Guidelines for Protecting Medical Records Outside the Practice

This section will identify best practices for protecting medical records outside of the practice.

Physicians have a legal and ethical obligation to respect patient confidentiality and to protect personal health information. The CMA Code of Ethics requires physicians to protect the personal health information of their patients. PIPA requires that physicians take reasonable measures to protect patients' personal information from risks of unauthorized access, use, disclosure and disposal and sets out consequences for violation. The Information and Privacy Commissioner has described reasonableness as "the measure by which security measures are objectively diligent and prudent in the circumstance" and stated that "what is 'reasonable' may signify a very high level of rigour depending on the situation."

Protecting Medical Records Outside the Practice

There are times when physicians and their staff may need to access personal information remotely while travelling, at home or in another location. This includes transporting records by car or airplane, working from home, attending meetings or conferences or making visits to a patient's home. The personal information may be stored in paper records or on portable electronic devices such as laptops, CDs, DVDs, external hard drives, USB storage devices, handheld electronic devices and smart phones. With EMRs and other forms of electronic communication, physicians and their staff are also able to connect to their practice network and may have access to sensitive personal health information from anywhere in the world.

Physicians must implement reasonable safeguards, including administrative, physical and technical measures, to reduce the privacy risks of accessing personal health information outside the practice.

Conversations

When having conversations outside the practice:

- Avoid discussing a patient's personal health information in public areas such as on elevators, in stairwells, while travelling by public transit or airplanes, in restaurants or on the street.
- Avoid using cell phones to discuss a patient's personal health information while in transit as these conversations can be intercepted or overheard.
- Use a dedicated phone line with password protected voicemail when working from home.

Paper Medical Records

When using paper medical records:

- only remove medical records from the practice when it is absolutely necessary for performing job duties
- require all staff to obtain approval from their supervisor before removing medical records from the practice
- use a sign-out sheet to document who is removing a medical record, the name of the individual whose personal information is being removed, and the date the record is being removed
- leave the originals in the practice, if possible
- take only the minimum amount of personal information required to perform the task
- if the records are large, consider using a courier to transport them to their destination
- place records in confidential folders, transport them in a secure container, and keep them under control at all times, including meal and break times
- keep records locked in a desk drawer or filing cabinet when working from home to reduce unauthorized viewing and access by family members or friends
- if transporting medical records by car, keep them locked in the trunk before the start of the trip
- never:
    - leave medical records unattended, even if they are stored in the trunk as these are no less accessible to thieves than the front seats
    - examine medical records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit)
    - leave medical records open for view in hotel rooms (e.g., keep them in the hotel safe)
- immediately return medical records to their original storage location upon returning to the practice
- securely destroy any copies that are no longer required

Portable Devices

When accessing medical records on portable electronic devices:

- Avoid storing personal information on portable electronic devices unless absolutely necessary.
- PIPA requires that any personal information stored on a portable electronic device must be protected by industry-standard encryption.
- Wireless transfer of personal information or storage on cloud-based programs must also be protected by industry-standard encryption.

- Protect portable electronic devices containing personal information with a strong password and use a secure method, such as two-factor authentication, to grant user access.
- Keep portable electronic devices secure to prevent loss or theft (e.g., in a locked briefcase, desk drawer, container or room) and keep them under one person's control at all times, including meal and break times.
- If transporting portable electronic devices by car, lock them in the car trunk before the start of a car trip.
- Never leave portable electronic devices unattended, even if stored in the trunk.
- Remove all sensitive personal information when no longer needed from portable electronic devices using a digital wipe utility program (do not rely on the delete function as the information may still remain on the device).

Electronic Records

When accessing medical records on home computers or portable electronic devices:

- Avoid storing any personal information on the hard drive of a home computer.
- Never:
    - use public computers or wireless networks to connect to the practice network as these are not secure
    - use a laptop or home computer that is shared with other individuals, including family members and friends
    - send documents containing personal information to or from a personal or otherwise unsecured email address
- Always:
    - log off from a laptop or home computer when not in use
    - set an automatic log out to occur after a period of inactivity
    - lock home computers that are used for work-related purposes to a table or other stationary object with a security cable
    - keep home computers in a room with restricted access
    - use strong, up-to-date, industry-standard encryption and password protection for any personal information that must be stored on hard drives
    - ensure that laptops and home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection
    - ensure the latest updates and security patches are regularly installed

- use an encrypted link to the host network, such as a virtual private network (VPN), when conducting business involving personal information over a network
- watch out for “shoulder-surfing” where family members or friends may casually observe the screen of the laptop or desk computer

For more information, see Protecting Personal Information Away from the Office.