2021 Annual Conference
August 11-13, 2021
Atlanta, GA

Tele/Health Boom: Liability, Privacy, Security, Cyber and Other Coverage Issues

I. What is Tele/Health

Tele/health, or tele/medicine, is the use of electronic information and telecommunication technologies to provide care when a patient and physician or healthcare provider are not in the same place at the same time. Using a telephone or a device with internet access, a patient can talk to your doctor live over the phone or video chat, send and receive messages from your doctor using chat messaging, email, secure messaging, and secure file exchange; and/or use remote patient monitoring to allow a physician to check on you at home. For example, you might use a device to gather ECG or other vitals to help your doctor stay informed on your progress. https://telehealth.hhs.gov/patients/understanding-telehealth/. Tele/health has grown in popularity during the COVID-19 pandemic because it has allowed patients and healthcare providers to limit physical contact, thereby reducing everyone's exposure to COVID-19. Patients have embraced it because it allows them to address health issues wherever they are, even from the comfort of home; cuts down on commuting, travel in bad weather, time off from work, and the need for child care; and can shorten wait times to see a provider and expand the range of access to specialists for people who do not live in close proximity to those services. Id. However, even the U.S. Department of Health and Huma Services website specifically warns that "Telehealth is not a perfect fit for everyone or every medical condition. Make sure you discuss any disadvantages or risks with your doctor."

II. Regulations

Medical Providers: States have different laws concerning when and how telehealth may be practiced, so it's important to check state statutes, regulations and policies, as well as state licensure boards regarding practice limitations before initiating services. In addition, the Centers for Medicare & Medicaid Services provide information on the scope of Medicare telehealth services. State professional licensing boards also regulate

who can legally provide tele/health services (known as a 'qualified providers'). Practitioners must also be appropriately licensed/certified/credentialed to practice in the state where their patient/client is located, and work under that state's scope of practice. Some states limit the kinds of providers that can provide services via telehealth. Practitioners must also be appropriately licensed/certified/credentialed to practice in the state where their patient/client is located, and work under that state's scope of practice, which may not be the same state where the provider is located. Some states and professions have entered into interstate compacts to expedite licensing of practitioner seeking to practice in multiple states. Practitioners must adhere to traditional clinical standards of care, and practice within the scope of practice authorized by law. The American Telemedicine Association has also promulgated a variety of practice guidelines.

HIPAA and HITECH: The HIPAA Privacy and Security Rules, HITECH, as well as all Administrative Simplification rules, apply to "covered entities", which include health plans, healthcare clearinghouses, and any health care provider who submits transactions electronically, like claims. Healthcare providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care. However, the HHS Office for Civil Rights (OCR) announced on March 17, 2020, that it would waive potential HIPAA penalties for good faith use of telehealth during the nationwide COVID-19 public health emergency. This applies to tele/health provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19. This notice meant that covered health care providers could use popular "apps" for video chats, such as Zoom, FaceTime, Google Hangouts video, and Skype (as opposed to more secure platforms), to provide telehealth during the COVID-19 crisis, without the risk of incurring a penalty for HIPAA noncompliance. Best practices would dictate that health care providers using these apps notify patients that such third-party apps potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications. Additionally, health care providers may also add privacy protections by providing tele/health video communication services through HIPAA compliant technology vendors, entering into HIPAA business associate agreements (BAAs) in connection with provision of their video communication products etc.

Cyber: The United States has not enacted overarching legislation governing cyber security. As a result, all 50 states have adopted their own laws and regulations, which vary widely as to stringency of cyber protocols and compliance, reporting and consumer notification requirements in the event of a breach, response timing and parameters, and penalties. Additionally, the EU has adopted very stringent laws under the GDPR, which differ significantly from U.S. rules/requirements, and within the EU, certain countries

such as Germany, have adopted their own even more stringent rules (including criminal penalties in some instances). As a result, depending on where a health care provider, patient, and the pertinent PHI are located/stord, multiple states' and countries' laws could come into play in the event of a security or data breach.

III. Risks

The risks of tele/medicine are proliferating, especially with changes due to the COVID-19 pandemic, beyond the professional liability scope. As a threshold matter, even though HIPAA requirements are "relaxed" during a pandemic to allow use of less secure video apps for medical "visits," health care providers still have a legal and ethical obligation to protect patients' private health information (PHI), which may be complicated by providing services remotely. HHS has advised that "Providers should always use private -locations and patients should not receive telehealth services in public or semi-public settings, absent patient consent or exigent circumstances[;]" and recommended using lowered voices, not using speakerphones, and suggesting patients move away from others when discussing PHI. Additionally, many health care providers, including large hospital networks, may not have the IT resources or infrastructure to host and maintain their own tele/health platform, and may rely on third-party platforms, creating additional risks. Health care facilities such as hospitals, labs, doctors' offices, and other health care organizations are particularly vulnerable to cyberattack, storing huge amounts of sensitive PHI. For this reason, such facilities have been well-known targets of ransomware attacks by bad actors. In these instances, new, unvetted tools can be a particularly big risk for information breaches. Providers eager to meet patients' needs via tele/medicine may adopt new platforms that are not HIPAA compliant, or lack adequate privacy protections. If not properly vetted for security, these tools can put doctor/patient confidentiality at risk and violate applicable privacy and security regulations. Jacobson, A. *The Benefits and Risks of Telehealth Services* (May 1, 2020) http://www.rmmagazine.com/2020/05/01/the-benefits-and-risks-of-telehealth-services/

When tele/medicine is conducted over systems that permit employees to BYOD (bring your own device for work purposes), requiring VPN protection may not be adequate to protect PHI. Health care professionals and providers who work from home or remotely now include clinicians, administrative teams, financial teams, and IT departments. These professionals use numerous devices (tablets, laptops, desk top computers, and cell phones) for patient communication as well as other job requirements, which also increases the risk of data breaches. Healthcare professionals should be hyper-vigilant to ensure no PHI is saved on such devices, and ensure that each device can be scrubbed remotely in the even it is stolen or misplaced. Additionally, the devices, apps, or software on the devices may not belong to the provider directly, making it difficult to ensure that security is properly maintained (e.g., security updates are delayed or go

uninstalled, connections are unsecure, or there is a lack of transparency in public networks that could make health systems susceptible to attacks).

Working from home also presents other security risks, both from the healthcare provider, third-party vendor, and patient perspective. Employees and contractors are also accessing the network remotely while working from home. The more people who access the network, the harder it is to keep track of all users and be alert to a fraudulent or unauthorized users. Risks include connecting to tele/medicine portals and video conferences via public Wi-Fi; conducting them in places where "wandering eyes and ears" can hear the private conversations or view what is on a screen; failure to encrypt sensitive data when being sharing it via email or in the cloud; failing to update all employees' security training; and failing to have adequate remote work policies and procedures as part of a company's data security strategy/protocol.

IV. Insurance Coverage Issues

These issues potentially implicate many kinds of insurance coverage. Lapses in a health care provider's legal and ethical obligations fall under traditional errors and omissions/medical malpractice policies including bodily injury claims. There could also be claims arising from AI programming errors. Beyond that, there are a number of other kinds of insurance may also come into play for the "hidden risks" of tele/medicine. For example, products liability coverage may be implicated in the event that specialized equipment used in tele/medicine fails. Cyber liability insurance would be implicated for HIPAA violations, data and PHI breaches and ransomware attacks resulting from vulnerabilities in tele/health services. Additionally, CGL coverage could be implicated to the extent there is damage to (loss of use) or hardware from such an attack. Kidnap & Ransom provisions of certain policies may also apply in the case of ransomware. Other insurance must also be considered for risk-spreading, including tenders to third-party service providers, contractors/sub-contractors, software/hardware manufacturers and licensees for additional insured coverage under their insurance policies, especially if required by contract.

V. Conclusion

Demand for telehealth services is expected to grow as connected devices proliferate and interoperability between healthcare providers expands. The provider-patient/client relationship will likely evolve as providers use telehealth to develop and maintain patient/client relationships over greater distances and patients/clients grow accustomed to new flexible, personalized care models. As healthcare continues to transform with the use of technology, the potential risks and need for coherent and vigilant risk management will also likely proliferate. Underwriters and claims handlers should be aware of the potential risks, not only from a professional liability/E&O

perspective, but from the privacy, security, cyber and other potential emerging risks posed by the interplay between medicine and technology at a swift pace.