Codify
BY AAPC

Health Information Compliance Alert

Reader Questions: Establish Upfront Medical Device Management Responsibility

Question: Our practice is exploring providing remote patient monitoring (RPM) devices, such as continuous glucose monitors (CGMs), to our patients, so physicians can easily track the patients' levels between visits. Who is responsible for the security of the devices?

AAPC Forum Participant

Answer: Ultimately, the healthcare provider has final responsibility for their environment. Whether you're implementing RPM devices, offering telehealth services, or allowing employees to use a VPN to work remotely, the healthcare provider needs to take the necessary steps to ensure the security of any devices connecting to their network.

The provider's goal is to ensure all compliance standards are met, address all legal and regulatory issues, and thoroughly document all technological and data security policies and procedures.

Your organization should make sure a robust data governance paradigm exists in the information security protocols for telehealth and RPM devices. NIST and ISO standards are great for establishing policies and procedures, but they aren't mandated in the healthcare space. As a result, telehealth and RPM devices can be compromised, if not properly secured.

CPT® 2023 American Medical Association. All rights reserved.

Your organization needs to be prepared if those devices are compromised. "The most important policy that every organization requires is a data breach policy. That is when to notify the appropriate authority when a data breach has occurred," says **Eddie Hearns, MA, CPMA, CPC**, Approved Instructor, of OLDME CPC LLC.

CPT® 2023 American Medical Association. All rights reserved.