Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 13
June 2007

Wireless Communication Technologies: Video Surveillance Systems

Section 12(1) of the *Personal Health Information Protection Act* (*PHIPA*) sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) 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 a widely publicized incident, for which an Order was issued – HO-005 – images of a patient giving a urine sample in a washroom were being accessed by a wireless mobile rear-assist parking device ("back up camera"), in a car parked near a clinic. The patient was attending a methadone clinic in which patients were required to give urine samples under direct observation. The clinic was unaware that such an interception was even possible.

Closed Circuit Television (CCTV) or video surveillance cameras are being used in the Ontario health sector for a range of purposes ranging from building security to observational research. Typically, these uses increase efficiency or help prevent negative patient outcomes. The unintended consequence of video surveillance, however, regardless of its primary function, is often an invasion of personal privacy. This risk is increased if wireless communication technology is used without adequate protection.

This fact sheet is intended to address privacy issues that arise from the use of wireless communication technologies. The standard established in Order HO-005 is that health information custodians in Ontario should not use wireless video surveillance cameras without strong security and privacy precautions. Any organization that chooses to use wireless communication technology to transmit personally identifiable information needs to take appropriate proactive measures to protect the privacy of individuals.

What is wireless video surveillance technology?

Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to television monitors, not computer screens. The most common commercial use of this equipment is for building security. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but will allow unauthorized access unless special precautions are taken. Health information custodians must ensure that no one other than specifically authorized staff have the capability of viewing patient images.

Wireless transmissions like CCTV broadcasts are inherently subject to interference and interception, especially when they use publicly available frequency bands. CCTV signals are generally not encrypted or secured, and may easily be captured by others with an appropriately tuned receiver. As there are only a limited number of transmission channels, the chances of inadvertent interception are quite high.

How can you secure the system?

As a general rule, wired solutions are more secure than wireless solutions due to the reduced likelihood of interception. Given that wired systems are enclosed in a physical casing, the signals transmitted within cannot be freely broadcast into the air waves. If a wired solution is not available, or if wireless is required for some other purpose, then a health information custodian is responsible for ensuring that the security provisions of the system meet privacy requirements. For example, any vendor selection process for wireless video systems must require signal protection so that patient images, if intercepted by third parties, cannot be viewed. The best way currently available to prevent the viewing of intercepted messages is by utilizing an encrypted, or scrambled, signal.

Internet Cameras (webcams)

Webcams, or Internet cameras, are an alternative to CCTV, but significantly raise the risk of inadvertent disclosure. Such cameras can be attached by wire, or wirelessly linked to a local computer network, and may make their video signal available as a streaming video website. While the advantages of using existing computer systems are clear, including the possibility of not requiring extra monitors, the risks are also substantially greater.

Unless the website of each camera is designed properly AND securely, overly broad access may become an issue. Since the video signal will be made available through a web browser, anyone with a computer connected to the network may become an unauthorized user of the data. If the network is publicly available, then the images would be available from anywhere on the web. Each IP camera's website must be protected by up-to-date encryption standards, and key management practices should be in place to ensure that only authorized individuals may view the video.

The use of wireless communications technology, such as the wireless CCTV camera which precipitated Order HO-005, is increasing as the underlying technologies become less expensive and more widespread. While this fact sheet has focused on wireless CCTV transmissions, there are numerous privacy concerns regarding the use of a broad range of wireless communication technologies that will be addressed in a second wireless fact sheet.

Conclusion

While the precipitating incident for this fact sheet occurred in the health care sector, and the accompanying Order is specific to a methadone clinic, the necessity to protect personal information collected by CCTV is a general requirement. The use of video surveillance and wireless transmission equipment requires due diligence and end-to-end care, commensurate with the sensitivity of the images captured. Especially when video images of any kind are to be used in a health care setting, the highest security precautions must be taken to protect patient privacy.

Other requirements

- Even when explicit consent is obtained from patients, special precautions must be taken to protect the privacy of video images.
- No covert surveillance should be conducted.
- Clearly visible signs should be posted, ensuring that patients are aware of the existence of video cameras.
- Where video cameras are used in private areas, such as washrooms, there should be a very visible indicator that the camera is in use.
- Where video cameras are used for purposes of observation only, recording devices should not be used.
- Only the minimum number of staff necessary should be allowed access to the video equipment.
- Staff should receive special technical training on the privacy and security issues involved with the use of video surveillance equipment, and the sensitivity required in such settings.
- Regular security and privacy audits should be conducted on an annual basis.

Checklist for Video Surveillance Systems

- ✓ Conduct a privacy impact assessment on the proposed video surveillance system, ensuring that all privacy requirements are identified and met.
- ✓ Confirm that security and privacy requirements are explicit in any procurement process.
- ✓ Confirm that the signal cannot be intercepted or received by anyone other than the authorized individuals on authorized devices.
- ✓ Confirm that the video camera will be off at all times except when used for designated purposes.