Evolution or revolution? **Smartphone** use in nursing practice

Smartphones can aid nurses' clinical practice, but they must be used in compliance with laws, policies, and procedures.

By Cheryl D. Parker, PhD, MSN, RN-BC, FHIMSS

SINCE SMARTPHONES were introduced in 2002, a communications revolution has taken place. We talk on our smartphones, we text on them, we take pictures and post them to social networks, we communicate in 140-character "tweets," and share our thoughts and events on our personal networks. We use smartphone applications to monitor our exercise, manage our calendars, and practice our deep breathing. For many people, forgetting their smartphone causes instant panic.

In health care, physicians' smartphone use has grown exponentially. Just 6 years ago, I listened as chief information officers (CIOs) at the largest healthcare organizations in Texas insisted emphatically that a bring-your-own-device (BYOD) policy would never happen in their facilities. Of course, things don't always go as planned. According to the Wolters Kluwer Health 2013 Physician Outlook Survey, approximately 80% of physicians now use smartphones in their work.

But in the context of nursing practice, the communications revolution is only now starting to make a direct impact. Most nurses continue to use voice-only phones, multiple pagers, or wearable voice-activated two-way communication devices provided by their employers. While we may use smartphones in our private lives, many of us still use outdated communication devices at work. Or do we?

After visiting healthcare facilities across the country, I'm convinced nurses are in on the communications revolution. I've seen them use their own devices—not those provided by their employers—to text other healthcare team members (including physicians) outside the facility, access reference materials, and perform many other functions on their smartphones that aren't supported by employer-provided technology.

Is this a problem? For several reasons, increasing use of personal smartphones should raise concern for healthcare facilities. (See *Infection prevention for smartphones*.)

Legal and regulatory compliance

The foremost concern is legal regulatory compliance. Despite hospital policies forbidding use of personal phones by employees during work hours, 67% of hospitals reported in 2013 that their nurses used personal devices to communicate and support their workflow. This means, in effect, that nurses could be violating federal laws (specifically, the Healthcare Insurance Portability and Accountability Act), hospital security policies, and the American Nurses Association's Code of Ethics. If they're sending protected health information (PHI) on their smartphones in a way that can be linked to a specific patient, they're also violating state nurse practice acts. Sending PHI could lead to loss of employment, financial fines, jail sentences, and loss of one's nursing license. To make sure they're not jeopardizing their jobs, nurses must determine if their communication and workflow habits comply with applicable laws, policies, and procedures.

Cellphone security

What about security? Don't most people secure their smartphones? In a word, no. Two of five people sur-

veyed don't take the most basic smartphone security precautions. Criminal hackers are focusing more attention on smartphones than on other electronic devices, according to cybersecurity experts.

A 2013 survey asked 1,000 full-time American workers to describe their personal smartphone use in the workplace. Among respondents who chose health care as their employment sector, 88.6% said they used their personal phones for work purposes. Among all respondents, 39% said they don't password-protect their phones. Potentially more dangerous, 52% used their smartphones on unsecured Wi-Fi networks, such as those at coffee shops. Use of unsecured Wi-Fi is a well-known security vulnerability because it can allow for easy phone data theft.

Do you know if your smartphone's Bluetooth is set to "discoverable" by other devices, such as your hands-free headset? This is another security layer most people don't think about. Data on an employer-owned phone usually can be deleted remotely if the phone is lost or stolen. This is sometimes called "wiping" or "bricking," meaning the device is no longer functional because the operating system, programs, and data have been rendered inoperable. But it's rare that data on individually owned devices can be deleted remotely. So even if you never use your smartphone for work, ask yourself if you could delete all those pictures, texts, and emails if you lost your phone. Do you have a backup of your phone's data just in case you have to delete everything?

Who owns the phone?

Employers have the greatest control over devices they own and distribute. But even in a BYOD environment, employers can require installation and use of applications that provide the necessary security. Policies and procedures help outline what devices are permitted and specify security requirements to ensure password protection. In many cases, the standard four- to six-digit password is not secure enough; a hacker could crack a password such as 654256 in less than 1 second.

Policies need to spell out clearly who's responsible for smartphone-related services, including dealing with problems accessing the facility's secure network. Employers need to decide which applications are allowed, when updates must be performed to maintain application security, and what happens if the employee leaves the organization.

In a BYOD environment, wiping the device in case of theft or loss becomes an interesting question. If the device is storing both organizational and personal data, both types will be lost in the wipe. What are the rights of the individual and the organization in this situation? This is another area where policies and procedures must be made clear to all. If you're using your personal device at work, find out if your organization has a BYOD policy and ensure that you're in compliance.

In the future, certain communication exchanges may become part of the electronic health record (EHR). Such data, including pictures, shouldn't reside on smartphones no matter who owns them, but instead should be stored on a secure server with audit tracking.

Infection prevention for smartphones

It should come as no surprise that mobile phones are dirty. In 2012, *The Wall Street Journal* randomly chose eight cell phones of office employees to test for bacteria. All of them showed abnormally high coliform levels, indicating fecal contamination. And these are the phones of office workers. Imagine what microbes nurses' phones might carry, given our work environments.

Recently, products for ultraviolet disinfection for both personal and enterprise use have entered the market. Waterproof phone cases allow disinfection with commercially available disinfecting solutions without damage to the device. Are such disinfecting methodologies available to you at work? Are you disinfecting your phone at home?

Future of smartphones in nursing

Facilities considering use of smartphones for clinical staff need to think about clinical communication as part of the patient-care process instead of just replacing current phones and functionality. Nurses need choices in communication methods, including secure, encrypted texting and email. Communication must be put in a clinical context to properly identify the patient, who should be at the heart of the communication exchange. Use of pictures, such as of a patient's wound, should be part of the available communication methods even if the photos can't be uploaded to the EHR.

Even more important, just as smartphones give us cognitive support in our personal lives, we need to look for solutions that do the same in the complex work of nursing. Just as personal smartphones remind us that our best friend's birthday is next Saturday, nurses could use employer-provided smartphones and technology to help them in clinical practice.

If you're asked for input on your organization's next communication solution, consider the issues discussed in this article. It's not enough that your phone can send texts. Is your phone data secure? Can the phone be disinfected? Will it survive the rough-and-tumble healthcare environment? What's the vendor's vision for the future of its platform, and how will it support nursing practice?

Envision the future of smartphones that can assist us both as nurses and in our private lives. And envision yourself using a smartphone in compliance with laws, policies, and procedures in a way that's safe and secure. ✭

Visit www.AmericanNurseToday.com/Archives.aspx for a list of selected references.

Cheryl D. Parker teaches nursing informatics at the Walden University School of Nursing in Minneapolis, Minnesota. She is chief nursing informatics officer for PatientSafe Solutions, based in San Diego, California.