cpsa
COLLEGE OF PHYSICIANS & SURGEONS OF ALBERTA

ADVICE TO THE PROFESSION

Electronic Communications & Security of Mobile Devices

The College of Physicians & Surgeons of Alberta (CPSA) provides advice to the profession to support physicians in implementing the CPSA Standards of Practice. This advice does not define a standard of practice, nor should it be interpreted as legal advice.

Advice to the Profession documents are dynamic and may be edited or updated for clarity at any time. Please refer back to these articles regularly to ensure you are aware of the most recent advice. Major changes will be communicated to our members; however, minor edits may only be noted within the documents.

Contents

Duty of Custodians 1
Privacy Impact Assessment 2
Security of Mobile Devices 3
- Considerations 4
- Physical Protection 5
- Virus Protection 5
- Data Protection 6
- Password Management and Access Control 6
- Electronic Data Transmission 7
- Patient Consent 7
- Security Breaches 8

Conclusion 8

Duty of Custodians

Regulated members have both a legal and ethical duty to protect the health information in their custody. Under Alberta's *Health Information Act* (*HIA*), custodians must take reasonable and appropriate measures to protect the security and confidentiality of their records, including addressing the threats and risks to patient information that is collected, stored or transmitted via electronic means.

cpsa
COLLEGE OF PHYSICIANS & SURGEONS OF ALBERTA

ADVICE TO THE PROFESSION

Electronic Communications & Security of Mobile Devices

Important to Know

- When communicating electronically with patients, colleagues or other healthcare providers, safeguards should be commensurate with the sensitivity of the health information.
- 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.
- A security breach may result in serious harm to patients and serious consequences for the regulated member.
- Security is only as good as its weakest link. Solutions require a layered defense which includes planning, protection against physical and digital threats and appropriate data management.

Note: Regulated members involved with other healthcare delivery organizations/institutions (e.g., Alberta Health Services) also have a responsibility to be aware of and follow that organization's/institution's policies regarding the use, storage and transmission of confidential health information.

Although the day-to-day responsibility of managing these safeguards may be delegated to an affiliate (person who performs services for a custodian) or Information Manager, it is the individual custodian who bears ultimate responsibility for the protection of the health information.

The key administrative components of a security strategy are threat-risk assessment, the development and adoption of policies and procedures to mitigate threats, and risks and training. Awareness of the issue and keeping yourself (and your staff) up-to-date on tools and practices is essential.

Privacy Impact Assessment

Under the *HIA,* a regulated member who is a custodian is required to complete a Privacy Impact Assessment (PIA) and submit it to the Office of the Information and Privacy Commissioner (OIPC) prior to implementing any administrative practice or information system relating to the collection, use and disclosure of individually identifiable patient health information. The purpose of the PIA is to demonstrate due diligence in identifying and addressing privacy and security risks within the custodian's context, including the:

- foreseeable security risks

- likelihood of loss/damage
- seriousness of the potential harm
- reasonable (not exhaustive) measures to address the risks

Some situations that don't introduce any new potential risk may not require a new PIA (e.g., an office move, upgrade to a computer system or software, bug-fixes that don't add functionality). In these cases, an internal privacy threat-risk assessment is still required.

For more information on PIA requirements, visit the OIPC website.

Security of Mobile Devices

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 accessible on 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 OIPC investigations in Alberta as well as other jurisdictions, and is considered almost entirely preventable.

The *HIA* 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 procedures in place for administrative, technical and physical safeguards, as well as ensuring the awareness and adherence to those policies and procedures 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 deployment of layers of security – administrative, physical and technical – minimizes 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
- secure transmission of data

As in all security matters, the benefits of the device or system, the risks and impact of misadventure and the costs and operational impacts of risk mitigation must be balanced in developing a solution. The obvious risks should be addressed first, followed by more detailed and comprehensive solutions.

CONSIDERATIONS

Regulated members are responsible for managing the security of the electronic messages on their devices and systems. Understanding the planned use of the device is critical. Questions to consider:

- 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?

Once threats and risks are understood, policies, procedures and training requirements should be identified:

- 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
- Training to ensure all staff who have access understand security policies and procedures

PHYSICAL PROTECTION

Maintaining physical possession and control of a device is an obvious and fundamental protection. When the device is not in your direct control (e.g., your laptop computer remains 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 a locked desk or cabinet.

Laptops are 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 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.

VIRUS PROTECTION

Devices also need protection against digital attacks such as viruses, spyware and hackers. Firewalls, anti-virus software and 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 real-time update protocols.

Electronic Communications & Security of Mobile Devices

DATA PROTECTION

The first line of data protection is to limit the data stored on the mobile device. Only store the information that is needed, and remove it when no longer needed on the device. However, all communications that pertain to patient care must be retained in the patient record as per the *Patient Record Content* standard of practice. This includes email messages and text messages sent and received by mobile device.

The OIPC recommends encryption as the best technical protection for data. While passwords and other authentication are effective in many circumstances, it's important to understand unencrypted information is still vulnerable if someone gains access to the device. For example, a person could install a new operating system on the computer, start-up, log-in and access the data. The storage within the device could also be removed and installed in another device.

If the data is encrypted with current encryption products, only the most dedicated of efforts will 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 of a medical record or information. Backup copies should also be encrypted, and stored with appropriate physical security.

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.

PASSWORD MANAGEMENT AND ACCESS CONTROL

In the event an unauthorized person gains physical access to the device, there should be some level of access control enabled on the device. This could include login control and passwords, device controls and access control for files and data.

Passwords are a simple and basic control to authenticate a user seeking access to the device. Passwords should be strong, made up of a random combination of letters, numbers and symbols difficult for individuals or password-guessing programs to guess or decipher. Passwords should also be changed regularly and should never be accessible with or near the device. Passwords to accounts accessible from the device should have the same

protection to ensure the device cannot be misused to access those accounts. Passwords can be replaced with biometric devices to provide a higher level of authentication.

Computers should be configured so the start-up sequence cannot be overridden or bypassed. Auto-login from a start-up sequence is 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.

ELECTRONIC DATA TRANSMISSION

Regulated members should take due care to manage the content of electronic transmissions (including email, text messages, etc.) with patients, medical colleagues and other healthcare providers. The OIPC recommends that information transmitted via unsecured networks be encrypted; at a minimum, emails should be password protected. See OIPC's Practice Note #5: Communicating with patients via email – know the risks

Cached data and temporary files should not be left in unsecured or unencrypted areas of storage.

It is important to understand that while email may be secure within the physical confines of a facility, it may not be secure if accessed remotely or wirelessly. Wireless networks require explicit strategies to ensure network access is limited to authorized users and/or devices, and that data is encrypted during transmission.

Transmitted data (emails, faxes, messages, etc.) are often retained and remain accessible on intermediary servers (e.g., service provider, corporate servers) en route to the intended recipient; care must also be taken to encrypt data that may be exposed to these sources.

PATIENT CONSENT

The OIPC advises that patient consent to use electronic transmission (e.g., email, text messages) **does not** relieve a custodian of their legal duty to protect the confidentiality of patient information. The *HIA* allows individuals to consent to certain disclosures of their health information; however it does not include a patient's right to consent to how their health information is collected, managed, stored or secured. Therefore, a patient cannot consent or otherwise waive the responsibility of the custodian to adhere to the *Act*.

SECURITY BREACHES

As part of their PIA or internal threat-risk assessment, custodians should have a process for monitoring activity and identifying potential security breaches. In the event of a security breach, immediate action is required and should follow a defined procedure. See Advice to the Profession – Lost or Stolen Patient Records

As well, physicians have a duty to report any loss of, unauthorized access to, or disclosure of individually identifying health information by themselves **or** their affiliates to the Commissioner, the Minister, and the individual who is the subject of the information.

For more information, please see the OIPC's "How to Report a Privacy Breach" and AH's "Duty to Notify" documents.

Conclusion

Security is only as good as the weakest link and requires a layering of defenses. It starts with awareness and planning, and must include physical protection of devices as well as technical measures to safeguard against unauthorized access. Given the inherent risks, care should be taken to limit the information stored on mobile devices 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.

RELATED STANDARDS OF PRACTICE

- *Disclosure of Harm*
- *Patient Record Content*
- *Patient Record Retention*
- *Responsibility for a Medical Practice*

COMPANION RESOURCES

- Advice to the Profession documents:
  - Legislated Reporting & Release of Medical Information

  - Lost or Stolen Patient Records
  - Physicians as Custodians of Patient Records
  - Social Media
- OIPC:
  - 8 Tips for Managing Emails
  - Communicating with Patients via Email: Know the Risks
  - Email Communication FAQs
- CMPA's Smart Phone Recordings by Patients