Best Practices in mHealth for Consumer Engagement

By Leah A. Grebner, PhD, RHIA, CCS, FAHIMA, and Raymound Mikaelian, RHIA

Health information management (HIM) professionals are familiar with mobile health (mHealth) technologies from a provider perspective, but technology has provided the ability for healthcare consumers to also utilize mHealth to become more actively engaged in managing their personal healthcare.

The HIM professional has a growing opportunity to serve in the role of educator with healthcare consumers. HIM professionals have knowledge about a variety of HIM principles that impact healthcare consumers and sharing this knowledge can facilitate responsible consumer decisions.

Educating Consumers on mHealth Products

Healthcare consumers are using a variety of wearable devices to collect healthcare data. These devices monitor exercise, asthma, blood sugar, vital signs, and may even be able to detect if the wearer has a fall. Wearable devices can alert the healthcare consumer if there are abnormal conditions, and some even communicate with the healthcare provider. The range of wearable devices include those that are as simple as a “smart watch” to more complex devices that involve EKG leads, smart contact lenses, and other health monitors.

Cell phones and other mobile devices provide consumers with limitless options for managing many aspects of healthcare, including monitoring blood pressure, glucose levels, and exercise. It is important for the healthcare consumer to review documentation regarding the privacy of information that is collected by the application. Frequently, these applications do not provide the consumer with a notice of privacy practices when health information is collected and transmitted. The healthcare consumer needs to be educated about the advisability of using applications with documented privacy practices and knowing who has access to their data.

In addition to wearable devices, there are diverse electronic options available to healthcare consumers for creating and maintaining personal health records (PHR). These range from use of web-based applications to PHR templates that may be maintained on a portable flash drive or even PHRs on mobile devices. HIM professionals again play the role of educating healthcare consumers, such as providing information regarding the importance of compiling and maintaining a PHR, along with what type of information to include and how to obtain the information. HIM professionals should ensure that healthcare consumers are informed about the importance of HIPAA compliance with web-based and mobile device PHR applications.

Privacy information should be available in conjunction with the portal. This is a good example of how the HIM professional can serve in the role of patient advocate to assist patients in initial navigation of the portal system for organizations that have those types of positions.

Patient portals are another technology that provides healthcare consumers with greater access to their health information directly from their providers, including the ability to communicate with the provider through the portal. However, a significant knowledge gap exists for healthcare consumers accessing their health information through a patient portal. Aside from the potential need for training to use the portal, which most providers are not supplying, healthcare consumers may also face issues related to low health literacy. A need exists for healthcare professionals, including HIM professionals, to develop health literacy training programs to give the healthcare consumer the ability to understand basic health information, along with information about how to navigate the patient portal and where to find additional reputable information about their health conditions.

Health literacy training could be developed as a community education initiative. Many healthcare systems have consumer health classes and this is a great topic for such a course. Development of a brochure that could be provided to patients would also be beneficial.

Maintaining Patient Privacy in mHealth

As mobile health (mHealth) applications began to appear with the rise of smartphone adoption and other technological advances, healthcare consumers had not deemed privacy and security an important issue. Early applications were very limited in their capability, and utilized a minimal amount of an individual's personal information. Early applications focused mostly on weight tracking, activity tracking, and health/wellness advice. While the apps utilized various elements of health information ranging from age, weight, sex, prescriptions (reminder apps), and even stage of pregnancy, the elements were used in a closed ecosystem and did not interact with covered entities, meaning that under HIPAA the collected elements are not defined as protected health information (PHI).

Fast-forward to today's mobile marketplace, where the Google Play Store and Apple's App Store boast more than 100,000 mHealth applications for consumers to download, according to one market report.[1] While many basic applications still exist, there is continued growth and development of advanced applications, which, in addition to basic functions, can utilize wearable devices to track heart rate, blood-glucose levels, location, and many other body functions. Not only do these advanced applications collect more personal and health data, but they have the ability to interface into other applications both in and out of the mobile-sphere. As these applications begin to interface and interact with covered entities, elements of health information become PHI, and the questions of privacy and security need to be addressed. Whether or not an app is integrated into a portal is something that varies from app to app.

The Apple Health application has the ability to collect data from several applications on an individual's phone, creating a repository of an individual's activity, health, and well-being. Applications created in the iOS marketplace for Apple Health are built within the bounds of HealthKit. According to Apple, HealthKit allows apps that provide health and fitness services to share their data with the new Apple Health app and with each other. Within HealthKit's reference material, it is evident that Apple has taken steps to promote the privacy and security of an individual's health data. For example, HealthKit data are only kept locally on the user's device, according to Apple's website.

Additionally, HealthKit is kept encrypted while the phone is locked. And a privacy policy must be provided for apps that use HealthKit's application program interface. Apple directs users to the Office of the National Coordinator for Health IT's PHR model for non-HIPAA covered apps. Apple then goes on to list HIPAA as the model for HIPAA-covered apps. While it is not required to use HealthKit to develop mHealth applications in the iOS world, those apps that wish to interface with Apple Health's repository are required to do so.

mHealth Security Needs Some Work

So how secure is the mHealth world? According to a security analysis conducted by Symantec Corporation, there are several vulnerabilities to device security, data storage, and data transmission in many mHealth apps and devices.[2] These vulnerabilities range from user location tracking, securing username and password credentials, unique identification used in third party analytics, and website security. Related to healthcare, medical identity theft would be the greatest concern due to these vulnerabilities. Knowing an individual's location and stolen login credentials could provide the demographic information necessary to steal an individual's identity.

With clear vulnerabilities present that can compromise an individual's PHI, it is evident that privacy and security of mobile devices will be an ever-growing concern for HIM professionals. As consumers become more engaged, the data that are collected from mobile and wearable devices will be crucial to the creation of a longitudinal personal health record. However, as these applications become more capable, the privacy and security of an individual's health information must be safeguarded at the highest level possible.

With the advent of patient portals, PHRs, and mHealth, healthcare professionals will be flooded with a wealth of data. HIM professionals have a duty to guarantee that data that are used and collected have purpose, integrity, and longevity. The need for information governance and data stewardship in our electronic world is growing, and HIM professionals must ensure they are paving the path for organizations and healthcare consumers.

Notes

1. research2guidance. “mHealth App Developer Economics 2014.” May 6, 2014. http://research2guidance.com/r2g/research2guidance-mHealth-App-Developer-Economics-2014.pdf.
2. Symantec. “Security Response: How Safe is Your Quantified Self?” August 11, 2014. www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.

Leah Grebner (lgrebner@midstate.edu) is the director of health information technology at Midstate College in Peoria, IL. Raymound Mikaelian (rmikaelian@svmh.com) is an HIM data analyst at Salinas Valley Memorial Healthcare System in Salinas, CA.

Article citation:
Grebner, Leah A.; Mikaelian, Raymound. "Best Practices in mHealth for Consumer Engagement" *Journal of AHIMA* 86, no.9 (September 2015): 42-44.