CARLTON FIELDS

Health Care Providers Are Under Attack. Are You Ready for 2021?

HEALTH CARE | CYBERSECURITY AND PRIVACY | TECHNOLOGY | CORONAVIRUS | DECEMBER 29, 2020

Patricia S. Calhoun

Patricia M. Carreiro

2020 can rightfully be called the year for remote health care. Fueled by necessity and accompanying loosened regulations, telehealth and the demand for remote patient monitoring boomed. Signs that this progress is here to stay continue to proliferate. Multiple states and the Centers for Medicare & Medicaid Services (CMS) have solidified their commitment to continue telehealth and remote patient monitoring expansion beyond the COVID-19 pandemic. But if 2020 was the year for remote health care, 2021 may be the year remote health care's privacy and cybersecurity needs come to the fore.

In 2020, the threat to patient privacy took a marked shift outward. Insider threats plummeted 20%, while reported hacking incidents increased by 48.6%. The American Medical Association, the Federal Bureau of Investigation, and private entities, like our earlier posts [here, here and here], all issued warnings to health care providers that they were, and are, under attack.

We likely do not know the full extent of hackers' success in 2020 just yet. Protenus' Breach Barometer reported that in 2019, it took an average of 224 days for providers to detect a health care data breach. But some attacks take longer to detect and report than others. For example, ransomware attacks, which rose significantly against health care providers in 2020, often involve complex forensic investigations that lengthen the time between detection and reporting. Add in the exponential demands placed on providers throughout 2020 and there is every reason to believe detection and reporting times may be longer for 2020.

Remote health care necessarily creates additional access points that increase providers' cybersecurity vulnerabilities. And while regulators initially relaxed providers' privacy/cybersecurity obligations, that approach is unlikely to continue beyond the pandemic. Rather, as remote health care settles in to stay, providers and regulators will have to come to terms with what HIPAA compliance will mean in this new era for health care. A task force on telehealth policy, which included the American Telemedicine Association, has already issued a report urging the "full[] reinstate[ment] … of Health Insurance Portability and Accountability Act (HIPAA) patient privacy protections that were suspended at the start of the public health emergency."

Providers relying on OCR's commitment to not fine providers that use technologies without full HIPAA safeguards nor an executed business associate agreement during the COVID-19 pandemic should prepare to transition back to HIPAA's more stringent technology requirements. Providers will soon be tasked with stretching their already limited resources even thinner to ensure the security of patients' information and providers' computer systems. What's more, the Department of Health and Human Services (HHS) is proposing some significant changes to HIPAA's Privacy Rule more broadly. To prepare, providers should create or revisit their plans for transitioning back to at least pre-COVID HIPAA compliance and, as necessary, consult counsel with experience interpreting and applying HIPAA's expansive and opaque regulations to new technologies and business lines. Here are some starting questions to help guide that undertaking:

- **Risk Analysis**. Have you done a risk analysis since you implemented or increased your use of telehealth or remote patient monitoring? Your latest risk analysis must reflect all your business's current means of collecting, accessing, using, storing, and transferring PHI.
- **HIPAA Policies**. Do your policies and procedures address the added risk associated with the increase in telehealth and remote patient monitoring? Do you need to create new policies to address telehealth and remote patient monitoring?
- **Business Associate Agreements**. Have you taken on any new vendors? Ensure that you have current business associate agreements in place with all business associates and, if necessary, confirm that the underlying agreements include the increased use of telehealth and remote patient monitoring.
- **Paper Trail**. Have you documented your efforts? Your documentation must justify the actions you have, and have not, taken with regard to privacy.
- **Employees**.
    - Have your employees been trained on any policy or procedural revisions? Are those employees following them? Are you auditing them to ensure this is true?

    - Have you informed your employees about the new risks and heavy targeting of health care by hackers?
- **Incident Response Plan.** Do you have an incident response plan in place to respond to any potential PHI compromise? Is your incident response team familiar with the plan, and have they practiced using it?

We will continue monitoring HHS' proposed privacy rule revisions, and we remain available to help providers as they navigate this evolving area.