CARLTON FIELDS

Cybersecurity Considerations for Providers Considering Telehealth During COVID-19's State of Emergency

March 19, 2020

Until recently, telehealth made up a very small percentage of medical claims (less than 1% according to FAIR Health's July 2019 white paper). But with the temporary loosening of telehealth restrictions, everyday providers are now able to immediately start providing telehealth services over widely used non-public facing remote technologies like Skype and FaceTime. Before doing so, however, providers should take some steps to reduce their future litigation risk.

Health care data carries an extraordinarily high value on the black market, typically worth 10 to 40 times more than a credit card number. Transferring such valuable information over unencrypted technologies, as now temporarily permitted, creates a situation ripe for hacking. Hackers can simply insert themselves in the unsecured communication, take the information they desire, and proceed to sell the information to perform various types of health care fraud or identity theft. And while the U.S. Department of Health and Human Services (HHS) has temporarily waived its right to penalties and sanctions for telehealth providers using such unsecured technologies, private plaintiffs could still claim negligence for a provider's use of such unsecured technologies for telehealth purposes. To reduce this risk, providers should:

1. Enable all available encryption and privacy modes on applications used for telehealth communications.
2. Explain the risks of using such technology to potential telehealth patients.
3. Disclose those risks in a privacy policy provided to patients.
4. Ask the patient if he or she agrees to continue with the telehealth service after being informed of the risk.

5. Avoid making statements about the secure nature of telehealth services. Statements like “it’s 100% secure” are a bad idea.

6. Keep a look out for new guidance from the HHS Office for Civil Rights on how covered health care providers can use remote video communication products and offer telehealth to patients responsibly. Make sure you’re complying with any new guidance. If not, plaintiffs will quickly use that guidance to argue that your practices are insufficient.

7. Remember that the ability to use Skype and FaceTime to deliver health services is for a limited time. Once the state of emergency is lifted, providers hoping to continue their foray into telehealth will once again need to bring their practices into conformance with HIPAA’s Security Rule.

8. Make sure you have a HIPAA-compliant breach response plan. While many HIPAA restrictions are temporarily lifted, providers have not been relieved of their data breach notification obligations. Make sure you have a plan in place.

Authored By

Patricia S. Calhoun

Patricia M. Carreiro

Austin Marshall Eason

Related Practices

Health Care
Cybersecurity and Privacy
Technology

Related Industries

Health Care
Technology