CARLTON FIELDS

Six Steps to Protect Against Increased Telehealth Cybersecurity Dangers

CYBERSECURITY AND PRIVACY | CORONAVIRUS | HEALTH CARE | TECHNOLOGY | APRIL 21, 2020

Patricia S. Calhoun

Patricia M. Carreiro

Last week, the American Medical Association (AMA) and the American Hospital Association (AHA), recognizing the increased cybersecurity threats facing health care providers, issued joint guidance for physicians working from home during the COVID-19 pandemic. Today, the FBI issued a cybersecurity alert warning of COVID-19 phishing attacks against U.S. health care providers. These alerts serve as helpful reminders of the cybersecurity dangers facing health care, and especially telehealth, during the COVID-19 pandemic. With that, here's a checklist of things health care providers can do to better secure their systems.

1. **Protect Home Computers, Smart Phones, Tablets, and Home Networks**

   A network is only as secure as its weakest link, so telehealth physicians should make sure their personal computers, smart phones, tablets, and home networks comply with the same security standards as their medical practice. That means that physicians still shouldn't share their login information with others and should have strong password policies, run only authorized software applications, ensure system and software updates are timely applied (including anti-virus software), use up-to-date browsers, and disable Microsoft Office macros. As far as home networks, you'll want firewalls installed, enabled, and properly configured; strong passwords (not just the password that came preinstalled); and proper Wi-Fi encryption. From the medical practice's perspective, the same requirements apply, but they should also make sure every provider has a unique user account name and password and not give people broader system access rights than they need.

2. **Fortify Medical Device Cybersecurity**

   Along the same lines, remember to fortify your medical device cybersecurity — they too are vulnerable to hacking. Make sure you have a formal process in place to coordinate and ensure their proper cybersecurity maintenance. This includes keeping an inventory of devices, their connectivity, operating systems, firmware, and software applications. As with everything else, make sure they are timely patched, use network segmentation, proper access controls, strong passwords, and encryption where available. Delete unnecessary patient information that may be stored on these devices, and consider disconnecting medical devices that cannot be patched from your network.

3. **Beware Increased Phishing Emails and Ransomware, and Prepare for an Attack**

   Hackers are increasingly targeting health care and have increased their phishing attempts. Consider sending out the FBI alert linked above and add a caution banner to emails sent from outside your organization. Be particularly wary of attempts to change payment instructions or requests for sensitive information. To prepare for the increased risk of ransomware, create secure backups, whose access is highly restricted and monitored. The AMA and AHA guidance recommends considering the 3-2-1 rule: three offline segmented backup data copies, in two different media types, and one cloud-based backup.

4. **Use a Virtual Private Network (VPN) and/or Cloud-Based Service**

   When using VPN or cloud-based technologies, use multifactor authentication and lockout parameters, limit remote access to

only necessary databases, ensure security patches are updated, require regular password changes, and consider using advanced threat protection (ATP) to detect malware.

5. **Opt for More Secure Telehealth Service Providers and Comply With Industry Cybersecurity Guidance**

   As we've previously warned, lesser cybersecurity measures, even if temporarily not subject to fines from the OCR, may still mean expensive litigation later. When considering your telehealth service providers, be sure to include the longer-term litigation costs in your calculus. Along the same lines, be sure you are aware of and complying with industry cybersecurity guidance. Plaintiffs will surely use any violation to justify a negligence claim in case of a breach.

6. **Plan for a Data Security Incident**

   Know what to do in case the worst occurs. You should have, and practice, a data incident response plan that includes the number of knowledgeable counsel. Getting counsel involved immediately is essential for preserving privilege and best positioning yourself for the inevitable claims. Experienced counsel can work with you to notify your bank quickly (if any funds were mistakenly transferred, they may be recovered if reported within 72 hours), start investigating, and notify others if appropriate in any given case (law enforcement, regulators, etc.).