Protecting Patient Information in and outside of the Office

This section will:
• Define safeguards for protecting patient records. • Identify best practices for protecting paper and electronic records. • Describe reasonable practices for protecting personal information outside of the office.

Safeguards are a combination of policies, processes, practices, and technologies that are intended to protect personal information. Regardless of how personal health information is recorded—whether on paper or electronically—appropriate and reasonable safeguards are necessary to ensure that privacy is protected and confidentiality is maintained.

Physicians have an ethical obligation to respect patient confidentiality, and the CMA Code of Ethics requires physicians to protect the personal health information of their patients. The Personal Information Protection Act (PIPA), requires physicians to take reasonable measures to protect patients' personal information from risks of unauthorized access, use, disclosure and disposal, and sets out the consequences for violation. In a report published in 2006, the Information and Privacy Commissioner for BC 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 Records in the Office

Patient records must be handled in a secure manner from the time the records are created to the time they are disposed of, regardless of the format upon which the information is stored.

The following guidelines should be considered and incorporated into the implementation plans for safeguarding patient records and any other personal information stored in the practice. Note that a combination of measures may be required during the transition from paper-based patient records to Electronic Medical Records (EMRs) where both methods of record-keeping may be maintained in parallel.

Staff[1] working in physician practices should:

1. Lock doors and cabinets where patient records are stored.
2. Wear building passes/photo ID if issued.
3. Query the status of strangers.
4. Know whom to inform if suspicious behaviors are noticed
5. Not tell unauthorized individuals how security systems operate.
6. Sign confidentiality agreements that specify obligations and expectations including repercussions for inappropriately collecting, using, or disclosing personal information.

Paper records should be:

1. Formally booked out from the normal filing system.
2. Tracked, if transferred, by confirming that the records arrived at their specified destination.
3. Returned to the filing location as soon as possible after use.
4. Stored securely within the clinic or office.
5. Placed in a location where members of the public cannot view the contents.
6. Not left unattended at fax machines or photocopiers.
7. Held in secure storage with clear labelling.
8. Kept on-site wherever possible. If the records must be taken off-site, they must be kept secure at all times.

With Electronic Medical Records (EMRs), staff should:

1. Log out of computer systems or applications when not in use or unattended.
2. Keep workstations positioned away from public view and access.
3. Not share an assigned user ID and password with others. If other staff members need to access the EMR, authorized access should be granted.
4. Not write down passwords.
5. Revoke user IDs and passwords as soon as authorized users resign or are dismissed.
6. Install firewall software where Internet access to computer systems exists.

[1] Staff include locum physicians, associates, visiting specialists, physicians-in-training, contractors, volunteers, and residents with whom you collect, use, or disclose personal information.

7. Ensure that data backup methods and disaster recovery plans are in place and periodically reviewed.

EMRs should provide:

1. A unique user ID and password for every authorized user.
2. Access to patient information on a "need to know" basis under a roles-based access model that determines whether the user has the necessary authorization and permissions.
3. Audit trails to track when a patient record is accessed, by whom, including date and time.
4. Enforced password changes at regular intervals.
5. Ability to easily manage user accounts (create, modify, revoke).
6. Password protected screensaver or auto log out after a period of inactivity to avoid unauthorized viewing.

Protecting Personal Information outside the Office

There are times when physicians and their staff may need to work with personal information while travelling, at home, or at another location. This includes transporting records by car or airplane, working from home, attending meetings or conferences, or making visits to a patient's or a client'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); however with the movement toward Electronic Medical Records (EMRs) and other forms of electronic communication, physicians and their staff are also able to connect to their office network, and therefore may have access to sensitive personal health information from anywhere in the world.

Under the BC Personal Information Protection Act (PIPA), physicians must implement reasonable safeguards to reduce the risks associated with working with personal information remotely while travelling, at home, or at another location.

Guidelines for conversations outside the office:

1. Avoid discussing personal information in public areas such as on elevators, in stairwells, while travelling by public transit or airplanes, in restaurants, or on the street.
2. When in transit, avoid using cell phones to discuss personal information, as these conversations can be intercepted or overheard.

3. If a staff member works regularly from home, a dedicated phone line with password protected voicemail is recommended.

Guidelines for personal information stored on paper or portable electronic devices when outside the office:

1. Remove records containing personal information only when it is absolutely necessary for performing job duties. If possible, leave a copy with the originals left in the office. Take only the minimum amount of personal information required.
2. Require all staff to obtain approval from their supervisor before removing records containing personal information from the office.
3. When travelling by car, keep records locked in the trunk before the start of a trip—don't put them there once at the destination. Where possible, do not leave records unattended, even if they are stored in the trunk. Car trunks are no less accessible to thieves than the front seats.
4. Do not view records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit).
5. Do not leave records open for view in hotel rooms; they should be kept in the hotel safe.
6. Upon returning to the office, immediately replace records containing personal information to their original storage location. Securely destroy any copies that are no longer required.

Guidelines specific to personal information stored on paper-based records when outside the office:

1. Use a sign-out sheet to document who is removing a record, the name of the individual whose personal information is being removed, and the date the record is being removed.
2. If the records are large, consider using a courier to transport it to the destination.
3. Place records in confidential folders, transport them in a secure container, and keep them under control at all times. This includes during meals or breaks.
4. When working from home, keep records locked in a desk drawer or filing cabinet to reduce unauthorized viewing and access by family members or friends.

Guidelines specific to personal information stored on portable electronic devices when outside the office:

1. Protect portable electronic devices containing personal information with a strong password when taken away from the office.

2. Avoid storing personal information on portable electronic devices unless absolutely necessary.
3. To prevent loss or theft, keep portable electronic devices secure at all times, in a locked briefcase, desk drawer, container, or room, and keep them under one person's control at all times. This includes during meals or breaks.
4. When travelling by car, keep all portable electronic devices locked in the trunk before the start of the trip— don't put them there once at the destination. Where possible, do not leave portable electronic devices unattended, even if stored in the trunk.
5. When no longer needed, remove all sensitive personal information 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.

Guidelines for appropriate use of home computers or portable electronic devices for accessing personal information:

1. Do not use public computers or networks to connect to the office network as these are unsecure devices and locations.
2. Log off from a laptop or home computer and set the automatic log out to occur when not in use.
3. Lock home computers that are used for work-related purposes to a table or other stationary object with a security cable and keep them in a room with restricted access.
4. When accessing electronic records from home, avoid storing any personal information on the hard drive of a home computer. Any personal information that must be stored on hard drives should be encrypted and password protected.
5. Do not share a laptop or home computer that is used for working with sensitive personal information with other individuals, including family members and friends.
6. Ensure that laptops and home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection. Ensure that the latest updates and security patches are regularly installed.
7. When conducting business involving personal information over a network, use an encrypted link to the host network, such as a virtual private network (VPN).
8. Ensure that staff do not remove any patient information from the office network without authorization from their supervisor.
9. Watch out for "shoulder-surfing" where unauthorized individuals may casually observe the screen of someone's laptop or desk computer. Consider installing a privacy screen filter to prevent viewing of the screen from an angle.

For additional information, see the BC Information and Privacy Commissioner's release on Physicians and Security of Personal Information, June 2006 at www.oipc.bc.ca.