Healthcare

ALERTBULLETIN®

A Risk Management Update | 2019 Issue 3

Clinical Use of Smartphones: Tips on Mitigating Ten Major Risks

Personal mobile devices are ubiquitous in every area of American life, including healthcare. Smartphones in particular – as well as tablets, laptop computers and personal digital assistants – have become an important tool for today's healthcare professional. According to a recent study, approximately 80 percent of physicians use smartphones for clinical purposes, up from 53 percent in 2010, and 94 percent of physicians make personal and/or professional use of a smartphone. These electronic devices not only facilitate communication with patients/residents and each other, but they also can provide fingertip access to a vast array of medical information and applications, including laboratory and imaging data, reference materials, clinical support resources and healthcare information technology (IT) systems, such as e-prescribing and provider order-entry platforms.

The near-universal use of personal mobile devices by providers and staff has significantly enhanced efficiency and productivity. At the same time, however, leadership must be aware of the safety and liability implications of these communication tools. This *AlertBulletin*® examines 10 of the most common and potentially serious risks associated with the use of personal mobile devices in the healthcare setting, and offers suggestions designed to mitigate these exposures. By adopting effective policies and procedures, organizations can help safeguard patient/resident privacy, prevent the introduction of malware and viruses into IT systems, reduce malpractice risks associated with user distraction and miscommunication, and protect patients/residents from the growing threat of bacterial infection via contaminated screens.

1. Unregulated and incompatible devices.

"Bring Your Own Device" (BYOD) policies permitting use of personal smartphones and other devices in healthcare settings may result in interface problems with network platforms. The following general strategies can help enhance compatibility and accountability when implementing a BYOD program:

- **State the types of mobile devices that the organization's IT network will support, and expressly prohibit incompatible devices.** For example, a non-Windows-based smartphone platform may not interface with the facility's healthcare applications.
- **Develop guidelines that specify who may access network data via personal mobile devices** (e.g., physicians, nurses, technicians, therapists, IT staff, administrators), and delineate the type of data that can be accessed in this manner.
- **Maintain an inventory of personal mobile devices used by providers and staff for clinical purposes,** and require mobile device users to notify the organization whenever they upgrade or replace a device.
- **Provide staff with access to an IT support line** to answer questions concerning generational changes made to devices and network platforms. Depending upon the size of the organization, the task of managing workplace smartphone use may require dedicated support staff.
- **Ensure that the BYOD policy clarifies who is responsible for paying phone service and data plan charges** when staff or providers access patient/resident care information.

2. Security risks.

Use of smartphones and other mobile devices in healthcare settings creates major confidentiality concerns. Yet the majority of facilities that permit these tools to connect to the organizational IT network do not adequately check users' security precautions, producing the risk of potentially damaging data compromise. (See "Privacy breaches" at right.) The following measures can help strengthen the organization's data security program and reduce the likelihood of unauthorized access to network data by an unsecured mobile device:

- **Require that devices have a remote lock-out capability** to prevent unauthorized access if they are lost or stolen. This security measure can be obtained from and installed by specialized vendors.
- **Request that users activate their location services tracking function** to aid in finding lost or stolen devices.
- **Authorize the facility to remotely wipe data from a device** in the event it is lost or stolen.
- **Segregate healthcare data from the user's personal information** to permit remote deletion of sensitive data when a user is no longer employed by the facility.
- **Ensure that mobile devices are passcode-protected,** thus minimizing potential third-party access to any sensitive files stored directly on the devices.
- **Teach staff secure password-setting techniques,** such as changing passwords regularly, avoiding obvious codes, combining letters and numbers, mixing upper- and lower-case letters, and using the first letter of each word in a memorized sentence.
- **Prohibit sharing of passwords,** and inform staff and others with access to network data that this rule will be strictly enforced.
- **Remind users to set their devices for automatic logoff** if they are idle for any length of time, and also to program devices to lock in the event of multiple failed log-on attempts.
- **Delete all stored information before discarding any mobile device** and disable file-sharing applications.
- **Educate authorized mobile device users about relevant policies and procedures,** including the protocol for reporting a data breach.
- **Conduct periodic risk assessments of mobile device use** and determine whether essential protective measures, such as user authentication and data encryption, have been implemented to prevent unwarranted disclosure of sensitive data.

3. Privacy breaches.

Inappropriate disclosure of protected health information (PHI) that is stored on or accessed through a mobile device constitutes a violation of the HIPAA Privacy Rule, potentially resulting in costly fines, settlements and/or criminal penalties.[1] Such breaches often take the following forms:

- **Loss or theft of an unsecured device** containing PHI.
- **Distribution of unauthorized photos** taken by cellular telephone or other mobile device. (See "Unauthorized photos," page 3.)
- **Communication of PHI via texting** or posting on social media.
- **Third-party access to PHI,** whether stored on a mobile device or network server.
- **Transfer of an unencrypted email containing PHI from an organizational account to a personal account** that lacks comparable privacy safeguards.

The following measures can help guard against the risk of inappropriate disclosure of patient or resident data:

- **Protect sensitive data from illicit access via encryption technology,** which renders PHI unreadable to unauthorized individuals. Under the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, encrypted data is not considered "unsecure." Thus, if a mobile device containing encrypted data were lost, the event would not constitute a security breach necessitating a report to the U.S. Department of Health and Human Services.
- **Prohibit users from storing PHI locally on mobile devices.** Instead, require users to log in to the organizational server and access centrally stored patient/resident data.
- **Limit the types of network applications open to mobile users,** and password-protect network files or applications containing PHI.
- **Adopt biometric authentication safeguards** designed to verify that the person using the device is authorized to access PHI.
- **Utilize a password-protected virtual private network for all email and text messages sent from mobile devices,** thus enhancing security and confidentiality.
- **Require utilization of a HIPAA-compliant healthcare messaging application,** which permits mobile device users to securely text electronic PHI to other authorized parties.
- **Designate a private area for telephoning outpatients** to protect confidentiality.

1 Note that on April 30, 2019, the U.S. Department of Health and Human Services issued a notice of enforcement discretion reducing maximum financial sanctions for most tiers of HIPAA violations, as established by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Notwithstanding the revised penalty structure, leadership must remain vigilant in monitoring the clinical use of mobile devices and preventing privacy breaches.

4. Computer bugs.

Mobile devices of all types are vulnerable to a wide array of threats, including viruses and malware designed to steal data, capture keystrokes, corrupt files or damage IT system functioning. Written agreements with users, which clearly state organizational expectations, restrictions and conditions of use, can help mitigate these and other cyber liability risks. The following suggested requirements, among others, can be adapted as necessary and conveyed to users:

- **Install and maintain effective antivirus/anti-malware software and other security controls on devices** and respond promptly to antivirus software update alerts.
- **Scan for viruses and malware on at least a weekly basis,** using antivirus software.
- **Refrain from backing up organizational data to an outside computer,** which may itself be "infected." Preferable alternatives include bootable (or "clone") backups, external backup drives and encrypted cloud backups.
- **Ensure that device operating systems are current** and fully supported in terms of security "patches."
- **Avoid using free and open Wi-Fi connections** in cafes and airports, which are not secure and could lead to infection.
- **Attend a workshop on unsafe online practices** – such as opening suspicious attachments, clicking on questionable links and using unsecured Wi-Fi networks – and communicate lessons learned to staff.

Clearly state that serious penalties may be levied for failure to adhere to these rules, including, but not limited to, termination of employment.

Mobile devices of all types are vulnerable to a wide array of **threats**, including **viruses and malware** designed to steal data, capture keystrokes, corrupt files or damage IT system functioning.

5. Unauthorized photos.

Digital photographs and videos of patients/residents are considered PHI and require appropriate security measures to prevent unauthorized access, transmission or manipulation. Procedural safeguards should be compliant with HIPAA privacy requirements, accreditation standards, and state laws and regulations, including patient/resident consent for the use and release of images containing identifiable health information. The following strategies can help mitigate the legal and regulatory risks associated with still and moving images of patients/residents:

- **Draft formal policies in regard to patient/resident images,** addressing such key questions as who is authorized to take photos or videos, how are images to be created and stored, and what purposes are they to be used for.
- **Prohibit staff and providers from taking photographs or videos of patients/residents for personal reasons,** as opposed to legitimate clinical ones.
- **Describe picture-taking policies in patient/resident admission packets** and in the organization's HIPAA privacy notice.
- **Educate providers, staff and volunteers about photo and video rules and policies,** using training sessions, online tools, pamphlets and posters. In addition, present key image-related policies during annual orientation sessions and request a signed statement of understanding.
- **Empower staff to decline requests from patients/residents and families to take photographs** if these images could compromise the dignity or privacy of patients/residents or others.
- **Exercise care when taking pictures of medical devices,** ensuring that they do not display identifiable patient/resident information.
- **Store and retain digital photographs within the patient/resident healthcare information record** to support clinical decision-making and continuity of care.
- **Obtain the consent of patients/residents and others who appear in images.** Personal photographs taken by patients/residents, family and friends do not require HIPAA authorization, but the privacy rights of third parties should be respected.
- **Permit patients/residents and others to revoke their consent after pictures are taken** and request deletion of unwanted images.
- **Ensure that photos taken for marketing purposes comply with HIPAA privacy requirements,** and require the marketing department and/or outside vendors to adhere to sound risk management principles when taking and using pictures of patients/residents.

6. Wi-Fi network interruptions.

The increased demands placed upon Wi-Fi resources by mobile devices can adversely affect telemetry monitoring and other critical wireless applications. The following measures can help prevent network interruptions:

- **Maintain an inventory of wireless medical devices** dependent upon network frequencies.
- **Analyze organizational Wi-Fi infrastructure** and calculate its ability to support the demands of medical and mobile devices.
- **Consider upgrading the network infrastructure** to fully support data and voice traffic by healthcare providers and others.
- **Create a guest network to handle inbound Internet traffic** from patients/residents and visitors accessing email, social media platforms, websites, video/music sources, etc.

7. Electromagnetic interference.

Smartphones and other mobile devices generate electromagnetic fields, which may affect the functioning of electronic medical instruments. Organizational policies, therefore, must weigh the convenience of mobile communication against the risks of electromagnetic interference (EMI). The following rules can help minimize potential EMI while permitting controlled use of smartphones and related devices within the facility:

- **Clearly mark zones where personal mobile devices cannot be used** – such as critical care units, imaging suites and other areas containing digital instrumentation – and instruct staff, patients/residents and visitors to turn devices off when in these areas.
- **Designate "safe areas" for mobile device use** by patients/residents and visitors, i.e., areas without sensitive electronic equipment.
- **Using signs and verbal reminders, prohibit patients/residents and visitors from using mobile devices in proximity to certain medical equipment,** such as life support systems and infusion pumps, and explain the reasons for this policy.
- **Instruct staff and visitors to stay at least an arm's length away from medical equipment when using a smartphone** or other mobile device to avoid potential EMI problems.

8. Clinical distractions.

Mobile devices can potentially distract healthcare professionals from the task at hand, placing patients/residents at risk.[2] The following cellular telephone use guidelines can help clarify expectations, enhance the mental focus of providers and staff members, and limit liability exposure resulting from errors caused by untimely interruptions:

- **When in clinical areas, place phones on silent** at all times to minimize distractions.
- **In aging services settings, instruct staff to silence cellular telephones when in resident rooms and after hours** to avoid disturbing sleeping residents. In addition, prohibit staff from taking telephones into shower rooms or using them when transferring or ambulating residents.
- **Exercise professional judgment when utilizing mobile devices in the workplace,** e.g., use a smartphone for Internet access only when necessary for healthcare-related reasons.
- **Adhere to the organization's policy on personal use of cell phones, email and social media,** and refrain from texting friends and family except during designated break times.
- **Do not provide patients/residents with a personal cellular phone number** and never contact them directly using an unauthorized mobile device.

9. Texting miscues.

Text messaging is most appropriate for reinforcing spoken communication and conveying relatively simple information, such as condition updates, reminders and laboratory results in the normal range. The following additional measures can help enhance the accuracy, usefulness and impact of text messages to patients/residents and other providers:

- **Clearly identify yourself and the patient/resident under discussion** in every text message.
- **Avoid potentially confusing "text-speak" when messaging.** Use only approved, universally understood abbreviations.
- **Send cogent, clear and succinct messages** that close with an unambiguous call to action.
- **Attach messages to the patient/resident healthcare information record,** or, if necessary, manually document the message, including date, time, content and responses received.
- **If updates and test results are texted to others, recipients must confirm receipt** and respond to any orders or instructions, thus ensuring appropriate follow-up.

2 A distinction should be made between *clinical distractions*, such as responding to a question from a patient/resident or fellow provider, and *non-clinical distractions*, such as visiting a social media site or checking email. From a liability standpoint, a clinical distraction contributing to an error is likely to be more legally defensible than a distraction unrelated to patient or resident care, which may come to light during the discovery process.

10. Cross-contamination.

Mobile devices carried in healthcare settings can harbor dangerous bacteria. When screens and other surfaces are not regularly cleaned and users do not adhere to sound hand hygiene protocols, electronic devices may produce cross-contamination. The following basic infection control measures can help minimize this risk:

- **Regularly remind staff of the importance of frequent decontamination of mobile device surfaces,** including liberal use of antibacterial wipes designed for this purpose and utilized according to the manufacturer's instructions.
- **Request clinicians to pocket their phones when they are providing care for patients/residents** and whenever the devices are not in use.
- **Enforce strict hand hygiene before and after contact with patients/residents** or any potentially contaminated surface, as well as before touching a mobile device.
- **Refrain from sharing smartphones and other mobile devices** with patients/residents and other staff members to prevent transmission of pathogens.
- **Consider utilizing "cell sleeves,"** disposable protective cases that allow staff and visitors to make use of their mobile phones in healthcare facilities while minimizing the risk of cross-contamination.

As with every technological innovation, the proliferating use of smartphones and other personal communication devices in healthcare contexts has produced both benefits and associated liability exposures, which range from distraction, miscommunication and cross-contamination to privacy breaches, computer viruses and electronic interference. Leaders should be cognizant of these varied and evolving hazards and implement sound, up-to-date policies designed to optimize the convenience of mobile communication technology while managing related risks.

Quick Links

- Cybersecurity Practice Guide SP 1800-4: "Mobile Device Security: Cloud and Hybrid Builds." National Institute of Standards and Technology and the National Cybersecurity Center of Excellence. February 21, 2019.
- "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." The U.S. Department of Health & Human Services. December 28, 2018.
- "Mobile Devices: Know the Risks. Take the Steps. Protect and Secure Health Information." A presentation from the U.S. Department of Health & Human Services' HealthIT.gov.
- Mobile Security Toolkit. Healthcare Information and Management Systems Society (HIMSS), November 2017.
- "Take Steps to Protect and Secure Information When Using a Mobile Device." A factsheet from the U.S. Department of Health & Human Services' HealthIT.gov.

Did someone forward this newsletter to you? If you would like to receive future issues of *AlertBulletin*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare