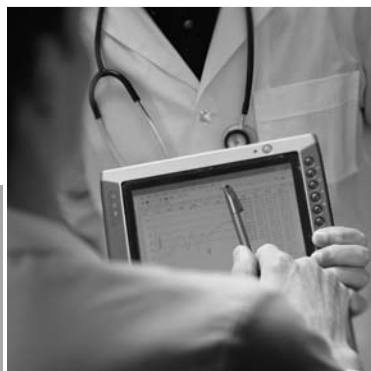


Data sharing principles

for Electronic Medical Record/
Electronic Health Record agreements



THE CANADIAN
MEDICAL
PROTECTIVE
ASSOCIATION

L'ASSOCIATION
CANADIENNE
DE PROTECTION
MÉDICALE

ASSOCIATION
MÉDICALE
CANADIENNE



CANADIAN
MEDICAL
ASSOCIATION

INTRODUCTION

This document is intended to provide some interim guidance with respect to the main principles that should be addressed when a physician is entering into an agreement for an electronic medical record (EMR) or an electronic health record (EHR) system. An EMR/EHR system typically involves a single, centralized electronic repository of medical records where access to and use of patient health information is based on a set of pre-defined access rights. Each provider of health care services, or custodian, has access to portions, or all, of the medical record to support the delivery of care to the patient.

This document recognizes that the principles applicable to data sharing may arise in many types of agreements relating to the implementation of an EMR/EHR system. For example, the data sharing principles may be applicable when physicians are creating an EMR for a group practice, when physicians are negotiating with a health authority for the creation of a region-wide EHR, and when physicians are negotiating with a service provider for the creation of an EMR (e.g. hardware, software, or hosting services). The document is intended to provide relevant principles to data sharing in multiple contexts, regardless of the type of contract that is being considered.

The principles set out in this document are not exhaustive and this document is not intended to provide any conclusions with respect to the potential risks or benefits of participation in an EMR/EHR system. Each physician will want to assess the risks/benefits in the context of his or her individual circumstances. As the custodians of very sensitive information, physicians need to carefully consider the extent to which patient information will be disclosed in the context of an EMR/EHR system. When that sensitive information is shared in an EMR/EHR, it is imperative that there be an agreement that governs who is accountable for maintaining the security and privacy of the information. A physician should also consider how patient consent will be obtained for the use/disclosure of health information through an EMR/EHR.

This document is for informational and reference purposes only and should not be construed as legal or financial advice, nor is it a substitute for legal or other professional advice. All agreements should be reviewed by the physician's own legal counsel and other professional advisers.

While the CMPA/CMA Data Sharing Principles are intended to provide guidance to physicians, the CMPA is hopeful they will assist all participants in addressing data stewardship issues associated with complex EMR or EHR systems.

CONTRACTING SCENARIOS

This document recognizes that in implementing an EMR/EHR system there may be any number of different contracting scenarios and structures. While it is not possible to consider all potential arrangements, the principles set out in this document are intended to apply regardless of the particular contracting arrangement or structure.

1. Physicians, Groups of Physicians and Physician Organizations

Physicians may organize themselves in a number of different ways when contracting for an EMR/EHR system. These include:

- 1.1 an individual physician (a “Sole Practitioner”) acting on his or her own behalf;
- 1.2 an unincorporated group of physicians (a “Group of Physicians”) which may include:
 - (a) a shared call group;
 - (b) a clinic with shared records; or
 - (c) a family health team or family health network; and
- 1.3 a physician organization, (a “Physician Organization”) which may be a corporation or which may be a partnership.

2. Service Providers, Health Regions and Hospitals

The parties with whom any of the above may contract for purposes of an EMR/EHR system may include:

- 2.1 a vendor or other service provider (e.g. software, hardware, ASP, hosting) (“Service Provider”);
- 2.2 a provincial government agency or organization such as a Regional Health Authority or Local Health Integration Network or Ministry (“Health Region”); or
- 2.3 a hospital (“Hospital”).

3. The Contracts

The principles set out in this document need to be reflected in the following agreements:

- 3.1 “Data Sharing Agreement” — in this form of agreement, a Sole Practitioner, Group of Physicians or Physician Organization on the one hand, will be contracting with a Service Provider, Health Region or Hospital, on the other hand; and
- 3.2 “Inter-Physician Agreement” — in this form of agreement, a physician will be contracting with other physicians. This may include an agreement between members of a Group of Physicians or as part of a Physician Organization. The agreement may deal with how an EMR in which the physicians are participating will be managed. Alternatively, these principles may be incorporated into a larger agreement that governs other issues with respect to the management of the group practice, clinic, or other organization (e.g. partnership agreement, shareholder agreement).

III

THE PRINCIPLES

This document provides an overview of the following principles that should be considered in a Data Sharing Agreement or Inter-Physician Agreement:

1 Ownership of Data/Data Stewardship

2 Confidentiality and Privacy

3 Security and Access

4 Accuracy and Data Quality

5 Record Maintenance Requirements

6 Quality Assurance

7 Services and Functionality

8 Termination and the Continuity of Operation of the Electronic Medical System

9 Termination for Convenience

10 Indemnification

11 Limitation of Liability

12 Representations and Warranties

13 Dispute Resolution

14 Governing Law/Forum

15 Funding

1 OWNERSHIP OF DATA/DATA STEWARDSHIP

1.1 WHAT IT IS:

For many years, the courts have recognized that the physician, institution or clinic compiling the medical records also owns the physical medical records (*McInerney v. MacDonald*, 1992). The owner of medical records has traditionally controlled issues relating to access and record retention. In the context of an EMR/EHR there is an intermingling of data from various sources which complicates the issue of ownership, as well as access and record retention.

The Data Sharing Agreement may also address the ownership of the intellectual property rights in the EMR/EHR system.

1.2 WHY IT IS IMPORTANT:

The historical approach to medical record ownership is being outpaced by EMR/EHR solutions that extend beyond the traditional model of a medical record under the custody and control of a single physician or group practice. The EMR/EHR is characterized by a sharing of custody of the information within the record based on the origin of the information item where the traditional concept of ownership is difficult to apply.

While the Data Sharing Agreement may also address the ownership of the records, the primary focus should be on ensuring that the physician has appropriate access to the personal health information, and that the physician has the ability to provide his/her patients with access to their medical record.

1.3 RECOMMENDATIONS:

Any provisions in a Data Sharing Agreement or Inter-Physician Agreement with respect to ownership of data should expressly provide that it does not prevent or interfere with a physician's ability to:

- (i) comply with the physician's obligations regarding medical records;
- (ii) access such records as otherwise set out herein; or
- (iii) transition the data to another service provider in the event of the termination of the Data Sharing Agreement.

It is possible that the EMR/EHR could be considered an asset that could be encumbered by its owner by way, for example, of a security interest in favour of third parties. The Service Provider, Health Region, or Hospital should be obligated to ensure the physician can continue to comply with his/her obligations and entitlements above, regardless of any encumbrances that may be asserted over the EMR/EHR system by other third parties.

2 CONFIDENTIALITY AND PRIVACY

2.1 WHAT IT IS:

Physicians have an ethical duty of confidentiality to their patients. In most jurisdictions, physicians and other custodians of personal information and personal health information are also bound by obligations imposed by privacy legislation.

Whether through privacy legislation or the common law, patients generally have a right of access to their personal health information and a right to ensure their information remains confidential.

2.2 WHY IT IS IMPORTANT:

When personal health information is stored in an EMR/EHR, it is accessible by a greater number of people, in addition to the physician who contributed the personal health information to the EMR/EHR. In accordance with the duty of confidentiality and/or requirements of applicable privacy legislation, physicians may have an obligation to control who has access to the personal health information they contribute to the EMR/EHR.

Physicians may have an obligation to ensure patients can access their medical records.

2.3 RECOMMENDATIONS:

The Data Sharing Agreement and any Inter-Physician Agreement should permit physicians to comply with relevant privacy legislation, the common law and provincial/territorial regulatory authority (College) policies that govern the confidentiality of patient information to ensure such an agreement reflects and protects the physician's obligations under binding policies and the law.

The Data Sharing Agreement should contemplate what patient information can be collected, used, and disclosed on the basis of implied consent. Where the applicable privacy legislation requires explicit consent for use or disclosure, this should be addressed in the Data Sharing Agreement. Similarly, the Data Sharing Agreement should contemplate where patient information can be collected, used or disclosed without patient consent. Collection, use, or disclosure that is not permitted by the legislation should be prohibited by the Data Sharing Agreement.

The Data Sharing Agreement and any Inter-Physician Agreement should not generally impose restrictions on a physician's ability to fulfill his or her legal obligations under applicable law to report confidential information such as the duty to report child abuse, the duty to report fitness to drive, and other applicable duties.

The Data Sharing Agreement and any Inter-Physician Agreement should contemplate how patient access to personal health information will be provided.

3 SECURITY AND ACCESS TO THE EMR/EHR

3.1 WHAT IT IS:

Most privacy statutes require custodians of personal health information to take all precautions to minimize the risk of loss, theft or unauthorized access to health information. Such requirements are consistent with a physician's duty of confidentiality. In some jurisdictions, where a security breach occurs, physicians may have an obligation to notify their patients.

3.2 WHY IT IS IMPORTANT:

The physician will need to comply with all applicable legal and ethical obligations relating to the security of personal health information maintained within the EMR/EHR.

3.3 RECOMMENDATIONS:

The Data Sharing Agreement should contemplate appropriate security protocols to provide access to those who require it for patient care or other purposes authorized by privacy legislation.

The Data Sharing Agreement should contemplate mechanisms for ensuring the information will not be accessed by unauthorized persons or for unauthorized purposes. Where a security breach occurs, physicians should be notified. The Data Sharing Agreement should address how notification of patients will be accomplished, where required.

If applicable law requires that patients have the right to restrict access to their personal health information available through an EMR/EHR system then the Data Sharing Agreement will need to address how these restrictions are implemented.

4 ACCURACY AND DATA QUALITY

4.1 WHAT IT IS:

In a traditional paper medical record, the physician and his/her staff may have been the only professionals who relied upon the information maintained in his/her medical record. Whereas in an EMR/EHR, multiple health professionals may rely upon the information that is maintained in the EMR/EHR. These health professionals may provide care to the patient without consulting with the physician who contributed the information to the EMR/EHR, upon which they intend to rely.

Further, most privacy statutes require custodians to maintain information that is accurate.

4.2 WHY IT IS IMPORTANT:

In delivering care to patients, health care providers need to rely upon information maintained in the EMR/EHR. The importance of accuracy is increased where the health care providers relying upon the information in the EMR/EHR may not necessarily consult with each other on a regular basis, if at all.

4.3 RECOMMENDATIONS:

The Data Sharing Agreement should contemplate mechanisms to ensure the accuracy and currency of the data maintained in the EMR/EHR. This should include mechanisms to make amendments in accordance with applicable requirements, and should include a system to notify users of previously accessed erroneous or outdated information.

5 RECORD MAINTENANCE REQUIREMENTS

5.1 WHAT IT IS:

Most jurisdictions have regulatory or legislative requirements governing the creation, retention and destruction of medical records. In some jurisdictions, specific requirements apply to electronic medical records. Medical records also provide evidence of the care that has been provided to the patient.

5.2 WHY IT IS IMPORTANT:

Physicians are required to comply with relevant privacy legislation, common law, and legislation or provincial/territorial regulatory authority (College) policies that govern the creation, maintenance and destruction of medical records.

Physicians should have access to the EMR/EHR for the required retention period specified by the College or through regulations. While the retention periods vary by jurisdiction, the CMPA recommends that members maintain clinical records for at least 10 years from the date of the last entry or for at least 10 years from the age of majority in the case of minors. The CMPA's recommendation is the same or longer than the requirement in most jurisdictions. However, in Ontario, the College recommends physicians maintain clinical records for at least 15 years.

5.3 RECOMMENDATIONS:

The Data Sharing Agreement should permit physicians to comply with applicable law as it relates to the creation, maintenance and destruction of medical records.

The Data Sharing Agreement should not limit, restrict or interfere with a physician's ability to seek medical-legal advice from the CMPA and/or legal counsel.

In the event that a physician becomes involved in a medical-legal matter, the physician will want to ensure that he or she has a record of the care provided to the patient. Documents should generally be created, maintained or retained with a view to satisfying court requirements regarding the integrity of the document and the process by which the record was created. The records should be maintained for a period that is consistent with record retention requirements and the records should be available to the physician in the event of a medical-legal matter. The Data Sharing Agreement should also address the destruction of records upon the expiration of the retention period. The Data Sharing Agreement should ensure when records are required to be destroyed, they are destroyed in the appropriate manner (e.g., physical destruction of hard drives, back up tapes).

The Data Sharing Agreement should contemplate what information will be included in the EMR/EHR in order that the content and form of the data complies with any applicable electronic record maintenance requirements.

6 QUALITY ASSURANCE

6.1 WHAT IT IS:

Quality assurance committee records are those records prepared by a hospital committee for the purpose of reviewing adverse events and evaluating the effectiveness of a hospital's practices and procedures.

6.2 WHY IT IS IMPORTANT:

It is generally accepted that in order for quality assurance programs to be successful and effective, physicians and other participants should seek satisfactory assurances that the committee's records will not be used outside of the quality assurance process. The public policy objective of encouraging health care practitioners to participate in quality assurance processes is reflected in legislation that protects quality assurance records from being disclosed in legal proceedings. Such legislation has now been enacted in all Canadian jurisdictions.

6.3 RECOMMENDATION:

The Data Sharing Agreement should contemplate how quality assurance records will be segregated from other records in order to ensure the legislative protection from disclosure is available.

7 SERVICES AND FUNCTIONALITY

7.1 WHAT IT IS:

There is substantial effort required to procure, operate and support the EMR/EHR system and the associated technical infrastructure. The scope of the services provided by the Service Provider, Health Region or Hospital as part of the EMR/EHR system needs to be documented in the Data Sharing Agreement.

7.2 WHY IT IS IMPORTANT:

There needs to be a legally binding agreement with respect to the scope of the services to be provided so that the Service Provider, Health Region or Hospital, as the case may be, can be held accountable for performance of the agreement. Due diligence will be required in selecting a Service Provider to ensure the service provider is reputable and knowledgeable.

7.3 RECOMMENDATIONS:

The Data Sharing Agreement should address:

- (a) details of the service offering;
- (b) functionality of the service;
- (c) documentation;
- (d) roles and responsibilities of the parties to the agreement;
- (e) financial terms;
- (f) vendor ownership;
- (g) transition into and out of the EMR/EHR system;
- (h) performance expectations;
- (i) service levels;
- (j) consequences of failure to meet service levels;

- (k) support and maintenance obligations;
- (l) system security;
- (m) server location;
- (n) reporting;
- (o) data back-ups;
- (p) disaster recovery;
- (q) hardware requirements; and
- (r) software requirements.

The Data Sharing Agreement should also contemplate how the physician, Group of Physicians or Physician Organization can terminate the agreement and transition to another service provider (including transition of the EMR/EHR data) in the event that they are not satisfied with the service being received. Continuity and quality of care would need to be maintained throughout any such transition period.

8 TERMINATION AND THE CONTINUITY OF OPERATION OF THE ELECTRONIC MEDICAL SYSTEM

8.1 WHAT IT IS:

A Data Sharing Agreement may typically be terminated by mutual agreement of the parties or by one party in connection with a breach of the agreement or insolvency of the other party. Additionally, a Group of Physicians may disband or a Physician Organization may be dissolved.

8.2 WHY IT IS IMPORTANT:

Continued access to the information in the EMR/EHR is required in accordance with the physician's record retention obligations as described above.

8.3 RECOMMENDATIONS:

The Data Sharing Agreement and any Inter-Physician Agreement needs to provide for the continuation of the operation of the EMR/EHR system or alternatively needs to specify what happens to the EMR/EHR records on termination of the Data Sharing Agreement or the withdrawal of a physician from a Group of Physicians or Physician Organization.

As further explained below, the agreements should contemplate maintenance of the EMRs in original form following termination, as well as continued access to the records by the physician and possible removal of the EMRs from the system. This may include the copying of medical records for any patient to which the physician provided care, the de-commissioning of the technical solution, the access to and eventual archiving of medical records and reporting to patients and other necessary bodies on the handling of the medical record as a result of the termination. The Agreement should address departure, termination, and death.

The physician will want to ensure that his or her former group practice colleagues will properly maintain the original medical records and that the physician will continue to have access to these records and the corresponding audit trail. The physician will want assurances the physicians who continue to have custody of the EMR/EHR will take all reasonable steps to prevent the information from being lost, stolen, or inappropriately accessed. The physician will also want to ensure the original records are destroyed when the applicable retention period has expired.

9 TERMINATION FOR CONVENIENCE

9.1 WHAT IT IS:

A termination for convenience clause permits a party to an agreement to terminate the agreement without cause by providing notice to the other party.

9.2 WHY IT IS IMPORTANT:

There are many reasons why a physician may need to terminate his or her participation in an EMR/EHR system under a Data Sharing Agreement or Inter-Physician Agreement. These may include the physician leaving the jurisdiction or ceasing to practice medicine as a result of disability, death, or other circumstances.

9.3 RECOMMENDATIONS:

In addition to the right to terminate the Data Sharing Agreement for breach or insolvency of the other party, a physician should ensure that the Data Sharing Agreement and Inter-Physician Agreement provides the physician with the right to terminate the physician's participation in the EMR/EHR system without cause by providing written notice to the Physician Organization, Group of Physicians, Service Provider, Health Region, Hospital or other party as applicable.

The Data Sharing Agreement should make clear that certain provisions of the agreement affecting the terminating physician, such as indemnities and confidentiality obligations, survive termination, and that such termination does not affect the rights and obligations applicable to any other non-terminating parties.

10 INDEMNIFICATION

10.1 WHAT IT IS:

An indemnity is intended to allocate to a contracting party risk and responsibility under an agreement and typically requires a party to contractually assume certain liability either (i) for matters that are the responsibility of such party; or (ii) in connection with that party's breach, negligence or other misconduct.

10.2 WHY IT IS IMPORTANT:

Liability may arise in a number of scenarios in connection with an EMR/EHR system in the context of a Data Sharing Agreement. For example and without limitation: (i) an EMR/EHR system may go down and a physician may be deprived of access to the information needed to treat patients; (ii) patient information may be improperly disclosed to or accessed by a third party; or (iii) an EMR/EHR system may contain inaccurate information that might be unknowingly relied upon by a physician or other health care provider providing care. Absent an indemnity in favour of the physician dealing with these issues, it is not clear how liability would be apportioned for harm caused to a patient arising from these scenarios.

In the context of a Data Sharing Agreement, a physician may be asked to give an indemnity in favour of a Group of Physicians, Physician Organization, Service Provider, Health Region or Hospital, for example, in connection with that physician: (i) making inappropriate disclosure of, or permitting unauthorized access to patient information; or (ii) submitting incorrect patient information into an EMR/EHR.

It is important to note the party giving an indemnity is typically liable for a broader range of damages under the indemnity than would be the case if the party merely breached a contract.

Generally speaking, when considering providing an indemnity and its scope, a party should be liable for those acts for which he or she would be responsible at law, which usually amounts to those acts or omissions over which the party has control.

Please note an individual physician may remain ultimately responsible to a patient notwithstanding the physician's participation in a Group of Physicians or Physician Organization and consequently the indemnities referred to above would need to appear in the Data Sharing Agreement between the Physician Organization and the Service Provider, Health Region, or Hospital, for example, whereby one or both indemnifies the individual physician who is not otherwise a party to the Data Sharing Agreement. An indemnity does not relieve the physician of liability if a patient is harmed due to inaccessible or incorrect data. However, in the event of such harm and where the patient brings a claim against the physician, the clause will permit the physician to look to the other party for indemnification of the damages.

10.3 RECOMMENDATIONS:

- (a) A physician should seek to be indemnified in connection with:
 - (i) any improper disclosure or use of personal health information by a Physician Organization, Group of Physicians, Service Provider, Health Region, Hospital or other party to the Data Sharing Agreement or Inter-Physician Agreement; and
 - (ii) a failure of an EMR/EHR system that results in harm to a patient.
- (b) Any indemnities granted by a physician or by a Group of Physicians or Physician Organization should be limited to liability resulting from those acts over which the physician, Group of Physicians or Physician Organization (or those for whom they are responsible at law) have control. Any indemnification provision should provide for some mechanism of notification, co-operation and the right of each party to retain its own counsel, and should provide the party granting the indemnity with the opportunity to approve any settlement. When granting an indemnity, the physician should be mindful that the CMPA does not consider itself bound by indemnities given by members to third parties. However, where an indemnity in favour of a third party specifically relates to the practice of medicine and the direct provision of patient care by the member, the member may be eligible for assistance from the CMPA with respect to the member's actions. The CMPA will not necessarily assist members with respect to promises of indemnification for administrative or non-medical care acts or omissions, which the physician may assume as an obligation under a Data Sharing Agreement or Inter-Physician Agreement.

Where multiple health professionals are parties to the Data Sharing Agreement, it may be advisable to seek indemnification from each of the professionals.

Any indemnity given by a physician or given by another for the benefit of the physician should always be reviewed by legal counsel for the physician. Particular consideration should be given to an indemnification that is made by a physician organization, which may create a joint and several contractual obligation on the part of all physicians in the organization. It will be necessary for the legal counsel to review the clause together with the entire contract.

11 LIMITATION OF LIABILITY

11.1 WHAT IT IS:

A party to a Data Sharing Agreement or Inter-Physician Agreement may seek to limit its liability for damages in connection with the agreement by including a limitation of liability clause. These clauses typically purport to limit liability to direct damages and exclude entirely certain other types of damages such as indirect, consequential, special and punitive damages.

11.2 WHY IT IS IMPORTANT:

From the perspective of a physician considering participation in an EMR/EHR system, both the nature of the potential risks and the scale of exposure associated with such participation are not entirely clear. For example, there is some uncertainty with respect to what damages might be claimed in connection with either an improper release of personal health information or the use of incorrect personal health information. Additionally, as noted above, software or hardware malfunctions resulting in “down time” for an EMR/EHR system could also give rise to liability.

A limitation of liability clause in favour of a Service Provider, Health Region or Hospital might limit the rights of a physician, Group of Physicians or Physician Organization to claim damages arising from a breach of the Data Sharing Agreement by the other party or the other party’s negligence. The clause may also restrict the physician’s ability to claim damages resulting from a claim brought by a third party against the physician, Group of Physicians or Physician Organization, as a consequence of an act or omission of the other party to the Data Sharing Agreement.

11.3 RECOMMENDATIONS:

- (a) A physician should not permit any other party to the Data Sharing Agreement to limit or exclude their liability for any acts or omissions that could result in liability to a patient or some other third party. For example, where possible, a physician should not permit a Service Provider, Health Region, or Hospital to limit their liability in connection with the improper disclosure or use by the Service Provider, Health Region or Hospital of personal health information.
- (b) The physician should try to include a limitation of liability clause in his or her favour with a view to limiting the physician’s potential liability in connection with the physician’s breach of the Data Sharing Agreement or the physician’s negligence in connection with the Data Sharing Agreement. As a general statement, it is typically difficult to extract a one-way limitation of liability clause in a contract unless the party getting the benefit of that clause has substantially greater bargaining power. It is more realistic that if a physician requests a limitation of liability clause in his or her favour, the other party will insist upon similar protection.
- (c) Any limitation of liability provision should be reviewed by legal counsel for the physician. It will be necessary for legal counsel to review the clause together with the entire contract.

12 REPRESENTATIONS AND WARRANTIES

12.1 WHAT IT IS:

A representation is a statement of fact (present or past) and a warranty is a promise that a particular fact is true. In the context of a Data Sharing Agreement, a party may give various representations and warranties, which may relate to the accuracy of personal health information contributed to an EMR/EHR system, how patient consent is obtained, and/or compliance with applicable law.

12.2 WHY IT IS IMPORTANT:

A party will be liable to other contracting parties if he/she makes a representation and warranty that is not accurate or that is not fulfilled.

12.3 RECOMMENDATIONS:

- (a) A physician should seek representations and warranties from other parties to an agreement as to:
 - (i) their existence, status and authority to enter into the agreement, (ii) the enforceability of the agreement, (iii) the fact that the entering into and performance of the agreement does not contravene any laws, constating documents or any agreements to which they are a party, and (iv) other matters specific to the subject matter of the agreement.
- (b) A physician should seek representations that the service provider will not infringe any third party intellectual property rights.
- (c) A physician should not give any representations or warranties with respect to matters over which the physician does not have control or in respect of which the physician does not have knowledge. The physician should ensure that any representation or warranty given by the physician is true and correct. To the extent that a physician gives representations and warranties they should, where possible, be limited to the knowledge of the physician, should be qualified by a concept of materiality and should have a finite survival period.
- (d) Any representations and warranties given by a physician should be reviewed by legal counsel for the physician, together with the entire contract.

13 DISPUTE RESOLUTION

13.1 WHAT IT IS:

A Data Sharing Agreement or Inter-Physician Agreement may include a dispute resolution and/or arbitration provision to provide a process for the resolution and settlement of disputes arising under the agreement as an alternative to court proceedings.

13.2 WHY IT IS IMPORTANT:

Alternative dispute resolution and/or arbitration can be advantageous in that it is generally less expensive, can be more efficient, and is more private than court proceedings.

13.3 RECOMMENDATIONS:

- (a) The dispute resolution and/or arbitration clause should not preclude assistance from the CMPA or the physician's personal legal counsel to ensure that the physician's interests are adequately represented should a dispute arise.
- (b) The dispute resolution and/or arbitration clause should not preclude the physician from seeking injunctive relief from a court where there is risk of immediate or continuing harm.

14 GOVERNING LAW/FORUM

14.1 WHAT IT IS:

Parties to an agreement may specify their choice of law which is to be applied in interpreting and enforcing the agreement. The parties may also specify the forum or location where any dispute is to be heard.

14.2 WHY IT IS IMPORTANT:

Where there is no choice of law or forum set out in the Data Sharing Agreement, then the court where an action is commenced may assume or decline jurisdiction. The physician, Group of Physicians or Physician Organization may be required to resolve a dispute in a location that is more convenient and more favourable to the Ministry, Service Provider, Health Region or Hospital that commenced or is responding to the action.

14.3 RECOMMENDATION:

Any Data Sharing Agreement should include a governing law clause that provides that the governing law and forum is stipulated to be the Canadian province or territory in which the physician practises and that any proceedings take place in a location that is convenient for the physician.

15 FUNDING

15.1 WHAT IT IS:

There will be costs associated with the operation, maintenance and support of an EMR/EHR system.

15.2 WHY IT IS IMPORTANT:

The costs associated with the operation, maintenance and support of an EMR/EHR system will be significant.

15.3 RECOMMENDATIONS:

The funding and support infrastructure for physicians for the EMR/EHR system should meet the needs of physicians.

Where physicians are considering the creation of a corporation or partnership for the purposes of the EMR/EHR system, it may be prudent to consult with a tax professional to ensure the corporation/partnership is structured to the advantage of the physicians involved.

Prepared by the CMPA in conjunction with CMA, for CMA Health Information Technology Committee



THE CANADIAN
MEDICAL
PROTECTIVE
ASSOCIATION

L'ASSOCIATION
CANADIENNE
DE PROTECTION
MÉDICALE

Mailing Address: P.O. Box 8225, Station T, Ottawa, ON K1G 3H7
Street Address: 875 Carling Ave., Ottawa, ON K1S 5P1
Telephone: 613 725-2000, 1 800 267-6522
Facsimile: 1 877 763-1300 *Website:* www.cmpa-acpm.ca

Adresse postale : C.P. 8225, Succursale T, Ottawa ON K1G 3H7
Adresse civique : 875, av. Carling, Ottawa ON K1S 5P1
Téléphone : 613 725-2000, 1 800 267-6522
Télécopieur : 1 877 763-1300 *Site Web :* www.cmpa-acpm.ca