Medical Records Stewardship

Policies of the College of Physicians and Surgeons of Ontario (the "College") set out expectations for the professional conduct of physicians practising in Ontario. Together with the *Practice Guide* and relevant legislation and case law, they will be used by the College and its Committees when considering physician practice or conduct.
Within policies, the terms 'must' and 'advised' are used to articulate the College's expectations. When 'advised' is used, it indicates that physicians can use reasonable discretion when applying this expectation to practice.

Definitions

Stewardship: For the purposes of this policy, stewardship refers to the care, handling, and management of medical records.

Policy

1. Whether in paper or electronic format, physicians **must** comply with all relevant legislation[1] and regulatory requirements related to medical record-keeping.

Establishing Custodianship and Accountabilities

2. Physicians who practise in a setting where there are multiple contributors to a record-keeping system (e.g., a group or interdisciplinary practice, settings with a shared electronic medical record (EMR)) **must** have a written agreement that establishes custodianship and clear accountabilities regarding medical records stewardship.[2]

3. Physicians **must** ensure their agreements:

    a. are in place prior to the establishment of the group practice, business arrangement, or employment, or as soon as possible afterward;
    b. comply with the *Personal Health Information Protection Act, 2004* (*PHIPA*) and with the expectations set out in this policy; and

[1] *Personal Health Information Protection Act*, *2004*, S.O. 2004, c.3, Sched. A (hereinafter *PHIPA*); Part V of the General, O. Reg., 114/94, enacted under the *Medicine Act, 1991*, S.O. 1991, c. 30 (hereinafter *Medicine Act*, General Regulation); General, O. Reg., 57/92, enacted under the *Independent Health Facilities Act*, R.S.O.1990, c.1.3 (hereinafter *IHFA,* General Regulation); Hospital Management, Regulation 965, enacted under the *Public Hospitals Act*, R.S.O. 1990, c.P.40 (*Public Hospitals Act,* Hospital Management Regulation).
[2] Section 14(1) of the *Public Hospitals Act* sets out that patient medical records compiled in a hospital are the property of the hospital. For the purposes of this policy, the provisions set out in the *Public Hospitals Act*, along with the terms of a physician's hospital privileges can serve as the official agreement for physicians who work in hospitals.

c. address custody and control of medical records, including upon termination of employment or the practice arrangement.[3]

4. Physicians with custody or control of records **must** give all former partners and associates reasonable access to their patient medical records to allow them to prepare medico-legal reports, defend legal actions, or respond to an investigation, when necessary.[4]

5. In accordance with *PHIPA*, in instances where a physician is moving to a new practice location and does not have custody or control of the medical records of patients who choose to follow them to the new practice location, the physician **must** obtain patient consent to transfer copies of the records to the new location.

6. If there is a conflict regarding medical records custody or control, physicians **must not** allow the conflict to compromise patient care.

Access and Transfer of Medical Records

Access to Medical Records

7. Physicians **must** provide patients and authorized parties[5] with access to, or copies of, all the medical records in their custody or control upon request, unless an exception applies.[6]

8. Physicians **must** provide patients and authorized parties with explanations of any term, code, or abbreviation used in the medical record, upon request.[7]

9. Where an exception applies and access is refused, physicians **must** inform the individual in writing of the following:

    a. the fact of the refusal;
    b. the reason for the refusal; and

[3] The Canadian Medical Protective Association's (CMPA) *Electronic Records Handbook* has additional advice for establishing such agreements.
[4] *PHIPA*, s. 41(1).
[5] Authorized parties include substitute decision-makers and estate trustees/executors of the estate where applicable, and third parties where consent has been obtained.
[6] *PHIPA*, s. 52; Section 52 of *PHIPA* contains a comprehensive list of the exceptions. There are also separate provisions for access to information related to an Independent Medical Exam. The CMPA's article, *Providing access to independent medical examinations* sets out advice on this issue.
[7] *PHIPA*, s. 54(1)(a).

c. the right of the patient to make a complaint to the Information and Privacy Commissioner.[8]

10. Where physicians rely on an external facility or organization to retain records, such as a commercial storage provider, diagnostic facility, or clinic, physicians **must** ensure that access to records is possible when necessary.

Transferring Copies of Medical Records

11. Physicians **must** retain original medical records for the time period required by the Regulation (see *Medical Records Retention* below) and only transfer copies to others.

12. Physicians **must** only transfer copies where they have consent or are permitted or required by law to do so.[9]

13. Physicians **must** transfer copies of medical records in a timely manner, urgently if necessary, but no later than 30 days after a request.[10] What is timely will depend on whether there is any risk to the patient if there is a delay in transferring the records (e.g., exposure to any adverse clinical outcomes).

14. In some cases a summary or partial copy of the medical records may be preferred. Where physicians opt to provide a summary or a partial copy of the medical record rather than a copy of the entire record, physicians **must** ensure this is acceptable to the receiving physician and/or the patient.

15. Physicians **must** transfer copies of medical records in a secure manner[11] and document the date and method of transfer in the medical record.

[8] *PHIPA,* s. 54(1)(c).
[9] For more information regarding disclosure, please refer to the College's *Protecting Personal Health Information* policy.
[10] *PHIPA*, s. 54(2). Physicians are required under *PHIPA* to respond to requests of records transfer as soon as possible, but no later than 30 days of the request. Sections 54(3) and 54(5) of *PHIPA* set out provisions for circumstances requiring expedited access and an extension.
[11] *PHIPA,* s. 13(1)

Fees for Copies and Transfer of Medical Records [12]

16. Fulfilling a request for copying and transferring records is an uninsured service. As such, physicians are entitled to charge patients, or third parties, a fee for obtaining a copy or summary of their medical record. In doing so, physicians **must**:

    a. provide a fee estimate prior to providing copies or summaries;[13] and
    b. only charge fees that are reasonable.

17. When determining what is reasonable to charge, physicians **must** ensure that fees:

    a. do not exceed the amount of "reasonable cost recovery";[14] and
    b. are commensurate with the nature of the service provided and their professional costs (i.e., reflect the cost of the materials used, the time required to prepare the material and the direct cost of sending the material to the requesting individual).[15]

18. As part of determining a reasonable fee, physicians **must** consider the recommended fees set out in the Ontario Medical Association's *Physician's Guide to Uninsured Services* ("the OMA Guide")[16,17] and the applicable orders of the Information and Privacy Commissioner.[18]

19. Physicians **must** additionally consider the patient's ability to pay when determining a reasonable fee.[19] In particular, physicians **must** consider the financial burden that these fees might place on the patient and consider whether it would be appropriate to reduce, waive, or allow for flexibility with respect to fees based on compassionate grounds.

[12] This requirement applies regardless of whether access is provided directly by a physician or an agent of the physician, such as a records storage company.
[13] *PHIPA*, s. 54(10).
[14] *PHIPA*, s. 54(11).
[15] In accordance with s. 1(1), paragraph 21 of O.Reg. 856/93 *Professional Misconduct*, enacted under the *Medicine Act, 1991* S.O. 1991. C.30 it is an act of professional misconduct to charge a fee that is excessive in relation to the services provided.
[16] The OMA Guide is typically updated annually, and so physicians must ensure they have reviewed the most recent edition.
[17] While physicians are not obliged to adopt the recommended fees set out in the OMA Guide, in accordance with s. 1(1) paragraph 22 of the *Professional Misconduct Regulation*, it is an act of professional misconduct to charge more than the current recommended fees in the OMA Guide without first notifying the patient of the excess amount that will be charged.
[18] See Information and Privacy Commissioner orders HO-009 and HO-14.
[19] The Canadian Medical Association Code of Ethics #16 states that "In determining professional fees to patients for non-insured services, consider both the nature of the service provided and the ability of the patient to pay, and be prepared to discuss the fee with the patient."

20. Physicians may take action to collect any fees owed to them, but **must not** put patients' health and safety at risk by delaying the transfer of records until payment has been received.[20]

Retention and Destruction

Medical Records Retention[21,22]

21. Even where records are copied and transferred, physicians **must** retain medical records in their custody or control for the following time periods:

    a. *Adult patients:* 10 years from the date of the last entry in the record.
    b. *Patients who are children:* 10 years after the day on which the patient reached or would have reached 18 years of age.[23,24]

Destruction of Medical Records

22. Physicians **must** only destroy medical records once their obligation to retain the record has come to an end.

23. When destroying medical records, physicians **must** do so in a secure and confidential manner[25] such that the reconstruction of the record is not reasonably foreseeable in the circumstances. As such, physicians **must**, where applicable:

    a. cross-shred all paper medical records;
    b. permanently delete electronic records from all hard drives[26] and storage devices by crushing or wiping clean with a commercial disk wiping utility; and
    c. destroy any back-up copies of records.[27]

---

[20] For additional guidance on fees please refer to the College's *Uninsured Services: Billing and Block Fees* policy.
[21] Retention requirements apply equally to records for patients that are living and deceased.
[22] Physicians who cease to practise family medicine or primary care have specific retention requirements under the law. For obligations related to medical records for physicians who cease to practice, see the College's *Closing a Medical Practice* policy. Hospitals have separate retention schedules for diagnostic imaging records set out in s. 20(4) of the *Public Hospitals Act*, Hospital Management Regulation. Independent health facilities have separate retention schedules for patient health records set out in s. 11(1) of the *IHFA,* General Regulation.
[23] *Medicine Act,* General Regulation, s. 19(1).
[24] Physicians are advised that s. 15(2) in the *Limitations Act*, *2002* allows for some legal proceedings to be brought forward 15 years after the act or omission on which the claim is based took place and thus may wish to retain records for longer than the 10 year requirement.
[25] *PHIPA*, s. 13(1).
[26] Where it is not possible to permanently delete records from the hard drive, the entire hard drive must be destroyed.
[27] For further information, consult the IPC's Fact Sheet #10 – *Secure Destruction of Personal Information*.

Storage and Security

Storage

24. Physicians **must** ensure medical records in their custody or control are stored in a safe and secure environment and in a way that ensures their integrity and confidentiality, including:

    a. taking reasonable steps to protect records from theft, loss and unauthorized access, use or disclosure, including copying, modification or disposal;[28]
    b. keeping all medical records in restricted access areas or in locked filing cabinets to protect against unauthorized access, loss of information and damage;
    c. backing-up electronic records on a routine basis[29] and storing back-up copies in a secure environment separate from where the original data is stored.

25. Where physicians choose to store medical records content that is no longer relevant to a patient's current care separately from the rest of the medical record[30], physicians **must** include a notation in the record indicating that documents have been removed from the chart and the location where they have been stored.

26. Physicians **must** ensure medical records are readily available and producible when access is required.

Security[31]

27. Physicians with custody or control of medical records **must** have records management protocols that regulate who may gain access to the medical records in their custody or control and what they may do according to their role, responsibilities, and the authority they have.[32]

---

[28] *PHIPA*, s. 12(1). What is reasonable in terms of records management protocols will depend on the threats and risks to which the information is exposed, the sensitivity of the information, and the extent to which it can be linked to an identifiable individual.

[29] The CMPA suggests daily or weekly back-ups be considered. The CMPA provides risk management advice regarding back-up and recovery practices for EMR systems in its *Electronic Records Handbook*.

[30] In accordance with section 14(2) of *PHIPA* and the retention requirements set out in the regulation and this policy.

[31] For expectations related to privacy breaches please refer to the College's *Mandatory and Permissive Reporting* policy.

[32] Records management protocols include both physical and logical access controls. Physical access controls are physical safeguards intended to limit persons from entering or observing areas of the physician's office that contain confidential health information or elements of an EMR system. Logical access controls are system features that limit the information users can access, modifications they can make, and applications they can run. Examples of the latter include the use of "lockboxes" and "masking" options to restrict access to personal health information at patient request.

28. Accordingly, where an electronic record-keeping system is used:

a. physicians **must** ensure their systems are equipped with user identification and passwords for logging on; and
b. physicians **must not** share their credentials or passwords.

29. Physicians with custody or control of medical records **must** ensure that:

a. all individuals who have access to medical records are bound by appropriate confidentiality agreements; and
b. data sharing agreements incorporating the requirements in this policy are established for all individuals who will have access to or who will be sharing patient health information with one another.[33]

Electronic Records

System Requirements

30. Physicians **must** only use electronic record-keeping systems (e.g., EMRs) that comply with regulation.[34] In particular, physicians **must** only use electronic systems that:

a. Provide a visual display of the recorded information;
b. Provide a means of access to the record of each patient by the patient's name and, if the patient has an Ontario health number, by the health number;
c. Are capable of printing the recorded information promptly;
d. Are capable of visually displaying and printing the recorded information for each patient in chronological order;
e. Include a password or otherwise provide reasonable protection against unauthorized access;
f. Maintain an audit trail (a record of who has accessed the electronic record) that:
    i. records the date and time of each entry of information for each patient,
    ii. indicates any changes in the recorded information,
    iii. preserves the original content of the recorded information when changed or updated, and
    iv. is capable of being printed separately from the recorded information for each patient;

[33] The CMPA's *Electronic Records Handbook* contains advice related to data sharing principles for Electronic Medical Record/Electronic Health Record agreements.
[34] *Medicine Act*, General Regulation, s. 20.

g. Automatically back up files and allow the recovery of backed-up files or otherwise provide reasonable protection against loss of, damage to, and inaccessibility of, information.

31. Physicians **must** only use electronic record-keeping systems that are capable of capturing all pertinent personal health information and allow the authorized user to access patient information in an efficient manner.

32. Physicians **must** only use certified electronic record-keeping systems (e.g., EMRs) unless they can independently verify that an unaccredited system meets the privacy and security standards required by *PHIPA* and the standards set out in the Regulation.[35,36]

33. Physicians **must** be proficient with their electronic record-keeping system in order to:

    a. meet the requirements for record-keeping set out in relevant legislation and this policy; and
    b. participate in all regulatory processes (e.g., College investigations and assessments).

Transitioning Records Management Systems[37]

34. When transitioning from one record-keeping system to another, (i.e., a paper-based to electronic system, or from one electronic system to another) physicians **must**:

    a. maintain continuity and quality of patient care;
    b. continue appropriate record-keeping practices without interruption;
    c. protect the privacy of patients' personal health information; and
    d. maintain the integrity of the data in the medical record.

35. To ensure integrity of the medical records, physicians who are transitioning from one record-keeping system to another **must** have a quality assurance process in place that includes:

    a. written procedures that are developed and consistently followed; and
    b. verification that the entire medical record has remained intact upon conversion (e.g., comparing scanned copies to originals to ensure that they have been properly

[35] OntarioMD and Canada Health Infoway provide certification for privacy and security.
[36] *Medicine Act*, General Regulation, s. 20.
[37] For additional guidance related to transitioning record-keeping systems please refer to the companion Advice to the Profession document.

scanned or converted).

36. Physicians who opt to destroy their original paper medical records once they have been converted into digital format **must**:

    a. use appropriate safeguards to ensure reliability of digital copies;
    b. save scanned copies in “read-only” format; and
    c. destroy medical records in accordance with the expectations set out in this policy.

37. Physicians who use voice recognition software or Optical Character Recognition (OCR) technology to convert records into searchable, editable files **must** retain either the original record or a scanned copy for the retention periods set out above.

38. So that complete and up to date information is contained in one central location, physicians with custody or control of records **must:**

    a. set a date whereby the new (electronic) system becomes the official record; and
    b. inform all health care professionals who would reasonably be expected to contribute or rely on the record, of this date.

39. Physicians **must** only document in the new system from the official date onward.