The Proliferation of Telemedicine Brings Significant Privacy and Malpractice Considerations

ATTORNEYS

Rafael P. McLaughlin
260.755.2280
rmclaughlin@reminger.com

Leslie L. Kizziar
260.203.1534
lkizziar@reminger.com

Brian T. Gannon
216.430.2183
bgannon@reminger.com

David Krause
614.232.2495
dkrause@reminger.com

Mark A. MacDonald
513.455.4021
mmacdonald@reminger.com

Matthew A. Taulbee
859.426.3667
mtaulbee@reminger.com

Christine A. Gilliam
502.625.7293
cgilliam@reminger.com

Ronald A. Mingus
317.853.7366
rmingus@reminger.com

PRACTICE AREAS

Health Care

Apr 1, 2020

Telemedicine – the practice of caring for patients remotely using videoconferencing – has increased exponentially during the COVID-19 pandemic. Telemedicine allows health care providers to consult with patients virtually in lieu of face-to-face visits. The benefits of telemedicine in times of pandemic are obvious: it reduces the risk of spreading contagion by obviating potentially harmful patient-provider interactions, not to mention concomitant patient-to-patient interactions. However, telemedicine presents a host of legal issues that health care providers should remain cognizant of as the use of telemedicine expands.

Cybersecurity Considerations

The electronic transmission of protected health information ("PHI") inherent in telemedicine gives rise to unique patient privacy considerations. "Covered entities," those who transmit PHI for which the Department of Health and Human Services has adopted standards, are bound by the Health Insurance Portability and Accountability Act (HIPAA) and the associated HIPAA Security Rule. The Security Rule establishes standards that protect electronically stored or transmitted PHI. To ensure compliance with HIPAA and its Security Rule, medical providers that use telemedicine should implement cybersecurity policies that protect the privacy of patient PHI. These cybersecurity precautions include the following:

(1) Business Associate Agreements

While HIPAA applies only to covered entities, vendors that provide telemedicine applications are typically considered "business associates" under HIPAA. A business associate is an entity that performs functions on behalf of a covered entity and, consequently, requires access to PHI. Therefore, a health care provider must enter into a business associate agreement ("BAA") with its telemedicine vendor that requires the vendor to comply with HIPAA. In developing a BAA to secure the privacy of patient data, the health care provider should define the methods by which the vendor will maintain the

confidentiality of patient data. Additionally, the BAA should identify vendor personnel who will be authorized to access PHI and to what extent. Furthermore, the BAA should specify procedures for regular audits to ensure that PHI is being protected and not subjected to unauthorized access.

(2) Access Control for Remote Connections

The absence of proper safeguards to verify the identities of the health care provider and patient before PHI is exchanged could lead to a privacy breach, including the disclosure of patient data to an unauthorized user. Implementing high-level security mechanisms, such as a multi-factor authentication system, can help control access to PHI and mitigate the risk of inappropriate transmission and dissemination. Multi-factor authentication is a security mechanism that allows a user to log into an account, such as a patient's online portal, only after presenting two or more forms of identity authentication. Such authentication generally includes the following: knowledge, possession, inherence, location, and time.

(3) Encryption

Telemedicine platforms that use end-to-end data encryption provide an extra layer of protection to health care providers and patients by ensuring that only authorized users can read the message or data. Encryption further secures the confidential transmission and storage of PHI by transforming the data into an unreadable format until the data reaches the authorized recipient. Encryption can mitigate the risk of an unauthorized third-party access to or theft of private health information.

Malpractice Considerations

Telemedicine carries unique malpractice concerns. Telemedicine allows a provider to diagnose, treat, and prescribe remotely without a "hands-on" physical examination. Providers rely on a virtual assessment of patient's signs and symptoms, including the information they elicit from the patient. The limits of a telemedicine evaluation; to wit, the lack of face-to-face interaction and crucial palpation, create the potential for misdiagnosis, which can expose a health care provider to liability. The duty of care specific to a telemedicine provider can vary by state. By example, in Indiana and Ohio, a telemedicine provider is subject to the same standard of care as the provider who performs an in-person consult. In contrast, the Kentucky legislature has not clearly defined the standard of care applicable to a telemedicine provider, however, the Kentucky Board of Medical Licensure has suggested that telemedicine providers are held to the same standard of care as traditional health care providers. Accordingly, it is important for providers to know their state's legal standard of care governing telemedicine.

While telemedicine can be a convenient and safe alternative to in-person consultations during a pandemic, it is not without legal risks. As telemedicine further proliferates, health care providers should be mindful of the unique liabilities telemedicine presents, and proactively enact policies and procedures that might effectively mitigate their legal exposure.

Should you have any questions regarding this issue, please contact any member of our Health Care Practice Group.