Codify
BY AAPC

Health Information Compliance Alert

Know the Cyber Risks Associated With RPM

Understand what constitutes an 'IoT device.'

If your practice ramped up its remote patient monitoring (RPM) usage during the pandemic, you're not alone. But, as helpful as RPM devices are at monitoring your patients' health in real-time, devices can pose a security risk to your network and must be managed appropriately.

"RPM relies on devices that are broadly referred to as the internet of things (IoTs). Most of these devices are not designed with security in mind. As a result, they are susceptible to vulnerabilities and malware exploitation," says **Funso Richard, CISA, CISM, CDPSE, CCSFP**, information security officer, Ensemble Health Partners, in Cincinnati, Ohio.

Reminder: IoT devices constitute almost any device that can connect wirelessly to a network and the internet. These devices include smart speakers, smartphones, smartwatches, medical sensors, and fitness trackers.

IoT devices are so commonplace that users may not realize the internal components can just as easily be compromised. "RPM devices have chips that execute as a computer. The chips that are associated with RPMs have the same vulnerability as CPU, GPU, and TPU," says **Eddie Hearns, MA, CPMA, CPC**, Approved Instructor, of OLDME CPC LLC.

As a result, RPM and telehealth devices carry several risks for healthcare organizations:

1. Encryption failures could open the door for more data breaches. Improper transport layer encryption between the device and your healthcare organization system can put data at risk.

2. Misconfigured devices can heighten chances of a cyberattack. An improperly configured RPM device could be used to launch an attack against any connected healthcare system.

3. Malfunctioning devices can be a danger to patients' health. If an RPM device malfunctions, there's a chance the device could be altered, which may result in the device sending a wrong reading to the physician. This incorrect reading could cause the physician to misdiagnose their patient.

4. Medical devices are not immune to malware issues. RPM and telehealth devices are prone to malware and traditional anti-malware protections may not be a reliable solution, which could put patient safety at risk.

5. RPM regulations vary by state. Federal rules about where and how RPM is used can be very different from an individual state's laws. It's essential that your practice checks state requirements related to hardware, privacy, and cybersecurity as well as the coverage restrictions and nuances among public and private payers.

Tip: If your organization is looking to employ RPM devices, prioritizing security should be the main concern. "The equipment that's used for telehealth must be compliant and state of the art. The same problems with technology and data security are escalated because now you are introducing the IoTs into the environment," Hearns says.