Canadian Nurses Protective Society

infoLAW®
Mobile Devices in the Workplace

Vol. 21, No. 1,
November 2013

Increasing numbers of nurses are using smartphones and other mobile devices to communicate with colleagues and patients by telephone, text message or email and even to photograph wounds or skin conditions. Understanding the risks involved in using mobile devices may prevent potential adverse personal and professional consequences.

Risk Management Considerations

Privacy Breaches

Unauthorized disclosure of a patient's personal health information (PHI) is a risk because mobile devices, such as smartphones, generally store and retain data on the device itself. Also, mobile devices are vulnerable to loss and theft because of their small size and portability.

Nurses have a professional and legal obligation to protect the privacy of patients' PHI. This is commonly accomplished through the use of strong passwords and encryption to safeguard electronic PHI being communicated through mobile devices. Employers generally have policies that require the use of such safeguards.[1] Without encryption, any emails, voicemails, pictures or text messages containing a patient's PHI could be inappropriately accessed or disclosed if the mobile device is lost, stolen or inadvertently viewed by a friend or family member. Unauthorized disclosure can also occur during the wireless transmission of personal data.[2]

There have been several reported privacy breaches in Canada involving mobile technology in the healthcare sector. Recently, a nurse lost an unencrypted USB key that contained the personal health information of approximately 83,500 patients who had been immunized for H1N1. The memory stick was not encrypted. This incident resulted in an investigation by the privacy oversight office and a class action lawsuit. In another case, a nurse working for a large teaching hospital had her laptop stolen from her car. The laptop contained records of approximately 20,000 patients. It was determined that the laptop was not encrypted, despite the hospital's stated policy.[3] These cases highlight that encryption is now the expected safeguard for data protection on mobile devices.[4]

Workplace Integration

Some employers have prohibited the use of personal mobile devices during work hours or in certain areas of the workplace, while others provide nurses with employer-owned mobile devices for clinical use. More commonly, healthcare employers are implementing bring-your-own-device (BYOD) programs in which employees are permitted or even encouraged to use their own mobile devices in the workplace. Employers with BYOD programs will generally implement corresponding policies, protocols and systems that enable healthcare practitioners to use wireless devices to securely interact with other healthcare practitioners and to access patient records.[5] However, the use of personal mobile devices without secure workplace integration, support (including the implementation of adequate encryption modalities) or knowledge can create an increased risk of a privacy breach and other adverse consequences.

"Encrypt Your Mobile Devices: Do It Now"

Ann Cavoukian, Information & Privacy Commissioner of Ontario

Managing Expectations

In some cases, nurses, including nurse practitioners, are using their mobile devices to communicate directly with patients, both during and after hours. In addition to managing the privacy and security concerns associated with these communications, nurses are reminded to manage patient expectations about permitted purposes of these communications, how quickly they will respond to enquiries and what to do if the nurse is unavailable. Reasonable limits and response times can then be clearly communicated to patients.

Infection Control

Studies have found high bacterial contamination, (including MRSA), on mobile devices, which are likely to have originated from the hands of the healthcare workers.[6] Since mobile devices are frequently handled and carried into multiple patient rooms, nurses are reminded to disinfect them often.

Consider Implementing the Following Precautions for the Security of Mobile Devices

- Use employer-issued mobile devices, where available, instead of your own device.
- Limit the use of your device for recording, transmitting or storing patients' PHI, unless there are clear organizational policies permitting this practice.
- Work with your employer's information technology department, if using your own device, to ensure your device has features and software that comply with your employer's BYOD policies.
- Follow employer policies and only use employer-issued mobile devices for taking photographs or videos of patients for clinical purposes.[7]
- Have and use strong password and encryption capabilities.
- Limit the amount of PHI stored on your device or, de-identify the PHI it contains.
- Turn off or do not enable WiFi and Bluetooth on any device containing or having access to patients' PHI without confirming the connection is secure and protected.
- Transfer patient health care information recorded on your mobile device to the patient's record as soon as practical, then use wiping software to permanently erase the information from your device.
- Use the time-out feature on your device, such that it automatically locks when not in use.
- Store your mobile device in a secure location; avoid leaving it unattended or allowing others to have access to it.
- Confirm whether your device has the capability to remotely erase data stored on the device, in the event that it is stolen.

Please contact CNPS at 1-800-267-3390 if you have questions regarding the professional implications of the use of mobile devices in the workplace and visit our website at **www.cnps.ca**.

1. Order HO-004, Office of the Information and Privacy Commissioner of Ontario; Fact Sheet: Encrypting Personal Health Information on Mobile Devices, 2007; Safeguarding Privacy in a Mobile Workplace, 2007; BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data, 2008, online: www.ipc.on.ca; Helpful Tips Best Practices: Mobile Device Security, Office of the Saskatchewan Information and Privacy Commissioner, 2009, online: www.oipc.sk.ca.
2. Office of the Information and Privacy Commissioner of Ontario, Fact Sheet: Wireless Communication Technologies: Safeguarding Privacy & Security, 2007.
3. Order HO-007 and Order HO-008, Office of the Information and Privacy Commissioner of Ontario, online: www.ipc.on.ca.
4. Investigation Report F12-02, Office of the Information and Privacy Commissioner for B.C., online: www.oipc.bc.ca.
5. Jerry Zeidenberg, "Massive acceptance of BYOD at MUHC", *Canadian Healthcare Technology* 18, 3 (April 2013).
6. Fatma Ulger et al, "Are we aware how contaminated our mobile phones with nosocomial pathogens?", *Annals of Clinical Microbiology and Antimicrobials* 8, 7 (March 2009).
7. Nurses Association of New Brunswick, *Practice Guideline: Ethical and Responsible Use of Social Media Technologies*, 2012.