College of Physicians and Surgeons of British Columbia

Professional Standards and Guidelines

Electronic Medical Records

Preamble

This document is a guideline of the Board of the College of Physicians and Surgeons of British Columbia.

In its drive to modernize the provincial health care system, and improve access to and quality of health care, the provincial government – together with the BCMA and with input from the College and other agencies – has developed a strategy for the electronic integration of information and communications among health care providers. Electronic medical records (EMRs), for which physicians are primarily responsible, are one of the key elements of this long-term "eHealth" strategy.

The transition from paper to electronic medical records is a significant undertaking that needs to be considered and managed from many perspectives – clinically, administratively and organizationally. While a physician's responsibility as the steward of patient data remains unchanged during this transition, the manner in which the information is collected, used and disclosed will alter significantly.

The following guidance will assist physicians in meeting their medical-legal and ethical obligations throughout the transition process.

College's Position

- Implementation of an EMR will necessitate process changes in your practice. Processes designed on the movement of paper charts should be assessed and altered accordingly.
- Protection of personal health information is of paramount importance. Assess the security risks in your office. Security policies and staff education should take place to address specific concerns.
- Physicians may choose either to scan paper records electronically in a "read only" format, e.g. pdf, or to start entering data from day one of their new EMR. Either way, the College recommends that paper records be kept in close proximity for at least six months. Unless they are completely scanned into the EMR, paper records must be kept indefinitely if the patient continues to attend. If the patient has left or moved, paper records must be kept for at least 16 years from the date of last patient contact (or until the patient reaches age 35 for patients under 19).

- Physicians must ensure that complete medical records (paper, electronic or a combination of both) are accessible at all clinical decision points and for the duration of the retention period prescribed under section 3-6 of the Bylaws under the *Health Professions Act.*
- EMRs must be able to be printed promptly if required.
- Each practice must identify in writing the level of access by any authorized persons utilizing EMRs.
- If your EMR is located on a server in your office, ensure that the server is physically secure and robust backup procedures are in place.
- Numerous commercial EMR products are available. A suitable EMR program must have the following attributes:
    - audit trail for information entry
    - capability of physicians to provide sign-off on documentation, orders and prescriptions using electronic signatures or equivalent authentication
    - regular backup of data
    - effective recovery

Secure Use of Electronic Medical Records

- Only use EMRs that permit password protection and encryption. Keep passwords confidential. At a minimum, the College recommends the use of a strong password to enable access to the EMR. For additional security, consider the use of two factor authentication, e.g. secure ID tokens, fobs, etc.
- Every user who accesses an EMR must have a unique ID with appropriate password controls.
- Audit logging must be enabled on the EMR to record actions taken by each authorized user.
- The College recommends the use of encrypted EMRs. If you choose an EMR that will be remotely hosted by an Application Service Provider (ASP), ensure that their database is encrypted. If you have a locally hosted EMR on a server in your office, physically secure the server in a locked area with limited access.
- Computers that are accessible by unattended patients, e.g. in an exam room, must be electronically “locked down” to prevent unintended access.
- Firewalls and anti-virus software are important protections against digital attacks such as viruses, spyware and hackers. Keep these products current using regularly scheduled updates or real-time update protocols.
- Ensure that an electronic backup copy of all EMRs is stored in a different, secure physical location to prevent the permanent loss of information. If you have a locally hosted EMR on a server in your office, ensure physical redundancy in the server setup to help prevent data loss.
- Place printers in non-patient accessible areas of the office.

- Mobile devices such as laptops, PDAs, and smartphones containing personal health information must be password protected and encrypted. When these devices are not in your direct control, you must take measures to protect them from theft or misuse.
- When working outside the office, you should log off or shut down your laptop or home computers when not in use. Set the screensaver to run after a short period of idleness and enable password protection.
- When computer hardware that has been used for EMRs is disposed of, all data must be erased from the storage media in a manner that ensures the information cannot be reconstructed.
- Emails containing personal health information should be encrypted.
- Local wireless networks within a physician's office must be encrypted and combined with a strong password. Additional security would include the use of two factor authentication.
- In the event of a security breach, follow the joint BCMA/College/BC Privacy Commissioner's *Key Steps for Physicians in Responding to Privacy Breaches*, available on the College website at www.cpsbc.ca under Data Stewardship Framework in the *Professional Standards and Guidelines.*

Council Approved December 2007
Updated June 2013