Why Health Care Providers Need a Smartphone Policy

LORMAN®

Published on www.lorman.com - November 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

As smartphones and tablets become more prevalent in the workplace, employers and management must develop and implement stringent regulations that prevent their misuse. This is particularly true for healthcare providers and their employees. While there are a number of important reasons that healthcare providers need a smartphone policy, one of the most significant involves the privacy of patients and the protection of their health information.

The Use of Smartphones in the Healthcare Environment

Patients and medical staff alike utilize smartphones, tablets and related electronic devices on a daily basis. A November 2011 study conducted by researchers with CompTIA showed that approximately 38 percent of doctors and medical staff utilize medical applications on their smartphones every day. This percentage was, at that time, projected to reach about 50 percent by the end of 2012. In addition, an increasing number of patients in healthcare facilities are demanding that they be able to utilize the facility's network to communicate, via smartphone, with their doctors and nurses while they are present as well as when they are discharged.

The majority of personnel smartphone use in medical facilities can be separated into four key categories. These include the collection of data and patient monitoring, scheduling of appointments, prescription management and summarizing patient records.

Collection of data and patient monitoring - Some smartphone applications provide a physician with the ability to remotely monitor data collected by various medical equipment via WiFi. This technology is aimed at improving patient care as well as the healthcare professional's level of efficiency when visiting multiple patients.

Appointments - The use of smartphones in appointment scheduling and rescheduling has become increasingly popular in a number of healthcare facilities, including private practices, clinics and hospitals. Doctors, nurses are assistants are able to keep track of new and existing appointments in real time and share pertinent appointment information between them for more efficient workflow and improved patient satisfaction.

Prescription management - A substantial amount of a physician's time each day is dedicated to authorizing prescriptions and refills for their patients from the office. Requests for these authorizations are submitted to the physician by the patient's pharmacy and smartphone use can effectively reduce the amount of time it takes for approval to be confirmed. In addition, pharmacies are able to

communicate more quickly with doctors concerning potential drug interactions for patients taking a new medication for the first time.

Patient records - Smartphone technology has begun to, in part, replace traditional methods of record keeping in some doctors' offices and hospital settings. The ability to call upon pertinent patient history and current medical data instantly is frequently more convenient than requesting physical files and waiting for their delivery. Management of patient records is easier when all of the required information is contained in a compact smartphone rather than in bulky file folders and remote onsite computer systems. In addition, smartphones are used to quickly review and amend patients' insurance data and legal information as needed.

The conveniences associated with smartphone use in healthcare facilities continue to assist medical professionals in their quest to serve their patients more efficiently. The privacy implications, however, must be considered in every facility in which smartphones and tablets are used, even if they are only utilized for tasks solely related to work. In situations in which smartphones are used for personal or social media use, additional regulations must be observed to ensure proper conduct on the job as well as HIPAA/HITECH compliance.

Individually Identifiable Health Information and Smartphones

HIPAA defines individually identifiable health information as any past, present or future data that can be used to identify a patient. Common types of information included are a patient's address, employer, social security number, telephone number and date of birth. Because this information is easily accessed by all members of authorized staff in any healthcare facility, action must be taken to prevent its direct and indirect misuse.

Though some advances in smartphone and tablet technology aim to serve patients more efficiently and to make providers' jobs easier, the presence of these devices within healthcare facilities presents a clear privacy problem that appears to be growing. Private patient information can now, more easily than ever, be recorded and transmitted via smartphones in a way that is unsecured and potentially quite harmful to patients and their families.

The information contained in a patient's personal health record is private for a number of reasons. Social security numbers and birth dates, for example, can be relatively easily used to create unauthorized accounts with financial institutions or to access other pertinent financial information. It is crucial that data directly related to a patient's physical

or mental health be secure, as this type of information may potentially be used against the individual in future employment endeavors.

The Importance of Patient Privacy and Information Security

The Health Insurance Portability and Accountability Act, more commonly known as HIPAA, establishes definitive guidelines for healthcare providers, insurance companies, health plans and any business associates with whom they share health information regarding patients. The Privacy Rule was implemented specifically to protect patients' private health data, which includes any individual identifiable health information, regardless of the media by which the information is transmitted. This includes oral communication, electronic transmission or physical, written files.

The Health Information Technology for Economic and Clinical Health Act, or HITECH, contains guidelines that serve to promote improvement of patient care through enhanced information technology in the healthcare industry. HITECH serves as a complement to HIPAA by broadening the scope of healthcare provider liability in the event of a breach of security regarding private patient information.

Healthcare providers from every sect of the industry are increasingly encouraged to review their HIPAA literature in light of enforcement updates in HITECH. All staff members with access to patients' health records, electronic and otherwise, should become closely familiar with the policies outlined in each, as well as the consequences for failing to comply. This is particularly important if staff actively utilize smartphones, tablets and other electronic devices while at work. An annual review of the newly enforced guidelines is strongly recommended, as this information is pertinent to the success of individual healthcare professionals, the security of their patients and the prosperity of the healthcare facility as well.

Consequences of a Security Breach

Under HITECH, more stringent enforcement of HIPAA guidelines concerning electronic records is mandatory. Legislators intend to enforce guidelines more strictly than in the past, hoping to discourage the misuse of patient information via financial means. A breach of security will result in litigation to determine the presence of willful neglect, which may escalate to civil penalties of up to $250,000. If these offenses are repeated or left uncorrected, penalties may extend up to $1.5 million.

In the event of a breach of secured information, the patient whose information has been compromised must be informed immediately. If 500 or more patients are affected by a breach, the healthcare provider must deliver official notification to the Department of Health and Human Services. In some cases, The Office of Civil Rights will conduct an investigation into the offending facility and the media will be notified in order to warn potential victims of the breach. Further legal action may involve the Attorney General's office, a more rigorous investigation and heftier financial penalties following individual lawsuits.

Implementing a Smartphone Policy

The ease with which these and other types of information can be obtained and shared via smartphones makes the necessity for strict regulations even more obvious. While the benefits of smartphone use in medical facilities are undoubtedly real, providers must exercise responsibility regarding their use in the workplace. A smartphone policy is designed with the security of patient records and personal data in mind while allowing for the effective use of work-related applications by staff.

One aspect of a successful smart phone policy involves the number and types of devices that are allowed to access the healthcare facilities servers and data banks. Smartphones that are connected to the facility's network must be password protected and armed against malware at all times. If any device with connectivity to the network or information regarding any patient is lost or stolen, this event should be reported to the proper superior as soon as possible to prevent further compromise of patient data.

Another component of smartphone policies in healthcare settings concerns the ability to audit all devices at any time. Frequent audits help to prevent and identify various problems that may result in the security breach of private patient information and records. These types of audits have been shown to be effective in businesses of all sizes and types throughout the country.

An effective smartphone policy will encompass all aspects of information security, accessibility to healthcare providers and ease of use for all patients and staff members. Reaching an ideal balance between the advantages of smartphone use and compliance with HIPAA/HITECH regulations is the only way to ensure that patient information remains secure in healthcare facilities in which these devices are regularly used.