Ontario Telemedicine Network
Position Paper
On Wireless Communications Technology In A Telemedicine Environment
October 8, 2010
Updated: September 2012

# Background & OTN Position

The rapid adoption of wireless communications technology is transforming the healthcare sector by offering unprecedented mobility, flexibility, convenience, and ease of use in a wide variety of applications. Wireless solutions, based on proprietary implementations as well as open standards, are increasingly becoming the communications technology of choice for many OTN Members.

Wireless local area network (WLAN) devices, for instance, allow Members and users of telemedicine the ability to move their laptops and videoconferencing equipment from place to place within their premises without the need for wires and without losing network connectivity. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printers, digital cameras, headsets and other peripheral device connections.

However there are inherent risks in any wireless technology. Some of these risks are similar to those wired networks; some are exacerbated by wireless connectivity; some are new.

The Ontario Telemedicine Network (OTN) recognizes the potential benefits of wireless technology in a telemedicine environment and is committed to working with its Members to ensure that these benefits are realized without compromising the privacy and security of patient information.

The protection of personal health information (PHI) in a telemedicine environment is a joint responsibility between OTN, its members and users of telemedicine. A breach of privacy at one end point puts at risk PHI transmitted from any other end point with which it communicates. For this reason OTN has developed a position paper on wireless communications technology in a telemedicine environment.

Members planning to deploy wireless communications technology and devices in their telemedicine environment should, at a minimum, consider the following:

1. Inform OTN of its intention to do so

2. Inform and involve their privacy officer and their information security officer

3. Comply with and adhere to its obligations under the '*Personal Health Information Protection Act, 2004*' (PHIPA)

4. Comply with and adhere to privacy and security requirements outlined in relevant IPC orders/papers and OTN position paper (s) and/or guidelines

## Risks to the privacy and security of personal health information with the use of wireless technology

It is important to understand the privacy and security risks inherent in the use of wireless technology. Specific threats and vulnerabilities to wireless networks and devices include the following:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.

- Mobile devices are easily stolen and can reveal sensitive information if not properly encrypted.

- **Wireless signal propagation.** In a wired system, a communication signal is confined to the wire on which it is transmitted. In order to intercept the signal, a receiving device must be attached directly to the wire. In a wireless system, a communication signal is broadcast over an extended spatial area, and anyone within that area, using an appropriate receiving device, will be able to intercept the signal.

- **Encryption requirements.** In order to preserve the confidentiality of information transmitted over the wireless medium (which is inherently susceptible to eavesdropping), the information must be encrypted. A secure wireless encryption scheme is difficult to design and implement, leading to the frequent absence of encryption capabilities in real-world wireless systems, as well as numerous weaknesses in systems that do provide these capabilities.

- **Interference and jamming.** Because wireless signals propagate over an extended spatial area, it is easy for two signals to interfere with each other, causing both to become corrupted. Interference may be caused by other wireless sources in the area, leading to degradation in the performance of a wireless system. Furthermore, a malicious attacker may intentionally generate a strong wireless signal designed to interfere with a wireless system, in order to prevent it from operating.

### What Can Happen?

In a widely publicized incident, images of a patient giving a urine sample in a methadone clinic washroom were displayed by a wireless rear-assist parking camera in a car parked near a clinic. The clinic was using a wireless surveillance system to monitor patients who were required to give urine samples under direct observation.

The video surveillance system did not have the encryption capabilities needed to protect the confidentiality of the transmitted video stream. (see http://www.ipc.on.ca/images/Findings/up-ho_005.pdf)

## Your responsibilities as a health information custodian

Section 12(1) of *the Personal Health Information Protection Act* (PHIPA) requires that a health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In her order[1] related to the methadone clinic incident, Ontario's Information and Privacy Commissioner has stated that any custodian intending to use wireless communications technology should only do so if strong, privacy protective precautions have been taken. According to the Commissioner, strong security and privacy precautions should involve the use of staff or third parties with appropriate expertise. One of the first steps a custodian must take is to inform service providers (including external ones such as vendors or internal ones such as IT departments) of its responsibility to protect personal health information under the Act. See http://www.ipc.on.ca/images/Findings/up-ho_005.pdf for the minimal steps the Commissioner outlines for custodians, its agents and other service providers.

[1] http://www.ipc.on.ca/images/Findings/up-ho_005.pdf

## Privacy and Security Guidelines for the use of wireless technology in a telemedicine environment

The following privacy and security guidelines have been adapted from fact sheets and papers published by the Office of the Information and Privacy Commissioner of Ontario. It is up to each Member or user of telemedicine to understand their requirements under PHIPA, determine the level of risk that can be accepted and the practices deemed appropriate to manage its risk.

These guidelines are applicable to OTN members and users of telemedicine who deploy or plan to deploy, wireless networked computing and communications devices (either synchronous such as videoconferencing equipment transmitting data in motion or asynchronous such as laptops, USB keys or other mobile devices containing data at rest) in their telemedicine environment.

Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to these technologies, Members and users of telemedicine are encouraged to take advantage of additional resources for more current and detailed information.

Guidelines adopted from the OIPC:

- Threat Risk Assessment and Privacy Impact Assessment. A HIC should inform the service provider of the custodian's responsibility to protect PHI under PHIPA. In light of this responsibility, the service provider makes recommendations, providing necessary explanations; in a larger organization this might involve conducting a Threat Risk Assessment (TRA) and/or a Privacy Impact Assessment (PIA). It is important that organizations ask technology providers, including any third-party application vendors, the right questions in order to confirm that PHI will be transmitted, accessed and stored in a secure manner.

- Encryption. End-to-end encryption of all data transmissions over wireless networks is critical to keeping PHI secure. In the event PHI is stored on wireless devices, the information should be encrypted. Encryption of data prevents unauthorized parties from accessing PHI stored in devices, even if a device is lost or stolen Encryption guidelines should factor in[2]:

  - Secure implementation of FIPS 140-2;

[2] Adapted from Health-Care Requirement for Strong Encryption, 2010

  - Secure and managed encryption keys;
  - Secure authentication of devices;
  - No unintended creation of unencrypted data;
  - Encryption by default; and
  - Availability of information lifecycle protection

- **Data authenticity.** Data authenticity allows the recipient to trust that a message was not sent by an unauthorized party that is pretending to be an authorized device. To prevent this from occurring, a wireless device should be required to authenticate itself to the network and enterprise systems, and the enterprise server should authenticate itself to the device.

- **Regular audits.** Once the wireless solution is installed, the organization should establish a schedule for objective and comprehensive privacy (including security) reviews appropriate for the system involved. For organizations that fall under PHIPA, failing to conduct regular reviews of their information technology from a privacy and security perspective is likely to fall short of meeting the reasonableness standard under the Act with respect to their requirement to protect PHI.

- **Privacy policies and procedures.** Privacy policies and procedures should comprehensively outline the organization's information practices, which address areas such as assigning accountability for privacy to specified individuals, defining the purposes for which personal information is collected, and outlining the organization's procedure for responding to privacy breaches. These policies and procedures should be made available to employees, students, volunteers etc.; communicated and posted in areas where they are likely to be viewed.

- **Data minimization.** The design of wireless solutions should begin with non-identifiable interactions and transactions as the default. IPC Order HO-004 advises that the first line of defense against unauthorized access is to avoid storing PHI on mobile computing devices at all.

- **Data integrity.** To establish confidence that PHI has not been tampered with or altered during transmission, wireless solutions should include mechanisms to prevent and detect any changes or modifications of data.

- **Control over third-party applications connections.** To prevent malicious third-party applications from being downloaded onto wireless devices, which may be designed to steal data, gain access to the organization's network or cause harm to the network, the wireless solution should allow system administrators to control or block the installation of third-party or untrusted applications.

- **Other safeguards.** A wireless device in the possession of front-line staff or clients can store PHI temporarily or for longer periods to allow users to view the information locally. If the device is lost or stolen, or is left unattended, PHI stored in the device could be accessed by unauthorized persons if the appropriate safeguards are not implemented. Organizations should search for wireless solutions that allow corporate system administrators to enforce and have full control over device-level security features, ensuring that they are applied consistently across all devices and cannot be overridden by individual users. The security policies and features that system administrators should be able to enforce remotely include:

  - mandatory password authentication/power-on passwords;
  - strong password length and composition;
  - password expiration;
  - the number of password attempts on the device before data on the device is deleted;
  - security timeouts that set the number of idle minutes before the device locks;
  - periodic challenges that will require the user to enter a password a certain period of time after unlocking the device;
  - wiping/erasing of device contents;
  - locking of devices; and
  - resetting of passwords.

- **Limiting retention and secure destruction.** PHI that is stored on the device could remain there indefinitely, increasing the opportunity for inadvertent disclosure, if there is no practical means to remove the information when it is no longer needed. PHI should be retained on devices only as long as necessary. To minimize privacy risks, organizations may wish to consider specifying a limited length of time PHI can be retained in wireless devices, before it is automatically deleted and securely destroyed/sanitized.

## Additional IPC Guidance

**Fact Sheet # 16: Health Care Requirement for Strong Encryption (July 2010)**

**PHIPA Order HO-007 Encrypt Your Mobile Devices: Do it Now (January 2010)**

**PHIPA Order HO-004 (March 2007)**

**Fact Sheet # 12: Encrypting Personal Health Information on Mobile Devices (May 2007)**

**Fact Sheet # 13: Wireless Communication Technologies: Video Surveillance Systems (June 2007)**

**Fact Sheet # 14: Wireless Communication Technologies: Safeguarding Privacy & Security (August 2007)**

## Further Reading

**FIPS standards:**
http://csrc.nist.gov/publications/PubsFIPS.html

**List of FIPS 140 certified encryption products:**
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

**ISO/IEC 19790:2006 – Security requirements for cryptographic modules**

**ISO 27799: Health informatics – Information security management in health using ISO/IEC 27002**

**Note: This paper reflects OTN's position with respect to risks and recommended best practices associated with wireless communications technology in a telemedicine environment at the time this document was written. Resources and further reading references are not meant to be exhaustive.**