Cell phones, smartphones, tablets, and other personal electronic devices (PEDs) are commonplace in health care and other workplaces. Use of PEDs has numerous benefits for both caregivers and residents. For staff, advantages include easier communication among themselves, instant access to reference materials, and quicker access to health data. For residents, use of PEDs can be a source of empowerment and freedom, and PEDs also allow residents to stay easily connected with friends and family.

But along with the benefits come serious health and safety risks, and organizational policies have often failed to keep pace with technology. Indeed, a February 2017 survey of more than 300 medical professionals found that only 65% of respondents reported that their facility had a documented strategy in place for mobile devices. Twenty-five percent of respondents stated that their facility had no method of enforcing mobile policies.¹

As a foundation of any effort to manage risks that include privacy breaches, distractions, the spread of infections, the introduction of malware, and more, organizations should develop a comprehensive PED policy governing the device use.

What to Consider Including in a Policy

The US Department of Health and Human Services’ Office of the National Coordinator for Health Information Technology (ONC) provides comprehensive resources on mobile device and health information privacy and security. Among them, ONC lists the following five steps health care organizations can take to manage devices used by residents and professionals:²

- Decide whether the organization will allow mobile devices to access, receive, transmit, or store residents’ health information or use them as part of the organization’s internal networks or systems (eg, electronic health records [EHRs]).
- Assess how mobile devices affect the risks (ie, threats and vulnerabilities) to the health information the organization holds.
- Identify the organization’s mobile-device risk management strategy, including privacy and security safeguards.
- Develop, document, and implement the organization’s mobile-device policies and procedures to safeguard health information.
- Train providers and professionals on mobile device security and privacy awareness.

Developing a PED policy that makes sense for each organization—one that balances the needs of staff members, residents, visitors, and the institution as a whole while clearly defining when, where, and for what purposes PEDs may be used—is key to protecting the facility against risks. The policy should include a clear definition of data ownership—that is, which data are considered owned by the facility and which are considered owned by the PED user—and clearly identify what constitutes sensitive information.³

Successful policies will also have the support of key leadership and the cooperation of PED users, including clinical and nonclinical staff, residents, vendors, and visitors. Also consider incorporating adherence to the PED policy into employment contracts and medical staff bylaws.

Guidance on Staff Text Messaging

Importantly, the facility’s PED policy should clearly outline the facility’s stance on text messaging. Joint Commission has prohibited the use of even secured texting platforms among caregivers.⁴ Nevertheless, unsecured texting is still occurring in health care.

The Healthcare Information and Management Systems Society (HIMSS) has released a list of administrative and physical precautions that organizations can take to establish guidance on text messaging by health care personnel and to address security risks presented by text messaging (Box 1).⁵

Establish Policies and Procedures for PED Use

One of the committee’s first orders of business should be to decide how restrictive the PED policy should be. In general,
Three basic approaches to allowing PEDs in the facility include the following:

**Facility-provided devices.** In this scenario, the organization purchases the devices and data plans for staff with the understanding that staff will use them for work-related activities. Facility-provided devices allow the organization to have greater control over how devices are used, because IT staff can dictate which applications can be downloaded onto the device, monitor the device, and install and update appropriate security software.

**“Bring your own device” (BYOD).** BYOD describes the practice of allowing staff to use their own PEDs within the health care facility for work-related activities. This approach, when implemented appropriately, allows users to continue using the PEDs they are comfortable with, while still enforcing the facility’s policies and ensuring the security of electronic protected health information (ePHI). BYOD policies can involve the installation of facility-approved software onto the PEDs, through which staff can communicate. If the facility chooses this approach, it will need to decide whether personally owned PEDs will be able to connect to the facility’s internal network or system, either on-site or remotely. According to an infographic from Spok, Inc, 71% of more than 350 health care leaders surveyed in July 2017 said their hospital allowed some form of BYOD at their hospital, an increase from 58% in 2016. This approach is generally seen as the most cost-effective.

**A hybrid approach.** A hybrid approach takes elements from both the facility-provided and the BYOD approach—for example, standardizing a specific brand of phone employees should use but allowing staff to use their own personal devices.

Any of these approaches can be implemented successfully, but each requires an analysis of the risk, thoughtful planning, and documentation of the rationale for the choice. A facility’s choice will reflect its preferred balance of cost, management effort, level of control, and degree of flexibility the user is afforded.

### What Else Should Facilities Consider?

Additional questions a facility should consider when deciding to allow PEDs are discussed below.

**How Will PEDs Be Managed?**

The committee will need to decide how to identify and track all PEDs that access the facility’s network and systems. It will also need to decide what security software will be used and which apps to approve for use. The committee should also assign responsibility to check mobile devices used for remote access to determine whether selected security settings are enabled, and it should determine whether mobile devices will be regularly reviewed and audited.

**Where Can PEDs Be Used?**

The committee must decide whether unrestricted use of PEDs will be allowed throughout the building. Alternatively, the committee may decide to ban PEDs from certain areas or to restrict them to certain areas, such as common areas or staff lounges.

**What Restrictions Should the Facility Enforce?**

If the devices are provided by the health care facility, the committee will need to decide whether users can bring their devices home and whether and in what ways staff are permitted to use their devices when away from the facility. The committee will also need to decide whether certain users will be

---

**HIMSS Recommended Precautions to Include in Texting Guidance**

- Do not text clients or members of the public without their written consent.
- Verify that the phone used for sending the text message is password protected and secured at all times, including at home and work, and verify that the cell phone number of the client is recorded correctly.
- Delete text messages after communication is completed and necessary information is documented appropriately.
- Do not include protected health information in a text message, and never use first and last names in a text message. Do not store first and last names in the address book used for sending text messages; rather, store the first name plus last initial only.
- Do not respond to a client-originated text that includes PHI; instead, send a new message that asks the client to call you.
- Use best practices when texting, including the following:
  - Be aware of tone.
  - Be professional at all times and do not use abbreviations.
  - Text messages should be short and concise; more than 160 characters will transition into two messages.
  - Respond in a timely manner.
  - Establish clear expectations with your clients and the public about two-way communications regarding whether you will continue a dialogue and how quickly you expect to reply.
allowed to use their PEDs to access the facility’s EHR system or internal networks remotely.

If a BYOD policy is implemented, a facility may insist that only devices that meet its security requirements—for example, those that support an appropriate level of encryption—are allowed access to the facility’s systems. This requirement provides a prudent measure of control, but it also may mean that certain smartphones will not be supported and thus staff will be unable to use them to gain access to the facility’s systems.

**How Will Lost or Stolen Devices Be Handled?**

To prevent ePHI from being inappropriately disclosed, the facility must have a procedure in place to wipe or disable a phone that is lost or stolen, including the personal devices of staff if the facility has a BYOD policy. User agreements should stipulate that, in exchange for access to the facility’s systems, users must allow the facility to remotely wipe data from the device if it is lost or stolen. This could mean that the user’s personal data will be deleted along with the organization’s data.

Health care facilities must also have a procedure to recover and delete information from the phones of providers who leave the organization. In addition, organizations with BYOD policies must identify a process to deal with old devices when users upgrade to new PEDs. The policy should require users to notify the organization when such changes are considered and to submit their old devices to the facility before donating or otherwise disposing of them so that the PEDs can be adequately secured and checked.

**How Will the Facility Handle Information Storage on PEDs?**

The committee will need to determine what type of information clinicians can store on their devices, as well as where and for how long it can be stored.

One option for data storage is to implement a “thin-client” configuration: rather than storing resident data locally on a PED, the device would instead operate as a terminal, allowing authorized users to log in and access information that is stored centrally on a server. For example, an application may allow remote viewing of a resident’s dietary log. The thin-client approach reduces security risks—if, for example, the device is lost or stolen—because no PHI is stored on the device.

Alternatively, some software solution companies offer tools to control which applications mobile users can access or to otherwise segregate health care facility data from the user’s personal information. Such approaches are promoted as allowing business and personal applications to coexist securely on the same device. These tools may allow the selective wiping of only the facility data, sparing the user’s personal data in the event that the device is lost.  

**How Will Device Misuse Be Handled?**

If they do not already exist, policies and procedures will need to be developed by the committee to address the misuse of PEDs, including staff education and disciplinary actions.

**How Will the Facility Handle PED Policy Training, and How Will It Hold Staff, Residents, Visitors, and Vendors Accountable for Compliance?**

Once the organization develops a policy, the committee will need to arrange for training of all clinical and nonclinical workers on the policies and procedures associated with PED use. Posters, leaflets, flyers, and videos are all ways that facilities can convey information about their mobile device policies and can serve as good reminders to staff.

In addition, the facility will need to develop user agreements for staff, residents, and visitors that clearly outline the new policy. If the facility allows staff to bring their own devices, the user agreement should specify that staff PEDs will be subject to the same security measures as the facility’s internal devices. The facility will also need to decide which person or department will bear responsibility for enforcing the PED policy.

**Conclusion**

Developing and implementing a policy is only a starting point for organizations to manage PED use. They will need to address basic elements, such as respecting resident privacy and confidentiality, and consider a host of concerns that range from cross-contamination when exposed to infectious agents to WiFi network overload to tripping hazards when devices are plugged in to charge. ECRI Institute has even received reports of incidents in which family members visiting hospital patients plugged USB cables into medical devices, such as infusion pumps and ventilators, to charge their PEDs; this raises the risk of device malfunction and even the inadvertent introduction of malware to the device and the organization’s network.

None of these additional risks can be managed, however, without a policy in place to set expectations for staff and provide meaningful guidance on acceptable behavior.

**References**


**www.annalsoflongtermcare.com**