

Security of Mobile Devices

Issued October 2007

The College of Physicians & Surgeons of Alberta provides [Advice to the Profession](#) to support the implementation of the [Standards of Practice](#). This information does not define a Standard of Practice nor should it be interpreted as legal advice.

This information is designed to aid practitioners in making decisions about appropriate care. This document does not define a standard of care nor should it be interpreted as legal advice. Variations in practice may be warranted based on the needs of the individual patient resources, and limitations unique to the institution or type of practice.

Introduction

This document has been established to provide advice to physicians in light of recent OIPC investigations regarding security of laptop computers and to reflect current best practices of the security of mobile computing devices.

Key Messages

- It is not acceptable to store identifiable patient information on a mobile device without adequate security.
- Security of mobile devices is a serious issue but the risks are almost totally manageable.
- This is a known issue with potentially serious harm to patients, and serious consequences to the physician in the event of a security breach.
- Security is only as good as its weakest link. Solutions must be a layered defense which includes planning, protection of the device, and appropriate management of the data on the device.

Background

Mobile computing devices offer convenience and flexibility to store health information as well as enabling remote access to medical records. Mobile devices can include portable computers (such as laptops, notebooks, PDAs, SmartPhones, etc.) as well as portable storage devices (such as USB flash drives, CDs and DVDs, floppy drives, backup tapes or drives, etc.).

Health information is inherently sensitive with potential for serious harm and warrants due consideration and care when stored or is accessible with mobile devices. The theft and loss of mobile computing devices, in particular laptops, is a known and publicized hazard and has been the subject of recent OIPC investigations in Alberta ([P2006-IR-005](#), [H2006-IR-002](#)) as well as other jurisdictions and is considered an almost totally preventable issue.

Physicians have both a legal and ethical duty to protect health information in their custody including controlling against any reasonably anticipated threat or hazard to its security or integrity. The *Health Information Act* has defined accountabilities and penalties for inadequate protection, and physicians could face embarrassment, legal action and other consequences as a result of such failures. Adequate security includes having sound policies and practices in place for administrative, technical and physical safeguards of that information, as well as ensuring the awareness and adherence of those policies and practices by your affiliates. There are readily-available and cost effective products for the majority of defined security risks for laptops and most other devices.

The accepted standard of practice for security is the ISO 17799 standard which involves the deployment of layers of security – administrative, physical and technical – to minimize the risk and exposure of mobile equipment in unprotected environments. At minimum, physicians should have policies and procedures for:

- security awareness
- physical device protection
- password management and access control
- data protection including encryption, backups and virus protection
- transmission of data using unsecured communication.

As is the case in all security matters, a strategy must strike a balance of the benefits of the use mobile devices, the risk and impact of misadventure, and the cost and operational impact of the security to develop an appropriate solution. The obvious risks should take precedence, followed by more detailed and comprehensive solutions.

Security Awareness & Training

The key administrative components of the security strategy include an assessment of risk, the development and adoption of policies and procedures, and training. An awareness of the issue and keeping yourself (and your staff) up to date on tools and practices is essential.

Security is only as good as the weakest link in the chain. Policies and training have natural limitations, which indicate that technical safeguards are also necessary. There should be a conscious and detailed risk assessment when health information is stored or accessible using mobile devices including a deliberate and prudent evaluation of the:

- foreseeability of the security risks and likelihood of loss/damage,
- seriousness of the potential harm and
- relevant standards of practice to address the risks.

Understanding the planned use of the device is critical. Examples of questions that may be considered:

- Who will have access to the device and how will access be controlled?
- Where and how will the remote device be used, and under what circumstances?
- What information is needed on the remote device for the defined use, and in what detail?
- Is the storage in the device removable, and how can it be accessed?
- Is storage on the mobile device the appropriate solution, versus a communication protocol (such as a virtual private network) to a more secure storage location?
- How and when will information loaded or collected on the device be synchronized with the medical record?
- How will a record be kept of what information is on what device?
- Will there be transmission of information over a network?
- Does the device enable access to the medical record or other remote applications, and what exposure does the device create to those applications?

Upon completion of the risk assessment, the development of policies and procedures, as well as individual training is required:

- Protection against physical theft, loss or damage of the device
- Storage and management of passwords
- Storage of account information (for remote access)
- Procedures for managing information on the device (including encryption)
- Procedures for the use of wireless transmission
- Procedures in the event of a security breach

Physical Protection of the Device

Maintaining physical possession and control of the device is an obvious and fundamental protection. When the device is not in your direct control (i.e. your laptop computer in your office while you are seeing patients in an examination room) you should take measures to protect the device from theft or misuse. Laptops can be physically secured to immovable objects using cable locks, and most devices can be placed in locked desks or cabinets.

Laptop theft is relatively common and an easy target for thieves, particularly if the carrying case is an obvious computer case. Traveling presents additional risks – theft of computers from vehicles is very common, as are thefts from hotel rooms and security check-ins at airports. Never leave a device unattended and always have a line of sight to your bag. Having your ownership identification engraved or attached can be valuable in the case of a lost item – if someone finds it they can return it and reduce the risk and uncertainty about the loss.

Devices also need the protection against digital attacks such as viruses, spyware and hackers. Firewalls, anti-virus, operating software security patches are all important protections against these kinds of malicious threats. Given the dynamic nature of electronic threats, it is critical to keep these products current using regular scheduled updates or realtime update protocols.

When a device is to be retired, all storage capacity should be physically destroyed or “wiped clean”. Data that is “deleted” usually just has the index value deleted and the data remains on the disk until that space is reused. A wiping process physically re-formats the storage area.

Data Protection

The first line of data protection is to limit the amount that is stored on the mobile device. Only store the information that is needed, and delete it when it is no longer needed on the device.

Passwords and other authentication are effective in many circumstances but the information is still exposed if someone has access to the device. For example, a person can install a new operating system on the computer, start-up, log on, and access the data. The storage within the device can also be removed and installed in another device. **Protecting the data through encryption is the most effective method of security for mobile devices.** If the data is encrypted with current encryption products, only the most dedicated of efforts would expose the data to malicious use. It is critical to protect the security of the encryption keys (the encoded value used to encode and decode the source data) and to keep them physically separate from the device.

Data and encryption keys stored on a mobile device should have a backup or a copy stored in a different location to prevent the permanent loss a medical record or information. Such backup copies should also be encrypted, and stored with appropriate physical security.

Password Management and Access Control

In the event that someone gains physical access to the device, there should be some level of access control enabled on the device. Limiting access to the device can include logon control and passwords, device controls, access control for files and data.

Passwords are a simple and basic control and should be used to authenticate the user to control the initial access to the device. Passwords should be “strong passwords”, those that are made up of a combination of letters, numbers and symbols that make it difficult for individuals or password-guessing programs to guess or decipher. Passwords should be changed regularly, and should never be accessible with or near the device. Passwords to accounts accessible from the device should also have the same protection to ensure that the device cannot be misused to access those accounts.

Passwords can be replaced with biometric devices as an additional security device to have a stronger level of authentication. Computers should be configured so that the start-up sequence cannot be overridden or bypassed. Auto-logons from a start-up sequence are a serious exposure that enables access to the file-sharing system in a device, bypassing the need for account credentials and passwords – this functionality should never be enabled.

Data Transmission

Ideally, information (including emails, websites, messages, etc.) communicated using unsecured networks should also be encrypted; at a minimum, password protection of emails should be used. Care should be taken that cached data or temporary files are not left in unsecured or unencrypted areas of storage. It is important to note that transmitted data (emails, faxes, messages, etc.) is often legitimately stored, cached or mirrored by service providers and/or corporate servers en route to the intended recipient – care must be exercised that unencrypted data is not exposed to these sources.

Wireless networks require explicit strategies to ensure that network access is limited to legitimate users and/or devices, and that data is encrypted during transmission.

Security Breaches

Security programs should include a process to monitor activity to identify that a security breach may have occurred. In the event of a security breach, immediate action is required and should follow a defined procedure. The CPSA has published advice in the event of lost or stolen patient records:

([http://www.cpsa.ab.ca/Libraries/Res_Advice_to_the_Profession/Lost or Stolen Patient Records.pdf](http://www.cpsa.ab.ca/Libraries/Res_Advice_to_the_Profession/Lost_or_Stolen_Patient_Records.pdf)).

Conclusion

Security is only as good as the weakest link and requires a layering of defenses. It must start with preparedness and planning, and must include the protection of the devices as well as technical measures on the device itself. Given the inherent risks associated with mobile devices, care should be taken to limit the information stored on the device to that which is necessary, and the information should be purged from the device when it is no longer needed on the device. At the end of the useful life of the device, adequate care is necessary to wipe or destroy the information.

Encryption is the best and final defense, and must be a necessary component of any security strategy!