How to keep patient information secure in mHealth apps

JAN 13, 2020

Tanya Albert Henry
Contributing News Writer

Mobile health (mHealth) apps must make sure the data they are collecting is secure from hackers, malware and other external threats and they must maintain the integrity, availability, confidentiality and resilience of the data.

Those elements are part of guidelines developed by Xcertia, an independent nonprofit that the AMA and other major health and technology organizations founded. When developers comply with the Xcertia mHealth app guidelines—which include sections that address privacy, content, security, design and operability—it helps provide a level of assurance that an mHealth app delivers value to patients, physicians and other users. More than 25 organizations have adopted the Xcertia guidelines as part of the product development process.

Xcertia recently called on its federal partners to adopt an initial app privacy framework utilizing industry guidelines.

“We believe there is an opportunity to leverage the Xcertia guidelines given forthcoming federal requirements around certified health IT design, development, and the increased availability of patient health information through application programming interfaces (APIs),” said Michael Hodgkins, MD, chair of Xcertia’s board of directors and AMA chief medical information officer.

“These guidelines can act as one set of criteria app developers should assert conformance to increasing transparency around an app’s data privacy and other practices,” he said.

In addition to being up front and clear with users about how they are securing data the app collects, app developers need to have security procedures that comply with the best practices and applicable rules and regulations that govern areas where the app is sold or used.

“It’s one thing to say you have a privacy policy and that you are not going to share the informationwith third parties, but if your security isn’t good, somebody is going to wind up getting the information,”Dr. Hodgkins said.

The guidelines call for putting an easy-to-understand, written description of the security features in a section of the app—a tab, button or equivalent—or to provide the information through an active link. The information should include, among other things, how the app safeguards personal information, how unique identifiers are linked to the correct user and which authentication methods are used.

8 other areas key to app security

In addition to operations, the guidelines address eight other areas surrounding security that app developers need to consider when they create mHealth apps that collect, store or transmit personal information.

Vulnerability management. When an app is released and when any upgrades are made, it must be free from malicious code or software such as malware, including viruses, worms, trojan horses, spyware, adware, rootkits, backdoors, keystroke loggers. This standard also applies to any advertisements displayed or supported through the app.

Systems and communication protection. Encryption must be used when mHealth app usernames and passwords, among other information, are collected, stored and transmitted.

Compliance. If HIPAA applies to the app or any of its users, the mHealth app must maintain and protect the confidentiality, integrity and availability of individually identifiable health information in a way that meets the federal regulation’s standards.

Access control and authentication. The app must offer at least one industry-accepted method for guarding against identity theft and remote access or privileged access should require two-factor authentication to reduce unauthorized access.

Asset management. Information assets should be classified by their value to the organizations and outside regulation; for example public, internal confidential, sensitive. Organizations should have a process to track the information and physical assets.

Physical and environmental security. The app publisher should keep a record of how it maintains security and it should have a physical security program that includes security and environmental controls for the building or data center that contains information assets and system.

Incident response. Apps must create and maintain an incident response system in case there is a security breach. If there is a breach, the organization should notify those who were impacted.

Disaster recovery and business continuity. Apps need to have a documented plan for what happens if the app, data or access is unavailable. Tests from the data back-up should happen regularly.

The AMA involvement in Xcertia stems from a 2016 policy recommended in an AMA Council on Medical Service report. Learn more about AMA efforts focused on validating digital health innovations.