Making Health Data More Mobile Means Making It More Vulnerable

Having patients actively involved in their own healthcare is positive, whatever way you look at it. Often, that deeper involveme means increased patient access to and more control over their protected health information (PHI). Certainly the Centers for Medicare & Medicaid Services (CMS) is a proponent of trusting individuals with their own health data, as evidenced by CMS Administrator Seema Verma's and Trump senior adviser Jared Kushner's comments to that effect at the Healthcare Informati and Management Systems Society's annual meeting in Las Vegas last month.

Recently, with the official launch of the latest version of its Health app, Apple has also joined the movement to bring patient he data to patients' fingertips … via their iPhones. And while on the surface this appears to be wholly beneficial, experts warn tha easier patient access can also mean easier bad actor access as well.

More than three dozen health systems sign on to iPhon Health app

Thirty-nine health systems are already on board with Apple's Health app. Those patients choosing to transfer electronic health record (EHR) data onto their iPhones should be aware of the risks and remain vigilant in order to minimize those risks, howev

Pennsylvania-based Geisinger was one of the first health systems to partner with Apple and allow patients to move their EHR to their phones. John Kravitz is the company's chief information officer. "The patient who downloads this information absolutel must secure their device to protect their own records," he told Modern Healthcare.

Janet Campbell is vice president of patient engagement for Epic Systems Corp. "Patients have requirements for strong passw and we can make them more secure by using newer features like Touch ID on the patient's mobile phone," she said.

This doesn't mean that the patient is the only one responsible for increased security in this age of increased access. EHR ven and health systems must operate using safety measures well before patients log into their provider portals and move data to t phones. Once the PHI is on the patient's phone, however, the individual might share it with apps that have not been designed the same kind of serious safeguards that go into protecting the patient portal.

Patients should understand the risks of transferring the

data

That's not to suggest that patients should be in the dark when it comes to their EHRs. "We enthusiastically support the consumer's right to access a copy of their data and to decide how it should be used," Don Bisbee, senior vice president of clinical and business strategy for Cerner, told Modern Healthcare. "But continued education is needed around the potential risks associated with choosing to expose sensitive health data to broader groups than the covered entities where HIPAA protections apply."

John Riggi is senior adviser for cybersecurity and risk at the American Hospital Association (AHA). Riggi made this comment to Modern Healthcare regarding the need for security standards in the world of mobile healthcare data: "The issue surrounding apps in particular is that ONC (the Office of the National Coordinator for Health Information Technology) has not promulgated specific security standards."

Riggi drew a parallel between banking apps and healthcare apps and the necessity for safeguards around both. He noted that banking apps are operated by the specific financial institutions consumers are interfacing with; the same does not hold true for health apps. Often the health system has nothing to do with the health app a patient is using to access health data.

Cyber-expert advises collaboration between providers and the government

Riggi, a veteran of the FBI, suggested: "There should be a measured approach in collaboration with HHS and the ONC and the providers to ensure whatever platform a patient uses to access the EHR has been fully vetted and complies with all HIPAA privacy and security rules."