mHealth data security in spotlight at 2016 Interim Meeting

NOV 9, 2016

Kevin B. O'Reilly
News Editor

Delegates to the 2016 AMA Interim Meeting in Orlando, Fla., this week will consider policy recommendations contained in a broad-ranging report of the AMA's Council on Medical Service that aim to address factors impeding acceptance and widespread use of mobile health technologies. Among the many issues addressed is how mobile applications and devices may expose patient users' personal data.

The council's report notes that the Health Insurance Portability and Accountability Act (HIPAA) generally does not cover mobile health applications, also called mHealth apps. That is true even if the apps "handle or store an individual's health information," the report says. "As such, mHealth apps are not required to protect the privacy and security of an individual's health information in the same way that a physician must because mHealth apps are not directly subject to HIPAA regulations."

More than 165,000 mHealth apps are available to patients, according to a September 2015 report from the IMS Institute for Healthcare Informatics.

"Patient privacy and data security need to be a priority in the digital health space, as mobile apps and devices can be subject to privacy and data breaches," the AMA council's report says. The AMA House of Delegates will consider a series of 11 recommendations put forward by the Council on Medical Service in its report. Among these are ones that specifically apply to concerns about mHealth data, which state that the Association should:

- Support requiring mHealth apps and associated devices, trackers and sensors to abide by applicable laws addressing the privacy and security of patients' information
- Encourage the mobile app industry and other relevant stake holders to conduct industrywide outreach and provide necessary educational materials to patients to promote increased awareness of the varying levels of privacy and security of their information and data afforded by mHealth apps, and how their information and data can potentially be collected and used
- Encourage the mHealth app community to work with the AMA, national medical specialty

societies and other interested physician groups to develop app transparency principles, including the provision of a standard privacy notice to patients if apps collect, store or transmit protected health information
- Encourage physicians to alert patients to the potential privacy and security risks of any mHealth apps that he or she prescribes or recommends, and document the patients' understanding of such risks

Other policy proposals offered in the council's report aim to ensure that mHealth apps have a clinical evidence base to support their use, that delivery of any services via mHealth apps is consistent with state scope of practice laws, and that these apps abide by licensure and medical practice laws in the state where the patient receives services facilitated by such technology.

Health data concerns span globe

The policy proposal at the 2016 AMA Interim Meeting comes on the heels of guidelines adopted by the World Medical Association (WMA) at an October meeting in Taipei, Taiwan.

A WMA statement on cyber attacks on health infrastructure notes that "security procedures and strategies in the health care sector have generally not kept pace with the volume and magnitude of cyber attacks. If not adequately protected, hospital information systems, practice management systems or control systems for medical devices can become gateways for cybercriminals. Radiology imaging software, videoconferencing systems, surveillance cameras, mobile devices, printers, routers and digital video systems used for online health monitoring and remote procedures are just some of the many IT structures at risk of being compromised."

The WMA is the international organization representing physicians from more than 100 national medical associations, including the AMA.

In its statement, the WMA urges national medical associations to raise awareness about cyber attacks and help develop an effective health information technology strategy to prevent them. The policy statement also "calls upon physicians, as guardians of patient safety and data confidentiality, to remain aware of the unique challenge cyber attacks could pose to their ability to practice their profession and to take all necessary measures that have been shown to safeguard patient data, patient safety and other vital information."

The WMA's policy "acknowledges that physicians and healthcare providers may not always have access to the resources (including financial), infrastructure and expertise required to establish fail-safe defense systems and stresses the need for the appropriate public as well as private bodies to support them in overcoming these limitations."

Meanwhile, the WMA adopted ethical guidelines for doctors involved in collecting and using identifiable health data and biological material in health databases and biobanks. These guidelines, dubbed the Declaration of Taipei, “set out the rights to autonomy, privacy and confidentiality that the WMA believes individuals should be entitled to in order to exercise control over the secondary use of their personal data and biological material, also beyond specific use in research,” according to a statement.

“These guidelines are based on the perspective of individuals and the need to increase transparency,” Dr. Jon Snaedal, chair of the WMA workgroup that produced the guidelines, said in the statement. “People quite rightly want to know what happens to their data. We believe that informed consent, although not perfect, is the strongest instrument for protecting personal autonomy, and with it self-determination and dignity. However, we recognize that when use of data is authorized by a national law adopted through a democratic process in respect of human rights, other procedures could be adopted when strict rules on data protection are implemented.”