Use of Mobile Health Technology for Communication in Healthcare

By Cris V. Ewell, Ph.D., CISSP, CISM, UW Medicine

The benefits of digital and mobile health are numerous and include improved point-of-care coordination, enhanced physician efficiency, increased healthcare quality, and increased information access and real-time communication.[1] Despite these benefits, the use of digital and mobile technology in healthcare is lagging behind other industries. In addition, the adoption and use of mobile technology for unified communication are not universally implemented. Some of the barriers to successful adoption of a mobile health strategy include the complexity of healthcare (including interfacing with the healthcare record), federal and state regulations, lack of infrastructure to support devices, and many security- and privacy-related issues.[2]

Physicians and nurses understand the importance of effective communication and often use their personally owned devices to aid in the coordination of patient care between healthcare teams. In one study of academic medical centers (AMCs), 85 percent of physicians said they own a smartphone and use the device in the healthcare setting,[3] and McBride and LeVasseur found that 94 percent of the nursing staff they surveyed use their personal phone at work—mostly to send emails and text messages to other healthcare members.[4] In a study of pediatric hospitalists, 91 percent of participants used a smartphone, 60 percent utilized text messages while at work, and 53 percent received work-related text messages when not working.[5]

While members of the healthcare workforce are using their smartphones for patient care related communications, according to an article in the *Journal of Medical Systems,* 59 percent of AMCs still provide one-way text pagers for clinical communications and only 35 percent provide a cellular or other mobile device.[6] In addition to the accepted use of pagers, another reason for the slow adoption of mobile devices used for patient care communication is the lack of clarity and guidance from the HIPAA regulation and internal hospital policies on what is required to protect the information from unauthorized access, use, or disclosure. The same study of AMCs found that 49 percent of the respondents believed that HIPAA prohibits text messages on personal mobile devices.[7]

To help guide the healthcare organization with the adoption of an effective mobile communication strategy that is compliant with federal laws and regulations, boards and senior leaders should consider the following initiatives.

Key Board Takeaways

Many healthcare organizations are not realizing the benefits from a unified communication strategy. Boards should ask the leadership team how the mobile communication plan is part of the larger digital and mobile health strategy. This includes asking:

- Does the organization have a mature communication strategy?
- How well is the implementation of mobile health technology supporting patient care and the workforce?
- How is the organization protecting patient care data on mobile devices?

Without a fully implemented plan, the organization is at risk for negatively impacting patient care and having a potential breach of PHI with company or personally owned devices.

1. Develop a Mandatory and Unified Communication Plan as Part of the Overall Digital and Mobile Health Strategy

Many healthcare organizations are using mobile communications but have not adequately analyzed their use of communication in the delivery of patient care. While hallway conversations, email, telephones, and one-way paging have been used for years, understanding the abilities and capabilities of more advanced mobile communication platforms can dramatically improve the satisfaction of the users as well as improve overall patient care coordination and compliance with regulations. Start with understanding the data and how physicians and clinical staff use the mobile devices. Next senior leadership should analyze the following four categories to better understand what is missing from your current implementation:

- Basic functionality and privacy/security requirements—i.e., message status, logs, mobile device management features, encryption, privacy/security settings, and record management
- Integration and advanced functionality—i.e., alerts and alarms, test results, roles and schedules, electronic health record (EHR), clinical decision support systems (CDSS), and other clinical application integration
- Communication and workflow functionality—i.e., group conversations, search functionality, sending options, multimedia attachments, status, directories, and availability for physicians, nurses, and support and ancillary services
- Technology needs—i.e., smartphone (IOS and Android) support, cellular and Wi-Fi capable, and application download availability

2. Define an Acceptable Use Policy for Mobile Devices

Understanding the limitations of what is acceptable when using the mobile device must be discussed, defined, and accepted by the medical and nursing

[1] David Kotz et al., “Privacy and Security in Mobile Health: A Research Agenda,” *Computer,* Vol. 49, No. 6, June 2016; Bruno Silva et al., “Mobile-Health: A Review of Current State in 2015,” *Journal of Biomedical Informatics,* August 2015.

[2] Mary Walsh and John Rumsfeld, “Leading the Digital Transformation of Healthcare: The ACC Innovation Strategy,” *Journal of the American College of Cardiology*, 2017.

[3] Orrin Franko and Timothy Tirrell, “Smartphone App Use Among Medical Providers in ACGME Training Programs,” *Journal of Medical Systems,* October 2012.

[4] D.L. McBride and S.A. LeVasseur, “Personal Communication Device Use by Nurses Providing In-Patient Care: Survey of Prevalence, Patterns, and Distraction Potential,” *JMIR Human Factors,* April 13, 2017.

[5] Stephanie Kuhlmann, Carolyn Ahlers-Schmidt, and Erik Steinberger, “TXT@WORK: Pediatric Hospitalists and Text Messaging,” *Telemedicine and e-Health*, June 2014.

[6] Robert Freundlich, Kathryn Freundlich, and Brian Drolet, “Pagers, Smartphones, and HIPAA: Finding the Best Solution for Electronic Communication of Protected Health Information,” *Journal of Medical Systems*, November 2017.

[7] *Ibid.*

staff. The policy should address issues like type of data to be included in the communication (minimum necessary), Joint Commission requirements (i.e., no patient care orders), whether direct physician-to-patient or nurse-to-patient communication is acceptable, and documentation of mobile communication in the medical record.

3. Understand the Ownership, Control, and Support of Mobile Devices

The consumerization of mobile devices has impacted healthcare. Users expect the organization's devices to perform as well as their own devices, and they don't want to carry more than one device. There are a few different options when it comes to ownership: company owned and used for business only, company owned and used for both personal and business, and personally owned. When it comes to support and control, it is much simpler to support company devices that meet specific standards. Healthcare organizations need to consider their own IT resources and how much control they might be willing to give to the users if personally owned devices are allowed. Implementing a mobile device management infrastructure is highly recommended for any organization with mobile devices.

4. Address Mobile Device Privacy and Security

While the HIPAA security and privacy rules do not require specific technology solutions, healthcare organizations do need to implement reasonable and appropriate controls to safeguard the protected health information (PHI) from any unauthorized access, use, or disclosure. The Joint Commission also recommends that unsecured mobile communication should be prohibited. To help facilitate compliance with the laws, it is necessary to understand how the workforce will use the mobile device and how the security and privacy controls may limit or impede on the usability of the device. Technology alone will not solve the privacy and security risk. Executive support, education, and a culture of security and privacy is required.

In summary, boards and senior leaders must understand what they want and need out of a mobile health strategy. The current workforce entering the medical field has been exposed to mobile devices most of their lives and will use these devices to help them perform their work. While this article doesn't discuss the patient's use of mobile technology, it is important to address the patient mobile experience as part of the overall strategy since many patients expect their healthcare interactions to be similar to other current uses of their mobile device. Without a unified communication strategy, adequate controls, and knowledge of how the devices will be used within the healthcare facility, the potential for a breach of PHI is dramatically increased and the ability to realize the benefits for patient care will be missed. ●

The Governance Institute thanks Cris V. Ewell, Ph.D., CISSP, CISM, Chief Information Security Officer and Affiliate Assistant Professor, Biomedical Informatics and Medical Education, at UW Medicine, for contributing this article. He can be reached at ewellc@uw.edu.