THE COLLEGE OF FAMILY PHYSICIANS OF CANADA

LE COLLÈGE DES MÉDECINS DE FAMILLE DU CANADA

Canada Health Infoway

Inforoute Santé du Canada

BEST ADVICE

Advanced and Meaningful Use of EMRs

MODULE 4

Privacy and Security

NOVEMBER 2018

In the digital era, the onus is on family physicians to inform ourselves about privacy and security issues related to electronic medical records (EMRs), as well as all other technologies used to communicate personal health information (PHI). While there are numerous benefits to using EMRs, the potential for privacy breaches has increased exponentially over recent years.

EMRs have multiple access points (e.g., computers, tablets, and smartphones; email, third-party software, etc.), resulting in numerous potential vulnerabilities. Therefore, physicians must ensure they are meeting the requirements for securing PHI in the electronic world.

Most physicians feel confident in their practice of medicine. However, these new technologies represent an area that they may feel much less adept to handle.

To help physicians address these issues, many organizations have created recommendations and guidelines. Unfortunately, the plethora of recommendations—sometimes with conflicting suggestions—can leave physicians feeling bewildered and trying to navigate an unfamiliar world. To complicate matters further, current guidelines exist at multiple geographic and jurisdictional levels (see Table 1), and most physicians will find that multiple recommendations apply to them.

This guide focuses at the national level. However, physicians should also familiarize themselves with relevant recommendations at provincial and local levels.

Table 1: Examples of organizations creating guidelines on privacy and security

National	College of Family Physicians of Canada (CFPC) Royal College of Physicians and Surgeons of Canada (Royal College) Canadian Medical Protective Association (CMPA) Canadian Medical Association (CMA)
Provincial	Colleges of physicians and surgeons Privacy commissioners Provincial medical associations
Local	Health care institutions Employers

DEFINITIONS

Privacy: The right to control access to one's person and information about one's self. The right to privacy means that individuals can decide what and how much information to give up, to whom it is given, and for what uses.[1]

Security: The mechanisms by which confidentiality policies are implemented in computer systems, including provisions for access control, integrity, and availability.[2]

Confidentiality: The assurance that information about identifiable persons, the release of which would constitute an invasion of privacy for any individual, will not be disclosed without consent except as allowed by law.[2]

PRACTICAL CASE

A physician works in an office with three other physicians, two nurses, and four administrative assistants, all using an EMR system. If everyone only accessed the EMRs when physically in the office, all of the computers were encrypted and protected, and the backups were all secure, this would be a relatively easy system to secure.

Now consider the following, which outlines a more typical use of technology:

- The home computer or laptop is used to access EMRs, and is backed up to the cloud or a hard drive
- A smartphone is used to access EMRs or communicate with patients, and is backed up to the cloud or a home computer
- Emails are sent to patients from any device (computer, tablet, smartphone) using an unsecure email account (e.g., Yahoo, Gmail, Hotmail, etc.)
- Another messaging format (e.g., text messaging, social media, etc.) is used to communicate with or about patients
- An IT service provider helps you with computer problems, sets up new computers, etc.
- A billing clerk deals with billing and accesses EMRs
- A third-party service provider supplies additional functionality (e.g., self-booking kiosk, tablets for patients to use that integrate with EMRs, etc.)

What should you take into account regarding privacy and security?

PRIVACY AND SECURITY CONSIDERATIONS

THE BASICS

- Ensure all users understand security as it relates to their role and obligations
- Select strong passwords and protect them from disclosure
- Never use another person's user ID or password
- Always lock your computer when you are away from it
- Install a privacy screen over your monitor to make it difficult for visitors to read the contents displayed
- Wear ID badges at work when they are supplied and question anyone without a badge to ensure they are authorized personnel

HARDWARE AND SOFTWARE

- Ensure that computer hard drives are encrypted
- Store PHI on a secure, shared drive only, not on individuals' computers
- Ensure data connections are secure
- Install firewalls and anti-virus software
- Install software updates and patches automatically, or in a timely manner
- Do not install unauthorized software of any kind
- Do not visit gambling or online gaming websites, or sites intended for adult-only audiences
- Scan computers weekly to ensure that spyware and unauthorized software is not installed

MOBILE DEVICES

This includes, but is not limited to, laptops, tablets, and smartphones.

- Do not store PHI on these devices; includes emails with patients, notes to self, or images that can identify patients
- Ensure mobile devices are encrypted and can be wiped remotely
- Secure laptops with a physical cable lock when using them in public places
- Ensure that mobile devices are backed up (e.g., to iCloud, Google Cloud, etc.), and that the backups are encrypted and secure
- Use strong passwords (e.g., combination of upper and lower case, numerals, and symbols) and change them regularly
- Ensure that firewalls and anti-malware are installed and activated

PHYSICAL VERSUS CLOUD STORAGE FOR EMR DATA

- Local physical server
  - Ensure the connection to the EMR is secure
  - Ensure the server is housed in a secure location, with an off-site backup
  - Ensure that an agreement is in place to govern privacy and confidentiality when using third parties to manage servers
- Cloud storage (application services provider (ASP) model)
  - Ensure secure communication lines are used for data in transit
  - Ensure cloud storage and backups are located in Canada; international locations are subject to those jurisdictions' privacy legislation (vendors should be aware of this)
  - Ensure you understand how the cloud storage is managed, and what your rights are with respect to your stored data:
    - Is the storage private or shared?
    - Who manages the infrastructure?
    - What are the service provider's information management and security practices?
    - Who can access the data?
    - Has a privacy impact assessment been done?
    - Can you detect privacy breaches?
    - Is a signed privacy and confidentiality agreement in place?
    - Can all data be permanently deleted, including backups, if you choose to change models?

BACKUPS

- Make regular backups of your data at least weekly (preferably daily), and keep them off-site
- Verify at least twice a year that data can be restored from the backups
- Keep all paper files and backup media in a fireproof container
- Backup of physical server

- Ensure the backup server is in a secure location away from your primary server
- Ensure the connection is secure
- Set up automatic backups

- Backup of cloud storage
  - Ensure you understand the practices of your cloud storage:
    - Are backups conducted?
    - How many copies are created?
    - Who owns the backups?
    - Do backups occur automatically?
    - Is the backup tested periodically?

EMAIL AND SECURE MESSAGING

- Emails with patients
  - Consider the benefits of having patient consent, preferably written, for electronic communications
  - Use a secure email account on an encrypted device, or alternatively send secure messages through a patient portal
  - Where are these emails stored? Will they be on various portable devices and computers, or is there a process to delete them from the email server?
  - Include the following information in email signatures or footers:
    - A statement that the email content is confidential
    - Instructions for handling emails received in error
    - Recommendations that those receiving emails use only secure email addresses that are password protected
  - Ensure there is a process to confirm that email addresses are up to date
  - Ensure there is a process to include emails in the patient's medical record
  - Have documented policies and procedures in place regarding electronic communications, and ensure that all staff and patients are aware of them

- Emails with other providers
  - If emails contain PHI, ensure senders and receivers use secure email accounts

Other forms of electronic communication (e.g., text messaging, social media, etc.) are not included here as they are considered insecure for communicating PHI. In addition, it is challenging to incorporate communication from these tools into the patient's EMR.

THIRD PARTY VENDORS INTERACTING WITH EMRS

Many offices engage outside vendors to help manage their EMR software, hardware, Internet access, servers, and office infrastructure. Vendors who access PHI should be familiar with data handling procedures, as well as privacy and security requirements.

- Potential parties
  - IT support personnel
  - Billing personnel
  - Additional functionality (e.g., patient self-booking software)
  - Labs
- Considerations
  - Is a data sharing agreement required, and in place?
  - Has a privacy and confidentiality agreement been signed?
  - Do the third parties access data in a secure manner?
  - Is any PHI stored elsewhere?

EDUCATION AND AWARENESS FOR CLINICAL AND NON-CLINICAL STAFF

- Ensure a privacy policy (and related procedures) for all staff is in place
- Ensure all staff take privacy and security training, both at the time of hiring and on an ongoing basis
- Designate a privacy officer
- Ensure confidentiality and end-user agreements are signed by all staff
- Ensure a process is in place for managing access only to data relevant to each staff member's role
- Ensure a process is in place for removing access when an employee leaves
- Ensure an audit process is in place for EMR data

PRIVACY BREACH MANAGEMENT

MANAGEMENT

- Is there a policy for managing a breach of PHI?
- Is a policy in place for managing a lost device (e.g., smartphone or laptop)?
  - The policy should include the ability to remotely deactivate and wipe the device immediately, and report to the telecom provider

CYBER INSURANCE

Undoubtedly, implementing these safeguards is challenging for busy clinicians. While there is no substitute for due diligence, there is an emerging need for insurance coverage in case something goes awry. Even the strictest policies and procedures cannot guarantee that hackers will be prevented from accessing either EMRs or a related device. Cyber insurance, a relatively new product, can help manage these risks and is considered a worthwhile investment by many people.

THE BIG PICTURE

There is no question that EMRs are here to stay. There is also no question that the complex privacy and security requirements for safeguarding these systems can produce stress and anxiety for family physicians.

Physicians are generally not well trained about information technology and its related issues. However, we are compelled to exercise due diligence in order to fulfill our professional obligation to maintain confidentiality. This module provides an overview of the privacy and security issues to consider, particularly as we see a shift toward team-based care in the Patient's Medical Home practice setting, and potential for privacy breaches across multiple access points of EMRs for sharing patient data. For more detailed information, consider the following national resources, in addition to your provincial/local jurisdictional guidelines.

PRIVACY AND SECURITY RESOURCES

CANADIAN MEDICAL PROTECTIVE ASSOCIATION (CMPA)

- The ransomware threat: Are you prepared?
- Using electronic communications, protecting privacy
- Protecting patient health information in electronic records
- Sample form: Consent to use electronic communications
- Electronic Records Handbook

CANADA HEALTH INFOWAY (CHI)

- Privacy and Security Requirements and Considerations for Digital Health Solutions
- Data sharing agreements and the interoperable digital health record: A discussion paper

CANADIAN MEDICAL ASSOCIATION (CMA)

- Guiding principles for physician electronic medical records (EMR) adoption in ambulatory clinical practice
- Data sharing agreements: Principles for electronic medical records/electronic health records
- Guiding principles for the optimal use of data analytics by physicians at the point of care

ACKNOWLEDGEMENTS

Thanks to Ms. Abigail Carter-Langford (Chief Privacy Officer, Infoway) and Ms. Nancy Cahill (Manager, Privacy Initiatives, Infoway) for their input on and contributions to this document.

References

1. Cavoukian A. *Privacy by Design: From Rhetoric to Reality*. Toronto, ON: Information and Privacy Commissioner of Ontario; 2012.
2. O'Carroll P, Yasnoff W, Ward M, Ripp L, Martin E, eds. *Public Health Informatics and Information Systems*. New York, NY: Springer Science & Business Media; 2006.