Privacy, security guidelines aim to bolster use of mHealth

OCT 25, 2018

Andis Robeznieks
Senior News Writer

Privacy and security guidelines aimed at securing the protected health information and personal, identifiable data of mobile health app users have been released for public comment by Xcertia, a nonprofit founded by the AMA and other major health and technology organizations.

"As the industry continues to deal with breaches of personal data and information, we made a decision to accelerate the release of this part of the guidelines in an attempt to address these issues," said Chuck Parker, Xcertia's managing director.

The final version of privacy and security guidelines, along with updated content, operability and usability guidelines are scheduled to be released for public comment at the Health Information Management and Systems Society (HIMSS) annual conference in February 2019.

HIMSS is one of the AMA's partners in the Xcertia effort, along with the American Heart Association and digital health nonprofit DHX Group. The updated privacy and security guidelines are now open for comment until early December at Xcertia's website.

Each of the Xcertia board members has committed to the adoption and integration of the guidelines and they encourage all stakeholder groups to adopt the guidelines to ensure safe and effective mHealth solutions. If you would like to participate in the process of updating the guidelines, contact Xcertia.

The Xcertia guidelines cover six privacy areas and nine security concerns.

For privacy, the guidelines call for:

- Disclosing to the app user how their data is collected, used and retained, and who has access to it.
- Disclosing how long this data is retained and the defined business purpose for doing so.
- Informing the user if the app accesses information from address books, credit cards,

- location services, photos or social media platforms—and requiring users' consent to do so.
- Disclosing whether users' protected health information is handled by a third-party business associate.
- Requiring that measures to be taken to protect child app users under 13.
- Requiring that, if the app is used to process information about individuals selling goods or services with citizens of the European Union, it must comply with the European Union General Data Protection Regulation.

Security measures called for in the guidelines include requiring that:

- Administrative, physical and technical safeguards be used to protect users' information.
- Any advertising displayed on the app be free of malicious code or software.
- Encryption be used if apps collect or transmit users' user names and passwords.
- Apps or third-party business associates comply with data privacy and security provisions of the Health Insurance Portability and Accountability Act (HIPAA).
- Apps offer industry-accepted measures for guarding against identity theft.
- If personal information is collected, stored or transmitted, app must maintain methodology for documenting the data.
- App developer maintain a physical security program.
- App developer must create and maintain an incident-report system.
- App developer must create and maintain a disaster-recovery and business-continuity plan.

There are more than 318,000 health-related mobile applications available, according to a report released by the IQVIA Institute for Human Data Science.

The AMA's involvement with the Xcertia effort is an outgrowth of policy adopted in 2016 by the AMA House of Delegates on the integration of mHealth apps and devices into medical practice.

Learn more about how the AMA's digital health leadership is ensuring the physician perspective is represented in the design, implementation and evaluation of new technologies.

One tangible product of that leadership effort is the AMA's Digital Health Implementation Playbook. The Playbook—created with the help of more than 80 physicians, care team members, health care administrators, patients and digital health thought leaders—packages the key steps, best practices and resources to accelerate the adoption of safe, effective, and trusted digital health innovations and helps physicians extend care beyond the exam room.