RECORDS MANAGEMENT

Records Management refers to the lifecycle of paper and electronic records from the point of creation to their secure disposal; this includes the access, security, storage, and disposal of medical records. Physicians, as Health Information Custodians, are responsible for ensuring effective medical record-keeping practices, as part of providing quality patient care.

Retention

- Records must be retained for at least 10 years after the last entry for patients 18 years or older or after patients reach 18 years of age.
- The College of Physicians and Surgeons of Ontario (CPSO) recommends retaining patient records for at least 15 years.

Frequently Asked Questions

How long should a physician retain the following medical records?
The last entry of a 17-year-old patient's record was made 10 years ago.
- 11 years – mandatory
- 16 years – recommended

The record of a 45-year-old patient was last updated 10 years ago, but the patient made a Personal Health Information (PHI access) request a month ago.

As long as necessary to fulfill PHI Access request under the *Personal Health Information Protection Act* (PHIPA).

Security

- Personal health information (PHI) in an EMR, external storage media or mobile devices must be strongly encrypted.
- Data sharing agreements, restricted access controls and audit trails must be in place among all parties and/or organizations that access records and PHI.
- Consider applying the same policies you use for paper records (limited access, audits etc.) to your electronic data as well.

Frequently Asked Questions

My mobile device is password protected. Does this meet the security standards of PHIPA?
No, PHI kept on mobile devices also requires enhanced security such as encryption.

What do I need to consider if my patient's chart is shared with a clinician in an out-patient setting?
Data sharing agreements must be established among physicians and organizations who will be sharing patient health information.

OntarioMD

Storage

- The security and safety of your paper and electronic records are paramount. Well-managed records require planning, organization and maintenance, regardless of medium.
- Appropriate measures must be taken to prevent loss, restrict access and maintain the privacy of records at all times.
- Regular back-up is recommended with copies stored in a secure environment separate from where the original data is normally stored.

Frequently Asked Questions

Are there specific areas where PHI should be kept?
All patient records and data must be kept in restricted access areas or locked filing cabinets to protect against loss of information and damage.

How often should records be backed up?
Electronic records must be backed-up on a routine basis and back-up copies stored in a physically secure environment separate from where the original data is normally stored.

Disposal

- Once the obligation to retain a record has come to an end, patient records can be disposed of in accordance with PHIPA's requirements[1].
- Records must be disposed of securely by permanently deleting them from all storage mechanisms.
- When using a commercial vendor to destroy records, a certificate of destruction should be provided and retained permanently.

Frequently Asked Questions

How do I destroy a batch of records at the end of the retention period?
The Canadian Medical Protective Association (CMPA) recommends that a list be made of the names of those patients whose records are to be destroyed, and that this list be kept perma-nently in a secure location. The purpose is to be able to later determine at a glance that a chart has been destroyed and has not simply been lost or misplaced.

What about patient information on hard drives?
Hard drives must be crushed or wiped clean with a commercial disk wiping utility and related back-up copies of records destroyed.

For more information: support@ontariomd.com | www.ontariomd.ca

---

[1] CPSO Policies #4-12, "Medical Records"