

Physicians as Custodians of Patient Records

Related Standards of Practice: [Closing or Leaving a Medical Practice](#), [Continuity of Care](#), [Patient Record Retention](#), [Relocating a Medical Practice](#)

The College of Physicians & Surgeons of Alberta (CPSA) provides advice to the profession to support physicians in implementing the *CPSA Standards of Practice*. This advice does not define a standard of practice, nor should it be interpreted as legal advice.

Contents

Introduction.....	1
Physicians as Custodians	2
Successor Custodian.....	3
Policies and Procedures.....	3
Privacy Impact Assessments.....	4
Affiliates.....	4
Information Sharing Agreement.....	5
Example scenarios	6
Information Manager Agreement	7
Appendix A: Scenarios Requiring an IMA or ISA.....	9

Introduction

Patient records are foundational to good medical care. Whether in paper or electronic form, a patient’s record must be a complete, accurate and legible account of their medical history, examinations, investigations, diagnoses and care provided.

While traditionally physicians kept patient records primarily for their own use, the shift to team-based care and electronic information management technologies has changed the way patient records are created, accessed and used, particularly in group practice. These changes have enhanced patient care and continuity of care, but also heightened the responsibility of physicians to protect patient privacy and ensure records are kept secure and accessible by authorized users.

Alberta's [Health Information Act \(HIA\)](#) and [Health Information Regulation](#) set out the legal obligations of physicians and other healthcare providers in managing patient information, and the College's [Patient Record Retention](#) standard of practice establishes further professional expectations. Built on the principle enshrined in the [Code of Ethics](#), the standard expects physicians to consider first the needs of their patients in meeting their custodial duties under the HIA.

Physicians as Custodians

Physicians in Alberta are designated custodians of patient health information under the *Health Information Regulation*. This designation recognizes physicians are responsible for the collection, use and disclosure of health information essential to the care of their patients and for protecting the confidentiality and security of the health information in their custody.

Physicians are also responsible for maintaining or contributing to patient medical records in keeping with the College's [Patient Record Content](#) standard of practice. Depending on the nature of his or her practice, a physician will do so in either a custodial or an affiliate role (see [Affiliates](#)). Physicians need to be clear which role they are fulfilling, as a custodian has greater responsibilities in maintaining the ongoing security and accessibility of patient records.

Custodial duties include:

- collect, use or disclose health information with the highest degree of anonymity possible
- protect health information
- ensure the accuracy of health information
- identify responsible [affiliates](#)
- establish [policies and procedures](#) for managing the health information in their custody or under their control
- prepare [Privacy Impact Assessments](#)

Under the College's [Patient Record Retention](#) standard of practice, physicians are responsible for maintaining the security and accessibility of the patient records in their custody for a minimum of 10 years after the last date of entry (or for minor patients, two years after the age of 18, whichever is longer).

Custodial duties cannot be relinquished, but in certain circumstances can be transferred to a designated [successor custodian](#) should the physician who created the records become unable to meet their custodial duties.

A physician who retires from practice remains custodian of their patient records unless ownership of the practice is transferred to another practitioner (successor) who agrees to take over the care of the retiring physician's patients and assume [custody of their records](#).

A retiring physician who closes their practice remains custodian, but may contract with an [Information Manager](#) to facilitate secure access to their patient records for the length of time identified in the [Patient Record Retention](#) standard of practice.

Successor Custodian

For continuity of care and to ensure patients have ongoing access to their health information, physicians who are custodians must have agreements and arrangements in place to deal with contingencies (e.g., they become ill, die or move to a geographically distant location). This includes designating an appropriate [successor custodian](#), a requirement under the [Patient Record Retention](#) standard of practice.

The designated successor must be eligible to be a custodian under the [Health Information Regulation](#) (i.e., not a spouse or relative of the physician unless also a custodian) and, if not practising at the same location, be located near enough to the original custodian's practice to ensure patients continue to have reasonable access to their records. ([Successor Custodian of Medical Records Agreement template](#))

A physician who neglects to designate a successor custodian not only breaches the standard, but puts their patients' needs for ongoing care and access to their health information at risk and unfairly places the burden of record care and storage on the profession as a whole if unable to fulfil their custodial duties.

Policies and Procedures

In the custodial role, physicians are responsible for establishing policies and procedures for the proper management of their patient records to ensure *HIA* requirements for maintaining the accessibility, security and confidentiality of patient health information are met.

Policies and procedures should address:

- role-based access (e.g., administrative, clinical), password protocols and data back-up for EMR;
- how access is monitored;
- appropriate disclosure of patient information;
- how requests for access and corrections are managed; and
- secure storage and (eventual) destruction of patient records, whether paper or electronic.

Security safeguards might include¹:

- alarm systems;
- secured server rooms;
- secured routers and wireless access points;
- measures to protect against environmental hazards based on risk (e.g., power loss, fire, flooding, etc.); or

¹ Source: Office of the Information and Privacy Commissioner of Alberta – [Guidance for Electronic Health Record Systems](#) (June 2016)

- maintaining backup and archival copies of health information in a secure off-site location.

Procedures should also include measures to ensure any [Affiliates](#) (e.g., staff delegated responsibility for aspects of records management) are aware of and adhere to the administrative, technical and physical safeguards put in place by the custodian.

Privacy Impact Assessments

A [Privacy Impact Assessment](#) (PIA) is a tool for identifying and managing risks to privacy that may occur in administrative and technological processes when handling confidential information.

The duty of a custodian or group of custodians in a shared practice to complete a PIA is mandated by both the *HIA* and the College's [Patient Record Retention](#) standard of practice. This underscores its importance as a safeguard for patient privacy, particularly in an electronic environment.

In Alberta, PIAs must be submitted for review by the Office of the Information and Privacy Commissioner (OIPC). Detailed information and resources for completing PIAs are available on the OIPC website at www.oipc.ab.ca.

PIAs need to be updated. A PIA must be reviewed every time a new procedure, process or technology changes how patient records are created, stored or used. This includes any change to the way the practice communicates with patients (e.g., introducing an email or text option for appointment confirmation). In most physician offices, the PIA should be reviewed at least every three to five years.

Affiliates

Unless you are clearly identified as an affiliate, you are most likely a custodian of any patient records you create or contribute to, and are responsible for meeting your custodial duties under the *HIA* and the *Patient Record Retention* standard of practice.

Under the *HIA*, an affiliate is an individual who is employed by a custodian or performs a service for a custodian as an appointee, volunteer or student, or under a contract or agency relationship.

Affiliates are authorized to access, enter and use health information only as necessary to perform their duties to the custodian. For example, non-medical staff members are often identified as affiliates by a custodian physician. In addition, most healthcare providers, including physicians employed by or performing a service for Alberta Health Services, are considered affiliates of AHS, which acts as custodian of the health information entered into AHS systems. (Note: Physicians who maintain their own EMR within an AHS facility are the custodians of the patient records in their own EMR.)

A physician (e.g., locum) entering into an agreement to provide services for a custodian should ensure their role as affiliate is clearly stated and understood, preferably in writing.

Any collection, use or disclosure of health information by an affiliate is done on behalf of the custodian; as such, affiliates must fulfil the custodian's duties to observe the highest possible degree of anonymity, protect health information, ensure accuracy and comply with the custodian's policies and procedures.

However, affiliates do not have any ongoing responsibility for maintaining patient records once their employment or service arrangement with the custodian ends, as responsibility remains with the custodian.

Information Sharing Agreement

Under the College's [Patient Record Retention](#) standard of practice, a custodian physician is required to sign an Information Sharing Agreement (ISA) whenever access to patient records is shared with other custodians in the practice for the purposes of continuity and quality of care (such as in a group practice).

The College's ISA requirement does **not** apply to the sharing of patient information for the purposes of [referral-consultation](#) or [transfer of care](#).

The purpose of an ISA is to provide clarity as to how custodians will manage shared patient records day-to-day and what will happen to the records in the event the professional arrangement between the custodians changes (e.g., a physician leaves the practice, the partnership dissolves, etc.). Without an ISA, there may be disagreement between the custodians regarding ownership of the records that could impact the care of patients and their ability to access their health information.

An ISA must include:

1. Roles and responsibilities regarding access, disclosure, transfer and return of patient information, such as:
 - the need for each physician to have an ISA with all the other custodian physicians who share the EMR;
 - an agreed process for determining custody of a patient's record in situations where any physician in the group might contribute to any patient's record (e.g., in a walk-in clinic, the first physician to see a patient becomes custodian or another method that complies with [Establishing the Physician-Patient Relationship](#) standard of practice); and
 - a means of identifying (and removing) the records in the EMR a custodian physician has ongoing responsibility for, as per the [Patient Record Retention](#) standard of practice.
2. How records are to be managed (and who will cover any associated costs) when a physician custodian leaves the practice, for example the:
 - physician removes their records and takes them;
 - physician names (recruits) a successor custodian to replace them in the practice; or
 - physician enters into an agreement with an information manager to maintain the security of their records and facilitate future access and destruction.

While a physician can charge a patient a reasonable fee to transfer their records to a new physician when requested, patients should **not** bear the cost when a physician transfers all their records to a new practice location. Patients also do not need to sign consent forms for the transfer of their records when all of a physician's records are being moved to a new location.

The best time to sign an ISA is when the physicians start their practice together. Whenever there is a change in practice membership, the ISA should be reviewed; this will allay any potential issues and set the stage for an amicable parting should the physicians decide to end their arrangement.

Example scenarios

In determining whether an ISA is required under the [Patient Record Retention](#) standard (see [Appendix A](#)), it is important to consider how the practice operates. For example, consider a group of physicians who work together in a clinic and use a shared EMR for their patient records.

Scenario 1: An Information Sharing Agreement IS required if:

- Each physician operates an individual practice within the clinic (i.e., is a partner or associate with the other physicians and is not considered an employee). All of the physicians are custodians of their own patient records in the EMR. Records are shared for walk-in patients and vacation/after-hours coverage.

Scenario 2: An Information Sharing Agreement IS required if:

- The clinic is owned by a business that is not a designated custodian under the *HIA*. Anyone can own the bricks-and-mortar building where a clinic operates, but **only a physician can “own” the practice of medicine** and be the custodian of a patient's medical records (i.e., a non-physician business owner of a clinic **cannot** be a custodian of patient records). All the physicians in this scenario are therefore custodians and need to sign an ISA. (Note: While not a custodian, the business owner can be an [Information Manager](#)).

Scenario 3: An Information Sharing Agreement is NOT required if:

- One physician owns the practice and is custodian of all the patient records in the EMR. All other physicians working in the practice are affiliates (an arrangement that requires Ministerial approval under the *HIA*). **The affiliate role should be clearly stated and understood, preferably in writing**, although an ISA is not required. The physician owner is **not** the default custodian of all patient records simply by virtue of being a physician. In an affiliate role, physicians are authorized to access the EMR for the purpose of providing patient care in support of the custodian. Affiliate physicians who leave the practice do not own the patient records to which they contributed, have any ongoing responsibility for the security or accessibility of the records and cannot take the records with them. However, any patient who chooses to follow a former affiliate to their new practice location may request that a copy of their own record be provided to the physician.

Information Manager Agreement

An Information Manager is defined as a person or body that processes, stores, retrieves or disposes of health information; strips, encodes or otherwise transforms individually-identifying health information to create non-identifying health information; or provides data management or information technology services.

For example, an Information Manager might provide EMR maintenance services, data back-up services, secure records storage and so on.

Under the *HIA*, a custodian must have a **written** Information Manager Agreement (IMA) with any service provider that meets the definition of Information Manager.

Per the [Health Information Regulation 7.2](#), an IMA must:

- identify the objectives and principles of the agreement:
 - privacy and security requirements;
 - retention and destruction expectations;
 - patients' right of access to their records; and
 - successor custodian contact information;
- indicate if the Information Manager may collect health information from other custodians and, if so, the purpose for which it may be collected;
- indicate if the Information Manager may use the health information collected and, if so, the purpose for which it may be used;
- indicate if the Information Manager may disclose health information and, if so, the purpose for which it may be disclosed;
- describe the process in which the Information Manager may respond to access requests or how to direct requests to the custodian;
- detail how the Information Manager may amend or correct health information or how to direct requests for amendments to the custodian;
- define how health information is to be protected, managed, returned or destroyed in accordance with the *HIA*;
- outline how the Information Manager addresses expressed wishes of patients for disclosing their health information or how to refer these requests to the custodian; and
- specify how an agreement can be terminated.

The Information Manager must be compliant with the *HIA* and may:

- be provided health information without the consent of individual patients for the purposes authorized in the agreement; and
- disclose information as provided for in the agreement.



Regardless of the agreement, the custodian remains responsible for compliance with *HIA* and maintains access and control of the records.

For more information, please refer to [Appendix 4: Components for Agreements Under the *Health Information Act*](#).

Appendix A: Scenarios Requiring an IMA or ISA*

	SCENARIO	IMA		ISA
		VENDOR	GENERIC	
1	Using a billing agent, external transcription service.	X		
2	Using a storage firm for electronic or paper records.	X		
3	Using an application service provider (ASP), remote data storage.	X		
4	Sharing patient information between clinic sites.			X
5	Sharing information within the Primary Care Network (PCN), large clinic group setting for the purpose of patient care.			X
6	Individual clinics providing identifiable health information to PCN for purposes including quality improvement, performance metrics, and guiding PCN direction. Exceptions: In the case of a centralized PCN, or a PCN with a small number of member clinics where the PCN is an affiliate acting under the clear documented direction of each custodian with respect to the ongoing use of the data, no IMA is required. Individual clinics exchanging identifiable patient information within the clinic for these purposes do not require an IMA.		X	
7	Providing health information to the Health Quality Council of Alberta.		X	
8	Pan PCN committee hires/contracts research analyst and provides clinic data collected by PCN.		X	
9	Centralized PCN staff collecting, coding and manipulating patient level data from all clinics.(non-health care related purposes)		X	
10	Completely non-identifiable data at patient or clinic level is shared with third parties – member clinics, public, etc. for information purposes (non-health care related)	No agreement required		
11	Data identifiable at the clinic level is shared with third parties – member clinics, public, etc. for information purposes (non-health care related)		X	
12	Patient level identifiable data is exchanged with AHS. (Sharing identifiable data with other custodians for secondary purposes)		X	
13	Completely non-identifiable data is exchanged with AHS.	No agreement required		
14	Disclosure to Minister or Department	No agreement required (HIA 46(1))		
15	Custodian is disclosing patient information to another custodian outside of his/her clinic for the purpose of continuity of care.	No agreement required		
16	Custodians sharing patient records within a clinic.			X

*Source: The Alberta Medical Association – [Privacy Agreement Matrix](#) (2018)