Managing Health Information in Mobile Devices

Save to myBoK

By Lydia Washington, MS, RHIA, CPHIMS

While the jury is still out on whether mobile devices will eventually replace laptops and PCs, many observers are predicting that their use will continue to explode in the next few years. There are currently at least 10,000 health-related apps that could be downloaded to a mobile electronic device like the iPad, iPhone, and Android-smart phones and tablet computers that are increasingly being used by consumers and healthcare providers to manage various aspects of health maintenance and healthcare.

Combined with government initiatives like the meaningful use EHR incentive program, designed to increase consumer engagement in personal healthcare, mobile health can only be expected to accelerate in the coming years. Mobile health technology can be used by consumers to download health information from provider portals, or by healthcare providers to collect, record, and report health information either manually or via interfaces with biomedical devices.

Because of this growing trend, HIM professionals should review the latest mobile health regulations and best practices, and develop internal policies aimed at protecting the integrity and privacy of patient records.

Five Concerned Agencies

The growing use of mobile devices for healthcare management has not escaped the attention of regulators. In March 2012, the Office of the National Coordinator for Health IT (ONC) hosted a roundtable discussion and put out a call for public comment on the topic. At least five federal agencies-the Federal Communications Commission, the Food and Drug Administration, the Federal Trade Commission, the Office for Civil Rights, and the National Institute of Standards and Technology-were present to discuss their regulatory and non-regulatory roles relative to mobile health technology. While each agency has a different approach to monitoring healthcare mobile device use, each reported a specific emphasis on privacy and security.

The **Federal Communications Commission's (FCC)** scope includes authorization of carriers whose networks are used by mobile devices to access, transmit or store information-including health information. The FCC also authorizes a variety of radio frequency medical devices, such as implanted medical devices and patient monitoring devices. It also establishes the technical rules used by Wi-Fi or other similar networks for short transmissions.

The **Food and Drug Administration's (FDA)** aim is to promote and protect public health by regulating any technology-including phones and other mobile devices-that is used for treating disease in patients. The FDA looks at the effectiveness of a medical device for healthcare treatment. The agency also evaluates the risks that the devices could bring to patients, including those related to security and privacy.

The FDA has published a report titled "Draft Guidance for Industry and Food and Drug Administration Staff on the Regulation of Mobile Medical Applications" that seeks to regulate three types of mobile devices:

- Apps that connect to a medical device for the purpose of controlling the device or displaying, storing, analyzing, or transmitting patient-specific medical device data (e.g., an app that controls the delivery of insulin by transmitting signals to the pump)
- Apps that, when attached to the mobile platform or smartphone, transform it into a medical device (e.g., an app that allows doctors to monitor brain activity by attaching EEG sensors to a mobile device)
- Apps that utilize formulae or processing algorithms to transform the input of patient-specific information into a patient-specific result, diagnosis, or treatment recommendation that assists in clinical decision making (e.g., an app that provides a questionnaire for collecting patient-specific lab results and computes a prognosis of a particular condition)

The **Federal Trade Commission (FTC)** attempts to combat unfair or deceptive practices related to healthcare mobile device applications. This could include any false or misleading claims or omissions of material facts in relation to a mobile device or app. The FTC has already been involved with two recent cases of enforcement concerning healthcare mobile devices.

The first involved an app that claimed to treat acne with a light emitted from the mobile device.[1] The second case involved the developer of a peer-to-peer file-sharing app that caused consumers to unwittingly share personal information on their mobile device.[2] Making misrepresentations about mobile health technology, including privacy policies or settings, could bring potential FTC enforcement activities.

The **Office for Civil Rights (OCR)** is charged with enforcing HIPAA regulations, which apply the same privacy and security protections that would be used with enterprise equipment like computers.[3] Since mobile devices are especially susceptible to being lost or stolen, OCR recommends taking all reasonable precautions to secure them-including encryption-which, though not required by HIPAA, is recommended if it's reasonably simple to do so. OCR also recommends other data security strategies, such as user authentication and role-based access.

The **National Institute of Standards and Technology (NIST),** a non-regulatory federal agency within the U.S. Department of Commerce, is concerned with measurement, standards, and testing. The institute produces a variety of publications related to computer security, including some with mobile security guidance.

Mobile Devices and Health Record Management

While much has been written stressing how extremely important security and privacy issues are in the use of mobile health technology, a question much less explored is how health information that is captured on mobile devices relates to the management of the health record.

It is widely accepted that any health information captured or stored by clinicians using either a personal mobile device or one provided by the healthcare organization becomes part of the HIPAA-designated record set if that information is used to make decisions about a patient. The same is true when health information that is collected or captured by an individual or patient is transmitted or communicated to a provider who uses it in the provision of care.

Most likely, this information is also part of an organization's legal health record and is subject to requests for disclosures, subpoenas, and e-discovery. Conceivably, the health information generated by a mobile device could also be useful for many non-clinical applications that use medical records-such as audits, health research, and information reporting. The problem for HIM professionals is how to track and preserve these records when they reside on mobile devices.

In addition to privacy and security policies, healthcare organizations would need to have policies that outline the conditions and acceptable uses of mobile devices that capture and store clinical information since that information may become part of a health record.

Policies would need to address how mobile devices are handled when the information they contain may become involved in potential litigation (legal holds) as well as methods for monitoring and tracking mobile devices that contain health information that is part of the organization's legal health record. The use of mobile devices that access health information and health records, whether personally owned or provided by the healthcare organization, need to be addressed in security risk assessments, litigation response plans, and human resources policies.

The use of mobile devices brings new regulatory, legal, and technological considerations for the management of health records. They present yet another opportunity for health information professionals to apply specialized skills in order to tackle this new challenge.

Notes

1. Dolan, Brian and Chris Gullo. "US regulators remove two acne medical apps." *MobiHealthNews*. Sept. 9, 2011. http://mobihealthnews.com/13123/us-regulators-remove-two-acne-medical-apps.

2. "Peer-to-Peer File Sharing: A Guide for Business." Federal Trade Commission's Bureau of Consumer Protection Business Center, January 2010. http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.
3. Rouse, Margaret. "HIPAA (Health Insurance Portability and Accountability Act)." Updated May 2010. http://searchdatamanagement.techtarget.com/definition/HIPAA.

References

"Mobile Devices Roundtable: Safeguarding Health Information." Office of the National Coordinator for Health IT. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__mobile_devices_roundtable/3815.

Pence, Canon and Podolny, Meghan. "Is There an App for That? Protecting Corporate Records in a Mobile Communications World." ARMA International, 2011. http://content.arma.org/IMM/January-February2011/IMM0111isthereanappforthat.aspx.

Lydia Washington, MS, RHIA, CPHIMS, (lydia.washington@ahima.org) is a director of practice management at AHIMA.

Article citation:
Washington, Lydia. "Managing Health Information in Mobile Devices" *Journal of AHIMA* 83, no.7 (July 2012): 58-60.