services under Medicare. The Social Security Act requires that a patient must be present at a rural, clinical originating site to receive care via telehealth. Medicare reimbursement for telehealth is only available at clinical sites in rural areas, and patients seeking care in metropolitan areas are unable to access these services. In 2015, CMS added additional telehealth coverage, including seven telehealth billing codes for: psychotherapy, prolonged office visits, and annual wellness visits conducted through electronic means. CMS also added language to pay for remote patient monitoring for chronic conditions. Prior to 2015, Medicare did not pay separately for these services and bundled them into 'evaluation and management' codes."

**General Data Protection Regulation**

The General Data Protection Regulation (GDPR) was approved by the European Union (EU) Parliament on April 14, 2016, and will be enforceable beginning on May 25, 2018. The GDPR replaces the EU's Data Protection Directive and is designed to unify data privacy laws across Europe. Matchinski indicated, "health care providers in the U.S. who care for EU patients via telemedicine will need to revisit consent forms, data sharing, and privacy monitoring because the GDPR will significantly change the way physicians and digital health companies approach patients and patient data."

Thompson explained that "the use of telemedicine enables providers to treat patients remotely, and if the provider is treating EU residents, providers are required to comply with GDPR's strict data protection standards." Even without a geographic presence in the EU, if a health care provider targets, solicits, or has patients in the EU, Thompson said, "then GDPR applies." If GDPR applies than additional EU requirements including required consents before collecting information, certain patient access rights, destruction requirements, and agreements with third party service providers must be implemented."

Thomas added that "academic medical centers (AMCs) increasingly provide care beyond U.S. borders and may have consultative relationships with EU providers where telemedicine may be used, implicating the GDPR. In addition, the AMCs or health care organizations may sponsor or coordinate a clinical trial in the EU that may require telemedicine services."

Matchinski recommended that stakeholders "stay tuned for the actual impact of the GDPR on telemedicine once the enforcement date arrives later this month."

**What's next for Telemedicine?**

As telemedicine increases its presence as a health care delivery mechanism, increasing numbers of entities will be impacted by privacy concerns. Stakeholders should begin by scrutinizing their BAs and BAAs. Additionally, entities need to take steps to secure devices and encrypt and de-identify data. Providers should be careful to consider how different types of telehealth services might implicate different privacy and security concerns. Additionally, as telemedicine progresses and increases its presence in health care, providers should be attentive to changing rules and regulations.

Attorneys: Ashley Thomas (Baker, Donelson, Bearman, Caldwell & Berkowitz, PC). Kelly A. Thompson and Chanley T. Howell (Foley & Lardner LLP). Jayme Matchinski (Greensfelder, Hemker & Gale, P.C.).

MainStory: StrategicPerspectives CMSNews ClinicalNews CoPNews CyberPrivacyFeed EHRNews HITNews HIPAANews ProgramIntegrityNews