Key points to consider

- Since the regulation of eRecords is continually evolving and can be complex, physicians should be familiar with the legislation, regulatory requirements, technological standards, and software options that apply to eRecords. For advice and information, doctors may consult with their colleagues; regulatory authority (College); provincial or territorial privacy regulator; provincial, territorial, or national medical association; and the CMPA.
  See page 5, Introduction.

- An eRecords system should meet the needs of a physician's practice as well as any applicable legal and regulatory requirements. Advice from a qualified service provider or an experienced user may help physicians in selecting and setting up an EMR. In some cases, physicians may be required by a hospital, regional health authority, or provincial or territorial government to use a specific eRecord system (such as an EHR).
  See page 7, Selecting an appropriate system.

- Physicians should consider having an agreement for a shared EMR or EHR. The CMPA’s Data Sharing Principles and the template titled, Contractual Provisions for Data Sharing, can be reviewed and serve as a model. An agreement should address issues such as ensuring a physician’s continued access to patient records after leaving a group practice or terminating agreements with external service providers. Physicians are also urged to require that their employees and staff members sign a confidentiality or non-disclosure agreement to ensure everyone understands their obligations in keeping patient information secure and confidential.
  See Appendix C, page 42, Data Sharing Principles; Appendix D, page 53, Contractual Provisions for Data Sharing; and Appendix E, page 63, Confidentiality/Non-Disclosure Agreement.

- Physicians should understand their obligations when they participate in an EHR system or when asked to upload portions of their office EMR to an EHR operated by hospitals, regional health authorities, provinces or territories, etc.
  See page 42, Data sharing and inter-physician arrangements.

- Physicians should consider speaking with patients about including personal health information in an eRecord. Patients’ express consent may be necessary when their personal information is shared with others for purposes other than providing healthcare (i.e. outside the circle of care).
  See page 12, Patient consent and rights to access.
Reviewing the security requirements of eRecords should be a priority. This includes ensuring applicable security and secure backup requirements are available, and all personal health information is encrypted. Further, eRecords should have an audit trail that can appropriately track if the record has been accessed or altered. eRecords should allow physicians to control access to patient information, including having “lock-box” or “masking” features if patients request that information be withheld from some healthcare providers. See page 15, Security and privacy issues.

Physicians need to consider appropriate security measures and procedures when communicating personal health information via email or other electronic means. See page 22, Sending and transferring records.

Retention periods for medical records are just as important with eRecords as they are for paper records. Once the required retention period for medical records has expired, the information in the eRecord can be appropriately destroyed. See page 24, Destroying and disposing of records.

Physicians will want to assess the implications of relying exclusively on patient-supplied electronic personal health records (sometimes referred to as “patient health records” or “PHRs”). Doctors should be cautious as patients typically control what information is included in PHRs. If using or accessing personal medical record services, or communicating with patients via portals or websites, physicians will want to discuss any privacy risks with patients. Social media, wireless devices, networks, and cloud computing services must be used with caution. Due to their public or shared nature, there is a potential to lose control of information that is posted or stored. Security and privacy issues must be considered to ensure there is no unauthorized access to, or disclosure of, personal health information. See page 30, Emerging issues.
Introduction

Electronic medical records (EMRs) and electronic health records (EHRs) have become an integral part of healthcare delivery in Canada. They can improve the management of individual patient care and bolster the overall effectiveness of the healthcare system.

Implementing and using EMRs and EHRs (eRecords) can raise a number of technological issues and medico-legal risks.

The regulation of eRecords continues to evolve and can be complex. Physicians should learn about applicable legislation, regulatory requirements, technological standards, and software options. For advice and information, they might consider consulting with their colleagues, medical regulatory authority, provincial or territorial privacy commissioner (or the equivalent), and provincial or territorial medical association, and with the CMPA.

Distinguishing between EMRs and EHRs

An EMR generally refers to an electronic version of the traditional paper record that physicians have long maintained for patients. The EMR may be a simple office-based system, but is more likely a sophisticated, shared electronic record accessible to those within a group practice, healthcare facility, or a network of health professionals (e.g. treating physicians, other healthcare providers, information managers, etc.).

EHRs are typically maintained by a hospital, health authority, or provincial health ministry and generally include a variety of repositories of patient data. They are usually accessible by several authorized parties from a number of places of care.

An EMR is an electronic version of the paper record generally maintained by doctors for their patients. It may be as simple as an office-based system, but is more likely a shared record that connects health professionals through a network.

An EHR is maintained by a hospital, regional health authority, or provincial or territorial government and typically includes a spectrum of repositories of patient data.
The term “eRecord” refers to the wide range of electronic record management systems available to physicians and other custodians of patient health information.

Distinguishing between custodians, information managers, and service providers

Under privacy legislation, individuals and entities that have custody and control of personal health information are ultimately responsible for complying with the legislation. In some jurisdictions these individuals and entities are called custodians. In other jurisdictions the legislation may use the terms trustee or organization. For example, a hospital is the custodian of an EHR used in the institution, and physicians are the custodians of the EMR used in their private practice.

Custodians’ responsibilities generally include collecting, using, or disclosing personal health information only with the consent of the patient, or as required or permitted by law. They must also take reasonable steps to maintain the administrative, technical, and physical safeguards that protect the confidentiality of the information. They are responsible for protecting the information from reasonably anticipated threats to its security or integrity, or from loss, unauthorized access, use, disclosure, or modification.

Physicians have a professional duty of confidentiality to patients, and this duty is augmented when physicians are also custodians of EMRs. In accordance with the duty of confidentiality, a physician should not disclose confidential patient information unless the patient has consented to the disclosure, or the disclosure is authorized or required by law.

Custodians may delegate some or all of their duties under privacy legislation to agents or affiliates. For example, when a physician practises within a hospital or clinic, the facility is the custodian of the personal health information. However, typically hospitals and clinics authorize a physician to act on the institution’s behalf for the purposes of assisting it in fulfilling its duties under the applicable privacy statute. If that occurs, a physician will then have similar obligations as the custodian under the applicable privacy legislation.

Distinguishing between the responsibilities of custodians and affiliates can be complex.

In one context, a physician may be considered to be an affiliate or agent of the hospital or regional health authority that has legal custodianship over the record. For example, when a request is made by a patient or third party for a copy of a medical record, the custodian will generally be responsible for responding to such a request.

In other contexts, however, the same physician may also have similar but separate legal and professional obligations to protect the confidentiality of the patient’s personal health information. Despite being an affiliate, the physician will generally be expected by privacy commissioners, regulatory bodies, and courts to meet certain obligations when it comes to maintaining patient privacy. Physicians should consider that irrespective of their role as a custodian or affiliate, they have a professional obligation to take reasonable steps to protect the personal health information of patients.

In fulfilling their duties, custodians of eRecords are often assisted by information managers or third party service providers. A service provider may offer information processing, storage, retrieval, or disposal services; data transformation or information management services; or information technology functions.

Some privacy legislation specifies that when engaging a service provider, a custodian must enter into a written agreement. Despite having such an agreement, the custodian remains ultimately responsible for complying with privacy legislation. As a result, if a service provider contravenes an obligation under privacy legislation, it is usually as if the custodian breached the legislation directly.
Selecting an appropriate system

- Access the needs of the practice and choose a system or software program that best meets those needs.

- Consider if and how the software program will operate with other eRecord systems, both current and future.

- Consult with provincial, territorial, or national medical associations, especially those with dedicated eHealth programs and services, which may assist with compliance with provincial regulations and expectations.

- Seek professional assistance from the software vendor or an information technology consultant, if appropriate.

- Consult with colleagues who have implemented an EMR.

- Consult personal legal counsel when dealing with business issues, including equipment leases or purchase agreements.

Choosing an electronic record system

In choosing an appropriate system, physicians should select a system that meets the needs of their practice, and the legal and regulatory requirements in their jurisdiction. In addition, they should consider how the selected system will operate with other eRecords systems. If linking to an EHR, doctors should be aware of compatibility requirements that may be prescribed by health authorities, healthcare institutions, or facilities.

To help in making the selection, professional help is available from a variety of sources including technology vendors; information technology consultants; provincial, territorial, or national medical associations; or local physician technical support programs, if available. Colleagues who have implemented an EMR may also provide useful information. Some jurisdictions have a pre-approved vendor list to make the selection process easier and might also provide funding to offset some or all of the acquisition and implementation costs.

The system vendor will likely require that the physician or physician group sign a software licence, which is a legal agreement governing the use and distribution of the copyright-protected EMR software. While granting permission to use the software, licence agreements also impose certain obligations and restrictions on the use of the product. Before signing, physicians should be aware of its terms. They are strongly encouraged to contact their personal legal counsel, or provincial, territorial, or national medical association for advice.

The system vendor may provide computers, tablets, PDAs (personal digital assistants), servers, or other
equipment to be used with the particular eRecord system. The equipment might be purchased or leased. If leased, physicians should be aware of the terms of the lease, including any early termination payments or penalties. If purchased, doctors should be familiar with the terms of the purchase agreement including any applicable warranties. Physicians are encouraged to consult their personal legal counsel before entering into any equipment lease or purchase agreement.

In addition to choosing the right system (including software and hardware), a number of practical points should be considered including:

- How will workflow be maintained while the EMR is being installed and records are being converted? How will patient care and record-keeping be managed during the transition stage? What should be done with paper records converted to electronic format or records that are partially converted?
- Is a privacy impact assessment required?
- What training will be conducted for physicians and their staff, and who will provide ongoing technical support and training, including during and well after implementation?
- What processes and practices will be put in place, both from a technical standpoint and from an office policy point of view, to ensure security and privacy of patient records?
- How will data integrity be ensured (e.g. audit trails, backup and recovery systems, quality assurance procedures such as audits, etc.)?
- How will the system be maintained, including making updates and upgrades?
- How easy is it to input information to the EMR and migrate information to another EMR? How will metadata be protected from being compromised or otherwise changed if data is being migrated?
- Does the system permit information to be printed for patients in an understandable format?
- What system will be in place to ensure records are appropriately destroyed after the required retention period?
- How will physicians’ continued access to patient information for the applicable retention period be ensured?
- What are the necessary agreements to be signed? These may include data sharing agreements (agreements setting out the terms for the sharing of electronic health information) with a health authority or government ministry operating an EHR. In addition, agreements may be required with service providers who will offer information technology services. When the EMR is being introduced in a group practice, it may be advisable to have an inter-physician agreement between members of the group.

**Working with decision support systems**

Some eRecords are equipped with decision support tools embedded in the software that prompt the user to consider certain factors or possible decisions in response to the inputted data. The software may also include alerts, flags, or instant messaging capabilities to assist physicians in diagnosing, treating, and monitoring their patients’ clinical conditions or managing their prescriptions.

A decision support tool in an eRecord may present unique and challenging issues that should be considered before buying the system. For example, physicians should determine if the system permits individual users to disable or disregard the decision support tool. If this is the case, doctors will want to consider the availability of a robust audit trail that tracks the advice that is accepted or rejected. Although each system functions differently, users should know in advance how the particular decision support tool operates and whether the information generated is reliable.

Decision support tools must not be used to replace a physician’s own judgment. Each suggestion offered by the decision support tool should be reasonably considered and assessed based on the circumstances of each case.

Physicians will want to consider documenting in the patient’s record their reasons for following or ignoring a suggestion provided by the decision support tool or
for acting on or disregarding an alert, flag, or instant message. If the diagnosis suggested by the software was ignored and proves in hindsight to be accurate, the physician may be required in the course of a legal action or College complaint to justify why the information was disregarded.

Similarly, ignored alerts, flags, or messages notifying the physician of abnormal test results or prescription errors could be used as evidence of negligence or professional misconduct in civil or College proceedings. Documentation of the physician’s rationale for disregarding a suggestion or notification would be helpful in the event of a College complaint or legal action. Similarly, if the decision support tool is disabled, physicians will want to document their rationale for doing so.

Developing and implementing policies

When incorporating an eRecord system into a medical practice, internal policies should be established to govern issues such as data integrity; consent; security; access; and transfer and destruction of records. In a group practice, policies might be developed as a team to ensure all staff members are engaged in the process and aware of the importance of privacy in the eRecord environment. In addition, staff should be appropriately trained to ensure they understand the policies and their obligations.

While the details of such policies may vary from practice to practice, it remains vital that in each practice the policies are applied consistently and in keeping with underlying privacy principles. Careful documentation of decisions and the steps that were followed will assist in defending those actions if there is a complaint or civil action.
Regulation of electronic records (eRecords)

- Become familiar with medical regulatory authority (College) requirements, legislation, regulations, or other expectations regarding the use of eRecords.

- Review privacy legislation as, in some provinces and territories, it may contain specific provisions or expectations regarding eRecords.

Regulations and guidelines on the creation, maintenance, retention, and destruction of traditional paper medical records generally extend to eRecords. As well, additional requirements may apply specifically to records in an electronic format. These will be determined primarily by provincial, territorial, or federal governments, and Colleges.

Privacy legislation

Privacy legislation governing the collection, use, and disclosure of personal information is applicable in all provinces and territories. In many provinces, the
legislation includes provisions that apply specifically to the privacy of electronic health records. Legislation governing electronic commerce may also be applicable and typically deems electronic records to be equivalent to paper records, regulates the use of electronic signatures, and addresses other legal requirements.

Privacy legislation obliges physicians and other custodians of patient information to take reasonable precautions to minimize the risk of loss, theft, or unauthorized access or use of that information. Some privacy legislation further requires custodians to implement specific safeguards when maintaining patient information in electronic form.

**Regulatory authority (College) requirements**

Several Colleges have policies, bylaws, rules, or regulations concerning eRecords that include some or all of the following:

- The system is capable of visually displaying and printing the recorded information for each patient promptly and in chronological order.
- The system is capable of displaying and creating a printed record in a format that is readily understandable to patients seeking access to their records.
- The system provides a way to access the record of each patient using the patient’s name and medicare health number, if applicable.
- The system maintains an audit trail that:
  - records the date, time, and identity of the user when records are accessed.
  - records the date and time of each information entry for every patient and the identity of the user making the entry.
  - indicates any changes in the recorded information and the identity of the user making the change.
  - preserves the original content of the recorded information when changed or updated.
  - is capable of being printed separately from the recorded information for each patient.
  - The system requires robust security features (including encryption, use of passwords, and access controls) to protect against unauthorized access.
  - The system automatically backs up files and allows the recovery of backed-up files or otherwise provides reasonable protection against information loss, damage, and inaccessibility.

While not all of these requirements may apply in every jurisdiction, every jurisdiction has express requirements for the creation and maintenance of medical records that must be followed.
Patient consent and rights to access

- Consider notifying patients that their health information will be stored in an eRecord, even if notification is not strictly required.

- Personal health information can generally be shared within the “circle of care” for the purpose of providing healthcare. (The group of people responsible for providing care to the patient is informally referred to as the circle of care.)

- Patients may be permitted to restrict access to their personal health information, for example by using lockboxes, masking, blocking, giving a disclosure directive, or opting-out.

- Express consent will often be required when disclosing patient information from an eRecord to a third party for purposes other than providing healthcare.

- Consider a written agreement with service providers documenting privacy obligations.

- When patients request access to their health information that is stored in an eRecord, provide it to them in a timely way and in a suitable format.

As with any patient information, physicians generally do not need express consent to include patient health information in an eRecord, or to share patient information with other healthcare providers for the purpose of providing treatment. Physicians can generally rely on a patient’s implied consent to share personal health information within the circle of care, which includes the healthcare professionals who need to know the information to provide care. For example, physicians in a shared call group can rely on a patient’s implied consent to exchange personal health information between them for the purpose of providing healthcare to the patient.

Privacy legislation also generally permits custodians to share personal health information with an agent or affiliate on the basis of implied consent. This may occur when a physician practising within a healthcare facility that is itself a custodian, is authorized to act on behalf of the facility for the purposes of fulfilling the custodian’s privacy obligations. Another example is when physicians hire a service provider (or information manager) to assist with their medical practice. In both of those cases, the custodian remains accountable for the personal health information in the hands of the agent. However, both the agent and the custodian share a professional obligation to adequately protect the information. Members should ensure that hired service providers understand the necessity of protecting personal health information and take the appropriate steps. Members are encouraged to have a written agreement confirming agents understand their obligations. In some jurisdictions, a written agreement is required by privacy legislation or the privacy commissioner.
Although consent can usually be implied, in some circumstances it may be prudent to notify patients that their health information will be stored electronically, particularly if stored in a shared EMR or an EHR where a number of people have access.

Express consent should be obtained whenever a physician is asked to disclose patient information from an eRecord:

a) to a third party outside of the circle of care, such as an insurer or employer who is not an agent of the physician

b) if the information will be used for a purpose other than treating the patient and it is not permitted or required by law

Disclosure in the latter case is often referred to as a secondary use of personal health information. Other examples of secondary uses include marketing, conducting research, or providing personal health information to an organization or government body for the purpose of health system planning. Some privacy statutes expressly permit the use of health information for these secondary purposes. Members will want to familiarize themselves with the exemptions in the relevant privacy legislation. When appropriate, patient information should be de-identified as much as possible before being used for purposes other than providing healthcare.

When express consent is required, it is generally prudent to ask the patient to execute a consent form. If verbal consent is obtained, it should be documented in the patient’s medical record. Regardless of the approach, the patient’s consent should be informed.

Patients can seek to restrict access to their information by others

Patients may ask that access to their health information in an eRecord be limited, even if it is for healthcare purposes. This can be done through a process called a lockbox or masking. Physicians with EMRs should consider whether their system permits masking, how they will manage requests for a lockbox or masking, and what their obligations are for informing recipients that the health information may be incomplete. If storing patient information in
a shared EMR or an EHR, members should ask those responsible for the shared system how to handle lockbox or masking requests.

Some eRecord systems may not permit masking of portions of the record, or there may be instances where doing so would be inappropriate. In those instances, consideration might be given to blocking access to the entire record. If a patient has requested that certain information be masked but the EMR software does not have the functionality to do so in the manner requested, this should be explained to the patient, if appropriate, and consent should be obtained before blocking the entire record. Physicians will also want to explain to patients that the masking of some or all personal health information could result in another healthcare professional not being aware of diagnoses, treatments, or laboratory results. These discussions should be fully documented in patients’ records.

In jurisdictions with provincial EHRs, there may be disclosure directive or opt-out processes that permit individuals to control their information. Although the scope and restrictions on the directive or opt-out may vary, they can relate to the type of personal health information contained in the EHR, the purposes for which personal health information may be disclosed from the EHR, the persons or classes of persons who may access the personal health information in the EHR. Although some jurisdictions require that all prescribed personal health information be uploaded to the EHR, patients may still limit or refuse the use or disclosure of specific information. This can be accomplished by a masking process that blocks the information from being displayed in the EHR when it is accessed by individuals who do not have patients’ authorization to see the information.

When such a disclosure directive or opt-out process exists and is recognized by law, it may restrict a healthcare provider’s access to the information, except in certain circumstances such as incapacitation, in an emergency, or with the person’s express consent.

Patients’ access to their own health information

Patients generally have a right to access their own health information. As a result, physicians must have a way to give patients access to their health information that is stored in an eRecord, and the information must be provided in a format that patients can understand. Physicians may charge a reasonable fee for providing copies of records to patients.

Despite this obligation, there are circumstances when physicians may be concerned about providing access to certain information. For example, a psychiatrist may believe it would be harmful for a patient to review information related to the psychiatrist’s impressions or analysis of the patient’s mental health status. In these exceptional circumstances, this concern can be addressed by segregating the potentially harmful information and granting the patient access to the rest of the record.

Physicians may wish to consult with their system vendor for information on how to segregate records in this manner. The CMPA can also be contacted for advice on responding to access requests in these circumstances.
Security and privacy issues

- Make sure the eRecord system is equipped with robust security features including access controls based on the user’s role and responsibilities; automatic logout; and anti-virus, malware, and spyware software. Consult the system vendor or provincial, territorial, or national medical association for assistance in choosing appropriate security features.

- Place encryption protection on all computer systems and portable data storage devices containing personal health information. Some privacy commissioners (or equivalent individuals with privacy oversight) and Colleges have stated that physicians and other custodians must encrypt patient information stored on mobile devices.

- Consult with the privacy commissioner or ombudsman, if required or helpful, on how to conduct a privacy impact assessment.

- Be vigilant about addressing security and privacy issues both when an eRecord system is implemented and on an ongoing basis. Issues such as physical security, secure backup of records, and the periodic review and updating of policies and training remain important considerations.

- Conduct periodic privacy audits of the EMR system to ensure it continues to comply with privacy obligations.

As with paper records, physicians have an ethical and legal obligation to keep all patient information confidential. However, when patient information is stored in a shared eRecord, it is likely accessible to a greater number of people than a traditional paper record and as a result protection is more complex. Robust security features and policies must ensure information in an eRecord is only accessible within the circle of care to provide patient care, or for other purposes that are authorized by law or with the express consent of the patient. This can be achieved through the use of secure login protocols. In addition to having security mechanisms that limit access to authorized persons only, where possible it is prudent to consider equipping the eRecord system with controls that restrict access based on the user’s role and responsibilities. Locating printers and fax machines in areas with restricted access, having an automatic feature that logs the user out after a period
of inactivity, and installing anti-virus, malware, and spyware software are other ways to protect patient information. Consult with the system vendor or provincial, territorial, or national medical associations for assistance in choosing appropriate security features.

In addition to addressing security and privacy issues when an eRecord system is implemented, it is equally important to ensure that these same issues are periodically assessed and revised, as necessary. The physical security, secure backup of records, and the periodic review and updating of policies and training remain important even after an eRecord system is implemented.

The CMPA strongly recommends that physicians consider implementing encryption protection on all computer systems (including desktops and laptops) containing personal health information. Those who store patient information on portable data storage devices such as tablets, smartphones, USB flash drives, and portable hard drives should also consider installing encryption software on these devices. Some privacy commissioners and Colleges have stated that physicians and other custodians must encrypt patient information stored on mobile devices. As new technologies evolve, physicians should continue to consult vendors and privacy commissioners, among others, about the appropriate degree of security.

When using a wireless network to access and send patient information contained in an eRecord, physicians should consider how to ensure that the network is secure. Particular caution should be paid to remotely accessing eRecords using a wireless device, including smartphones and tablets. Appropriate security controls should be installed on mobile devices and wireless networks to prevent unauthorized access to eRecords.

Additional requirements may apply when transmitting a patient’s personal health information outside of the province or territory where it was collected. For example, patient notification may be required when using a service provider outside of Canada for transcription of dictation.

Privacy impact assessments and audits

Some jurisdictions require a privacy impact assessment before changes are made to an EMR system. While the assessment may not be a legal requirement in every jurisdiction, it is a prudent and valuable procedure. These assessments identify and minimize the privacy risks associated with the implementation of the EMR system. Physicians are encouraged to consult with their privacy commissioner or ombudsman on how to conduct a privacy impact assessment. Some privacy commissioners have published guidelines. In some jurisdictions, it may be necessary to submit the completed privacy impact assessment to the privacy commissioner for review and comment.

Once the EMR system is installed, it is prudent for practitioners to periodically conduct privacy audits. These ensure that access to patient records in the eRecord has been restricted to authorized individuals for authorized purposes. With regular audits, unauthorized access can be identified early and managed appropriately (see the following section, Maintaining data integrity, for further discussion of audits).

Transportation of data

There are risks with physically transporting electronically stored personal health information. The Canada Border Services Agency and some foreign governments have stated they have unequivocal authority to search and potentially seize electronic devices that a traveller may be attempting to bring into the country. In some cases, information obtained in a border search may be broadly shared. Obviously, this raises concerns for the privacy and security of patients’ personal health information that is stored on a device and subjected to a border search.

Members are encouraged to contact the CMPA before physically transporting or electronically transmitting health information across borders.
Maintaining data integrity

- Ensure the eRecord has an audit trail that clearly indicates alterations but does not obscure the original record. Comply with applicable policies, by-laws, or regulations that stipulate audit trail functionality.
- Back up electronic patient information, possibly daily or weekly.
- All healthcare providers using the eRecord, especially in a shared eRecord environment, should make reasonable efforts to know who contributes to it and how often it is being accessed.
- In the event of a legal proceeding, physicians employing an electronic signature device will want to be able to explain how the device works and attest to its reliability.

Physicians have a legal obligation and professional duty to their patients to keep records that are accurate, complete, and up-to-date. With electronic record systems, physicians must ensure the authenticity and integrity of both the electronic data and the process by which it was created. Some measures may be required by legislation or by the Colleges.

Audit trails

An eRecord should have an audit trail detailing who accessed the record, their activities, and any alterations. The audit helps demonstrate that the information is authentic and reliable by providing a technical log of the activity in the record through the creation of “metadata.”
Physicians should comply with all applicable policies, by-laws, or regulations that stipulate the audit trail functionality. Generally, the system should enable the physician to:

- identify who has accessed the record
- identify what, if any, alterations have been made
- identify who made a specific alteration and when
- print and view a copy of the unedited, original version of the record (any amendments should be separately visible without permanently deleting the original entry)
- demonstrate that the chain of custody of the record or entry is sound

**Editing, deleting, correcting records**

Physicians have a responsibility to maintain accurate records. Fulfiling this responsibility includes complying with requests from patients seeking access to their record. Patients have the right to access their records and to request a correction or amendment. These requests should be reasonably accommodated. Physicians, however, are generally entitled to refuse requests to correct medical opinions or information that is necessary for clinical purposes. The decision must be made on a case-by-case basis and in keeping with any applicable legislation or College requirements. For example, privacy legislation may set timelines for responding to patient requests, establish parameters for granting or refusing correction requests, identify how the record is to be amended, and require certain steps be taken once a request is granted or refused. Doctors should be familiar with those provisions and comply with them.

Physicians should also be aware that multiple healthcare providers may be treating the patient and making entries into the eRecord. If a patient requests that the physician correct or amend an entry made by another healthcare provider, it would be prudent to direct the patient’s request to that provider. If the entry is relevant to the treatment the doctor is providing or has provided to the patient, the doctor may consult with the other healthcare provider to determine whether the change should be made and by whom.

If refusing a patient’s request for a change, physicians should keep the following in the record: a copy of the request, the letter of refusal setting out the reasons for refusing, and any communications received or sent via email or other electronic means. Some privacy legislation also requires that physicians retain copies of any letters of disagreement the patient sends upon learning of a refusal. Physicians are encouraged to contact the CMPA for assistance in these circumstances.

Physicians also have a general duty to correct inaccurate information in a patient’s record, especially when the information is vital to the patient’s treatment.

If a doctor believes the record must be changed, as much as possible the amendment should be made in accordance with applicable College requirements. It should not obscure or delete the original entry. In an electronic environment, changes can usually be made using an addendum or digital strikeout. The date, time, and initials (or electronic signature) of the person making the alteration should be visible on the electronic record. A “track changes” function (similar to that found in most word processing programs to monitor changes to documents) could be used. When this is not available, an addendum should be placed in the record explaining what change is needed, preferably next to the original entry, if possible.

**Notifying other users of erroneous or outdated information**

If physicians become aware that an eRecord to which they have access contains outdated, incomplete, or inaccurate information of clinical significance, it is prudent to alert other users within a reasonable time so the patient’s treatment is not compromised. Then, physicians should try to correct the erroneous information as soon as possible. Changes should be made in accordance with College requirements.
Doctors should also be aware that privacy legislation generally requires custodians who correct records to notify others to whom the relevant information has been disclosed.

The data sharing agreement should ideally contain a provision that addresses the procedures for correcting the eRecord and requiring notification of previously accessed erroneous or outdated information.

**Receiving data or records from other healthcare providers**

A unique challenge with EHRs (and shared EMRs) is that other healthcare providers have access to the data and may contribute to the eRecord directly. A physician may also receive data or records from other healthcare providers that are incorporated into a patient’s EMR. These physicians may be unfamiliar with each other’s practices and may not consult with each other regularly, if at all.

The importance of accuracy is increased in these circumstances and all healthcare providers using the eRecord should make reasonable efforts to know who contributes to it, how often it is being accessed, and how information they have added should appear on the screen or printout (e.g. initialed or signed and dated entries, strikeouts, and addendums for changes to original entries, etc.).

**Converting paper records to electronic form**

Physicians who choose to adopt an EMR might question whether their existing paper records should be transferred to an electronic format and whether, once scanned, the original records can be destroyed.

Documents converted into electronic format are considered copies. However, they are nonetheless generally admissible in legal proceedings. The rules concerning the admissibility of copies have been modified in most Canadian jurisdictions to take into account the reality of electronic record-keeping.

Responding to a legal request to produce an electronic record can be challenging. It may be necessary to produce the “metadata” embedded in all electronic documents, including the audit trail, records of key strokes and deletions, and decision support information. Specialized technical assistance may be needed to ensure that all the required data is included. Upon receiving a subpoena or a court order to produce medical records (in paper or electronic form), physicians are encouraged to contact the CMPA for advice.

Most, if not all, Colleges permit the destruction of paper records once they have been appropriately scanned. However, the CMPA encourages physicians to consider the following guidance to ensure paper records converted into electronic format meet the legal requirements:

- An experienced and reputable commercial organization may assist in establishing procedures for the conversion.
- The conversion should take place in a consistent and careful manner, with appropriate safeguards so as to ensure the digital copies are sufficiently reliable.
- Written procedures should be established and consistently followed for the conversion process (including a record of the type of conversion process used), with the physician keeping a copy of these procedures.
- The process should involve some form of quality assurance (e.g. comparing the digital copy to the original to ensure the information has been accurately converted), and a record should be kept of the quality assurance steps taken with respect to each document.

Scanned records should be kept in “read-only” format so they cannot be altered or manipulated after conversion. Physicians should be aware of the differences between scanning and optical character recognition. Scanning simply generates a non-editable digital representation of an image whereas optical character recognition (OCR) is a technology process that converts an image of handwritten or typewritten text into machine-editable text. Once an image has been converted using OCR, the text can be changed,
searched, or otherwise manipulated. OCR may be used in conjunction with scanning. However, OCR alone should not be used when converting paper records to electronic form, unless the original paper records will also be scanned or will be maintained in paper form.

When the appropriate steps have been taken, it may be reasonable for practitioners to destroy the original record. However, in exceptional cases, such as when the quality of the paper records makes the converted document difficult to read, it may be prudent to retain the paper records for at least the period of retention recommended by the CMPA: at least 10 years from the date of the last entry or, in the case of minors, 10 years from the date on which the minor reaches the age of majority. Physicians should be aware that Colleges in some jurisdictions have adopted lengthier retention periods to reflect changes in the limitation periods for the commencement of medical malpractice actions. In those jurisdictions physicians are encouraged to retain records for a longer period to reflect those limitation periods.

The eventual destruction of the paper records should be in keeping with the physician’s obligation of confidentiality as well as any applicable legislative and College requirements. Physicians should contact the CMPA with any questions they may have about the applicable requirements in their jurisdiction.

Data migration
Physicians who are already using an EMR and wish to switch to a new EMR software or vendor will need to consider how to maintain the integrity of the patient data as entered in the old EMR system. Options may include migrating the data from the old system into the new system or archiving the data in the old system. Regardless of the process, physicians will want to ensure they have continued access to their patients’ data for the applicable retention period and that the information, including the metadata, is not compromised or otherwise changed in the process. This can be a challenging and labour intensive process, so physicians may wish to consult with IT professionals and their system vendor.

Backup and recovery
It is not uncommon for computer systems to fail, which can lead to the loss of patient information contained in an EMR. In some jurisdictions, legislation and regulatory authority policies require that electronic files are routinely backed-up and that the system allows files to be recovered.

Even if there are no specific regulatory requirements in a particular jurisdiction, it is a good practice to back up patient information daily or weekly and to ensure the backup files are encrypted. Physicians may also want to regularly test the restore process for these backed up files. Furthermore, they may wish to use an off-site backup system to protect patient records, in case an office computer is stolen, lost, or destroyed. An example of such an off-site system is the use of cloud computing technology to deliver backup services.
over the Internet. Physicians should consult with their vendor or service provider for more information about the backup and recovery capabilities of their system and the options available for off-site backup.

**Electronic signatures**

The critical function of a signature is to associate the signatory with the contents of the document. Can an electronic signature effectively serve the same purpose in an eRecord? Legally, it can. An electronic signature, although not tangible in nature, can still be evidence of the association of the signatory with the document and its contents.

Electronic signature is a generic term that refers to a wide variety of non-manual signature options, including digital signatures. It is commonly defined as electronic data created or adopted by a person to sign a document. The data is then attached to or associated with the document.

A digital signature is a technology-specific type of electronic signature. It is one of the many techniques that satisfy the functions sought to be performed by electronic signatures. A common misconception is that electronic signatures are merely a digital version of a handwritten signature. While a signature entered on a touchpad is one example of an electronic signature, a more common example are those consisting of one or more letters, characters, numbers or symbols that are attached to or associated with an electronic document.

Although electronic signatures are generally recognized as being as valid as manual signatures, they cannot yet be used in all circumstances. Currently, the exclusive use of electronic signatures in ePrescribing is permitted in some, but not all, provinces and territories.

When they are permissible, electronic signature devices must meet certain reliability requirements. In the event of a potential future legal proceeding, physicians using this type of device will want to be able to explain how it works and attest to its reliability. Without this assurance of reliability, a court or tribunal may not allow the electronically signed document to be admitted as evidence or it may be given reduced weight.

It is therefore important to be able to demonstrate the electronic signature was properly associated with the document in question (e.g. report, consent form, etc.). Without this assurance of reliability, the other side in a dispute could argue that the patient did not know what document to which he or she was affixing a digital signature when signing with a stylus on a digital signature pad. Alternatively, it could be argued the physician’s signature was not associated with the correct report and the physician did not, in fact, review the relevant document.

To effectively respond to such arguments, physicians should consider a system with the following characteristics:

- The person signing the document electronically is able to verify the electronic signature on the screen.
- An audit function that permits the physician to ascertain the date and time the signature was made, and to what document it was associated at that time.
- Individuals are only able to enter their own electronic signature.

Physicians are encouraged to explore the various electronic signature options with an information technology consultant.
Sending and transferring records

Electronic records facilitate the quick transmission of patient information to other healthcare providers or to the patient. In a shared EMR or an EHR, it is likely other healthcare providers involved in the patient’s care will have direct, independent access to the patient’s record and the information necessary to provide treatment. In these circumstances, the treating physician has a limited role in making the patient information available.

If uploading patient information from an EMR to another eRecord, physicians should consider whether the network they are using is sufficiently secure. Again, doctors should consult with their College for any applicable policies or guidelines. Similarly, when a physician receives a request from another treating healthcare provider for patient information contained in an EMR that is not shared, the physician should choose a secure means to electronically transmit the information such as fax, email, or another eRecord.

Communicating electronically with patients and others

Colleges and privacy regulators may have policies or guidelines on communicating with patients through email or fax. Physicians should be aware of those that apply in their jurisdiction. Before using email and fax to communicate with patients and transmit their health information, doctors should discuss the risks with patients and obtain their consent. Physicians should document any discussions in the medical record and use a written consent form (see the CMPA Consent to use electronic communications form, available at www.cmpa-acpm.ca)
Email
Several potential risks with email communication relate to privacy and security, timeliness of response, and clarity of communication. At least one provincial privacy commissioner has indicated that physicians should avoid communicating personal health information via email unless the email service is secure and offers strong encryption. The commissioner has further indicated that it would be inappropriate to rely on patient consent to waive the protection afforded by encryption and other security measures. Physicians should establish policies and procedures for handling email communications. Employees should be informed, through a policy or otherwise, of the risks of inappropriate email communication.

If a physician is employed by or holds privileges within an organization, institution, or hospital, it may be difficult to protect sensitive email correspondence from being accessed by the organization. For example, a physician working from a hospital might be vulnerable to the hospital administration accessing email correspondence that has been prepared on a hospital computer or transmitted over the hospital system. If it is necessary to use email to communicate sensitive personal matters, consider using a personal email account accessed from a computer you personally control such as at your office or home.

Fax
Doctors should also implement standard procedures to minimize the possibility of misdirected faxes containing patient information. For example, depending on the recipient and the sensitivity of the information being faxed, it may be prudent to contact the recipient before sending the information and confirm the fax number and ensure the recipient is present to receive the document.
Destroying and disposing of records

When destroying patient information in electronic form, ensure the eRecord is permanently deleted or irreversibly erased. This may require physical destruction of the electronic storage device.

As with paper records, procedures are required to ensure eRecords are adequately destroyed. In fact, some Colleges and privacy legislation require that written policies be established for the retention and destruction of records containing personal health information. The following are some key points to keep in mind when considering the retention and destruction of EMRs:

- The required retention period for medical records — whether print or electronic — varies significantly from jurisdiction to jurisdiction. The CMPA recommends that physicians 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. In some jurisdictions where limitation periods extend beyond 10 years, the College may require records be retained for a longer time. Physicians should consult with their College’s policy on records to determine the appropriate length of time to retain records.
- Patient information contained in an eRecord should normally only be maintained for as long as is necessary for the purpose for which the information was collected and to permit the patient to exhaust
any recourse under privacy legislation with respect to an access request.
• Once the retention period has been exhausted, the information in the eRecord should be destroyed in a manner that maintains confidentiality.
• Physicians should be familiar with all applicable rules or obligations for destroying medical records.

Some privacy legislation requires physicians keep a record of:
• the individual whose personal health information is destroyed and the time period to which the information relates
• the method of destruction and the person responsible for supervising the destruction

Effective destruction requires the eRecord be permanently deleted or irreversibly erased. When destroying the information, physicians must consider whether it is necessary to destroy not only the original records, but also any copies of these records, including backup files.

Some privacy commissioners recommend that the electronic storage device (e.g. hard drive) be physically destroyed to ensure the permanent deletion of patient information. This may include physically destroying the electronic storage device, or it may be sufficient to use wiping software to delete the information on the hard drive. However, depending on the sophistication of the software, wiping may not irreversibly erase every bit of data on a drive. Physicians should avoid selling or giving away electronic storage devices that contain or once contained patient information.

As technological expertise is required to effectively destroy electronically stored information, it is preferable that physicians hire an accredited service provider to destroy patient information maintained in EMRs. Some privacy commissioners have stated that when engaging a commercial service provider to dispose of patient information, physicians must enter into a written contractual agreement with that service provider. The agreement should clearly spell out the responsibilities of the service provider to securely destroy the health information records, and how the destruction will be accomplished, under what conditions, and by whom. While not currently a requirement in all jurisdictions, this is a prudent practice for all physicians who engage a records disposal company.
Data sharing and inter-physician arrangements

- Review the CMPA/CMA Data Sharing Principles (Appendix C), including issues of privacy and confidentiality.
- Develop and implement a data sharing agreement (the CMPA has developed a sample agreement titled, Contractual Provisions for Data Sharing in Electronic Medical Record/Electronic Health Record Agreements, which can be found in Appendix D).
- Use confidentiality and non-disclosure agreements, such as the sample developed by CMPA and reproduced in Appendix E.
- Exercise due diligence and be sure to understand the agreement with a vendor of an eRecord system.
- Where no information management agreement exists for an EHR system established by a health authority, or when linking an EMR to the EHR, a data sharing agreement should be used.
- Make sure the inter-physician agreement addresses access to patient records, including after a physician departs the practice.

Storing electronic health information data with third parties

Even technologically savvy physicians will likely engage an outside service provider to assist in implementing, maintaining, and storing data contained in electronic medical records. In addition, many provinces, health authorities, and hospitals are seeking to set up their own EHRs that may integrate physicians’ EMR systems. Accordingly, there are a number of different scenarios and structures that will see a physician contracting with a third party to implement an eRecord system.

Some of the potential contracting arrangements that a physician may consider include:

- a data sharing or management agreement with a vendor or other service provider, for example for software, hardware, and hosting
- a data sharing or management agreement with a provincial government agency, health authority, or hospital
- an inter-physician agreement among a group of physicians, for example, a shared call group, a clinic with shared records, a family health team or family health network, or a physician corporation or partnership

In any of these situations, certain fundamental principles should be considered. The CMPA, in conjunction with the Canadian Medical Association, provides guidance in the booklet, Data Sharing Principles for Electronic Medical Record/Electronic Health Record Agreements (Appendix C). The CMPA has also prepared sample Contractual Provisions for...
Data Sharing in Electronic Medical Record/Electronic Health Record Agreements (Appendix D), which reflect each of the principles identified in the Data Sharing Principles document. The sample provisions can guide physicians who are entering into an agreement for an eRecord system or sharing patient information in electronic form. Physicians should also consult their personal legal counsel when considering a data sharing agreement or inter-physician agreement.

Some jurisdictions have developed data sharing frameworks at the provincial or territorial level. The CMPA has been asked by several jurisdictions and various organizations to comment on or assist with frameworks and agreements. Physicians are encouraged to contact the CMPA to confirm whether the Association was consulted on a specific data sharing framework.

Choosing a third-party vendor to set up or maintain an eRecord

Physicians considering implementing an EMR system may need to retain a third-party vendor to provide advice on software, hardware, electronic storage, etc. Some provincial governments have set up specific programs to provide technical and financial assistance to physicians, including screening and approving vendors to ensure they conform to applicable requirements.

While a government or another authoritative endorsement of an EMR vendor may provide some reassurance of a system’s suitability, doctors will need to exercise their own due diligence and ensure they understand the agreement they sign with a vendor. The agreement should fully describe the services and functionality to be provided by the EMR system. As well, the scope of the vendor’s services must be adequately detailed so the vendor can be held accountable for the performance of the agreement. To ensure they understand the data sharing agreement, physicians may wish to ask the vendor the following questions:

- What services are being offered?
- What is the functionality of the service?
- How will the service be documented?
- What are the roles and responsibilities of the vendor, the physician, and any other parties to the agreement?
- What are the financial terms? (e.g. What does the service cost? Are there any other additional or hidden charges? Are there any financial penalties?)
- Does the vendor own the EMR system or have appropriate authorization to sell it?
- How will the physician transition into and out of the EMR system?
- What expectations should the doctor have of the EMR system’s performance?
- Does the system meet applicable provincial standards and College expectations?
- What service levels will the vendor provide?
- What are the consequences if the vendor fails to meet service levels?
- What are the vendor’s support and maintenance obligations?
- How will system security be assured?
- Where will the server be located?
- What is the vendor required to report to the physician and when?
- How and when will data be backed up?
- What provisions are made for disaster recovery?
- What are the hardware requirements?
- What are the software requirements?
- How will system security be assured?
- Where will the server be located?
- What is the vendor required to report to the physician and when?
- How and when will data be backed up?
- What provisions are made for disaster recovery?
- What are the hardware requirements?
- What are the software requirements?
- How may the agreement be terminated and how will continuity of care be assured?

Implementing an inter-physician agreement for shared EMRs

When a doctor practises within a group of physicians or a physician organization, it may make practical and financial sense to have a shared EMR system for all the practitioners. This system may or may not be integrated with a hospital, regional, or provincial EHR system.

An agreement among a group of physicians or a physician organization with an information technology consultant should include the same considerations as when a third-party vendor is being chosen. In addition, there should be an agreement on the shared EMR
An agreement on a shared EMR may be stand-alone or may be included in a larger agreement between the physicians that governs the management of the group practice, clinic, or other organizational structure (e.g. partnership agreement or shareholder agreement).

Once a patient’s medical record contains contributions from various individuals and is being accessed by a number of healthcare providers, questions of ownership and security become significantly more complex. In addition to the fundamental principles already discussed, the inter-physician agreement should pay particular attention to ensuring a patient’s record is accessible only by authorized users for authorized purposes. It will likely be necessary to have mechanisms that restrict access to only those physicians and staff who need access to a particular patient’s record to provide medical care or for other authorized purposes.

Data sharing agreements with health authorities

In some jurisdictions, the medical association has negotiated some form of data sharing or information management agreement to govern physicians’ use of an EHR managed by the health authority. Where no information management agreement exists, physicians who are seeking to be a user of an EHR system established by a health authority or to link an EMR to the EHR should consider entering into a data sharing agreement. The principles of this agreement are the same as those discussed previously, and in Appendix C — Data Sharing Principles.

Data sharing agreements between physicians and health authorities may face the unique issue of protection for quality assurance and quality improvement records. Where a hospital quality improvement committee has prepared records for the purpose of reviewing adverse events and evaluating the effectiveness of a hospital’s practices and procedures, these records should be segregated from other records to ensure that any legislative protection from disclosure is maintained. The data sharing agreement should stipulate how records will be segregated and how access to records will be limited. For example, the data sharing agreement should stipulate that this information (i.e. personal and quality assurance or quality improvement information) will not be disclosed unless required by law.

Protecting against liability when sharing personal health information

A number of provisions can and should be incorporated into any data sharing agreement or inter-physician agreement to minimize the risk of liability including:

- indemnification
- limitation of liability
- representations and warranties
- dispute resolution
- governing law or forum

These provisions are discussed in detail in Appendices C and D.

Termination of agreement and ensuring continuity of operation

There may come a time when parties mutually agree to terminate a data sharing or inter-physician agreement, for example when a group of physicians disbands or dissolves. The agreement might also be terminated due to a breach of the agreement or the insolvency of other parties.

A physician’s participation in the eRecord system may come to an end for many reasons, such as leaving the jurisdiction or ceasing to practise medicine as a result of retirement, disability, or death. Practitioners should ensure their data sharing or inter-physician agreement includes a clause permitting its termination without cause by providing notice to the other party.

Indemnities and confidentiality obligations in the agreement should continue to apply despite termination. Physicians also need to ensure they have
continued access to the information in the eRecord so they can meet their record retention obligations. Even physicians who are no longer practising medicine may receive requests from patients to access their medical records. Physicians may also require the records in the event of a medico-legal issue. The agreement should require that the custodians of the records maintain them in their original form, make them available to the physician, and take reasonable steps to prevent the information from being lost, stolen, or inappropriately accessed. Provisions should be included to ensure the original records are appropriately destroyed when the applicable retention period has expired.

Confidentiality or non-disclosure agreement

Physicians have an obligation to ensure that the patient information entrusted to them is kept secure and confidential. Certainly, physicians’ employees and staff share in the responsibility of meeting these obligations, but the ultimate accountability rests with the physician.

The CMPA encourages doctors to have their employees and staff members sign a confidentiality or non-disclosure agreement. It may be beneficial to have the agreement renewed annually. Such agreements help employees and staff understand their obligations, encourage respect for confidential patient information, and provide valuable reassurance to the patient.

A sample confidentiality/non-disclosure agreement can be found in Appendix E.
Emerging issues

- Do not rely exclusively on the information contained in an electronic health record that is created or provided by a patient.
- Carefully assess the privacy and security implications of storing data with a cloud service provider.
- If using wireless devices to access eRecords, including smartphones and tablets, consider steps to ensure the device and the network are secure, and there is no unauthorized access to patients’ personal health information.
- When using social media, avoid inadvertently disclosing information that might identify a patient and breach privacy.
- Be informed about the rules that apply to ePrescribing in the jurisdiction and strictly follow them.

Physicians are witnessing increased use of technology to manage patient health information. eRecords will likely continue to develop new functionality, including the use of patient portals through which patients can access their information, interact with healthcare providers, and possibly upload data. Beyond eRecords, Internet-based products that facilitate the creation of health records by patients themselves or provide cloud computing services are quickly entering the marketplace. There is increasing interest in the use of messaging services, social media, and wireless devices to share information and access records. ePrescribing is likely to become more common, as is digital dictation and other technological advances that improve and facilitate the daily practice of medicine. Many of these innovations, while beneficial to physicians and patients in several ways, can present medico-legal issues that need to be addressed.

Patient health records and patient portals

Unlike an EMR or EHR, which is typically created and maintained by a healthcare professional or facility, a patient health record or PHR commonly refers to a compilation of information (including past and present medical conditions, medications, and allergies) that has been personally gathered and maintained by the patient using a third-party service or tool. Some of these applications offer a self-diagnosis tool through additional Internet-based information about symptoms, causes, and treatments.

Patients may choose to grant physicians and other healthcare providers access to the information entered into their online patient health record. Many products also allow hospitals, clinics, laboratories, pharmacies,
and individual physicians to upload additional health information into the electronic health record created by the patient. Emerging new functionality allows patients not only to access their information online, but also to interact with healthcare providers and upload data, such as blood pressure readings, temperature, or blood sugar levels.

Since the information contained in patient-controlled electronic health records can be unreliable, doctors should be cautious about relying on it exclusively. In some circumstances it may be prudent to verify that the information is accurate and complete. Patient-created health records should not be considered a replacement for a physician’s own record-keeping obligations, nor should they replace a physician’s assessment of patients including asking direct questions about patients’ medical history. When a patient asks a physician to upload information to an online health record, the physician should discuss the request with the patient, and carefully consider issues about consent and security.

Physicians may choose to create a website accessible by their patients or other health professionals. There are endless possible uses for such websites. Some are used to communicate with patients. Some contain portals through which patients can request appointments, prescription renewals, or information about lab results. Some of the more advanced physician websites and patient Internet services offer online tracking tools to facilitate and monitor patients’ ongoing follow-up care, for example chronic disease management. These tools generally permit patients to enter their health information through a secure web-based patient portal for review and monitoring by the physician. Physicians can respond to the data by communicating with the patient via email alerts or secure messaging. These patient portals can offer valuable services to patients but must be appropriately secured and managed.

The CMPA generally recommends that physicians include terms of use on their websites. The Association has a template agreement that doctors can use as a guide, which includes a provision for websites with patient-access portals (see cmpa-acpm.ca: “Terms of Use Agreement Template for Physician Websites”). Physicians should seek appropriate legal and other professional advice to adapt this template to their particular circumstances and as technology evolves. Advancements in portal technology and Internet-based patient records require an analysis of privacy, security, and the integrity of those records. The extent to which physicians should rely on the information in patient communications or patient-created health records, the extent to which physicians should permit interfaces between those records and eRecords, and the extent to which those lines of communication are sufficiently secure and permit compliance with applicable privacy legislation must be explored. Other issues that need to be addressed are patients using portals or PHRs for urgent or time-sensitive health issues, a physician’s separate record-keeping obligations with respect to portal communications and PHRs, and ensuring that patients have given informed consent to the use of the technology.

Cloud computing

Cloud computing is an emerging technology that may find routine application to eRecords. It allows users to receive unlimited computing services such as data storage, backup, and data processing, over the Internet for minimal cost. This enables users to access records from anywhere there is an Internet connection and reduces the costs of buying hardware, software licences, and infrastructure. Cloud computing may be especially attractive to physicians in private practice who want to reduce their overhead expenses, lack technical expertise, and would benefit from the mobility offered by the cloud services.

While there are potential efficiencies to using cloud computing services, physicians must carefully assess the risks before signing a cloud service agreement. The federal privacy commissioner published two helpful documents to guide those contemplating the use of cloud services (see www.priv.gc.ca: “Fact Sheet: Introduction to Cloud Computing” and “Cloud Computing for Small- and Medium-Sized Enterprises”).
Physicians should be aware that there are privacy and security concerns that they must address before storing data with a cloud service provider. Since cloud computing involves outsourcing data to a cloud service provider, a physician’s continued control over the data remains paramount. Doctors remain accountable for the information they transfer to a cloud service provider.

For example, physicians will want to be certain that the cloud services agreement prevents secondary uses of personal health information or that patient consent to such secondary uses has been obtained. Audit trails, restricted access, strong password protection, encryption, notification procedures to physicians in the event of a privacy breach, and backup procedures to prevent data loss and outages are all important security measures that should be explicitly addressed in the agreement. In addition, physicians will want to ensure they have access to the data at all times to enable them, for example, to make corrections, investigate complaints, or respond to patient access requests.

Practitioners should also be aware that the data sent to the cloud may be physically located on servers in several jurisdictions. Issues such as whether patient notification is required and what privacy laws apply to the transferred information must be considered.

Standard cloud service terms of use agreements may not be sufficient to permit physicians to fulfill all of their privacy and confidentiality obligations. Consulting with information technology and legal professionals will ensure physicians comply with their obligations under the terms of the agreement.

**Wireless technology**

Medicine’s use of wireless devices and networks is steadily growing. Accessing records and resources wirelessly from home or from other locations allows physicians to provide more efficient and effective healthcare. Many doctors have begun using tablets and smartphones to view eRecords, email, the Internet, and learning and decision support tools.

Mobile applications on wireless devices permit remote monitoring of patients with chronic conditions, and consultations with specialists or research resources (e.g. MDapps.ca).

The use of wireless devices raises concerns about loss or theft of the device and unauthorized access to personal health information. In addition to password protection and encryption, the ability to remotely lock or wipe the device if it is stolen or lost is also a valuable feature to protect patient privacy. Some privacy commissioners, or their equivalent, have taken the position that personal health information transmitted wirelessly must be either de-identified or encrypted. Physicians will want to be assured that appropriate security controls have been implemented on their mobile devices and the entire wireless network to prevent unauthorized access to eRecords.

There are a growing number of public wireless networks (hotspots) available to mobile device users. The security of public wireless networks cannot be assured and as such they generally should not be used to access or transmit personal health information. Moreover, physicians should avoid connecting to 2 wireless networks simultaneously (e.g. Wi-Fi and Bluetooth), since doing so can turn the physician’s mobile device into an access point to the wireless network.

**Social media**

Social media is another rapidly growing area of patient-physician online interaction. Physicians are increasingly aware of the potential of platforms such as Twitter, LinkedIn, Flickr, MySpace, YouTube, and Facebook as learning and information sharing tools. Social media can be useful for health promotion, allowing physicians to reach out and engage with patients and the public on general health issues. Blogs and wikis are also increasingly being used in medical education as the online equivalent of a study group.

Physicians who communicate through social media must remember that in the virtual world they are governed by the same professional and ethical
standards that apply in the physical environment (i.e. hospital, doctor’s office, or clinic). As well, the laws on defamation, copyright, and plagiarism apply equally to the web and social media as to print and verbal communication.

Doctors using social networking sites may not realize that if they discuss specific cases with colleagues in a manner that identifies the patient, they are breaching patient confidentiality. Password protected social networking sites may give physicians a false sense of security, leading them to believe that the environment is exclusive. In reality, the information or discussion can be circulated widely, well beyond the original group or circle of friends. This lack of control over the information and the public nature of the sites make it particularly challenging for physicians to maintain patient confidentiality.

Physicians should also be cautious about interacting with patients or other members of the public through a social media forum. Medical information or advice posted by a physician on a blog or other social media platform could be seen to have established a therapeutic relationship with the individual accessing and relying on the information.

Furthermore, maintaining appropriate professional boundaries when using such technology is important. Physicians who use social media are advised to activate the strictest privacy settings whenever possible. On Facebook or LinkedIn, for example, users can adjust privacy settings, within the profile sections of their pages. Remember, however, that even though privacy settings have been adjusted, confidential information should not be shared on public social sites.

Some regulatory authorities have issued guidelines and policies on the use of social media. Physicians should be aware of any College directives in their jurisdiction. The Canadian Medical Association has also published guidelines entitled, “Social media and Canadian physicians — Issues and rules of engagement.”

**ePrescribing**

Physicians have started to electronically communicate prescriptions to pharmacies. The technology for true “ePrescribing” exists, but the necessary regulatory framework required for ePrescribing in clinical practice remains to be developed and implemented. Many regulatory authorities and statutes still require a physician’s handwritten signature on a prescription. However, as electronic signature technology advances, the requirement for an original signature may be eliminated.

It is anticipated that ePrescribing will evolve significantly in the coming years as eRecords systems become increasingly commonplace, electronic links to pharmacies are developed that also maintain patient choice, and the technology permits an electronic prescription to replicate all the qualities of a handwritten one. For ePrescribing to be effective, the technology must support the activity appropriately, and regulations and standards must be developed to ensure the process is secure and reliable. Physicians should stay informed about the requirements related to electronic prescribing in their jurisdiction and comply with those rules accordingly.

**Summary**

All of these emerging technological advancements promise more efficiency and reduced costs in medical practice. Patients and physicians stand to benefit from the ease with which physicians can access and exchange information to provide timely and quality care. At the same time, new technologies should not be adopted or used before the privacy and security risks are fully analyzed, along with the measures that should be taken to enable physicians to comply with privacy legislation.
Conclusion

Electronic records can improve the management of individual patient care as well as the overall effectiveness of the healthcare system. While encouraging, the implementation and use of eRecords in medical practice introduce complexity.

When converting to or using eRecords, physicians will want to familiarize themselves with applicable legislation, College requirements, privacy guidelines and directives, regulations, and other expectations regarding the use of eRecords. Other critical issues such as access and security, data integrity, consent and data sharing agreements should be thoroughly considered and assessed before an eRecords system is implemented.

There is a patchwork of privacy legislation across Canada. Only some statutes deal directly with personal health information while even fewer specifically regulate the use of eRecords. It is hoped that, with time, a consistent legislative framework will be implemented that applies to all personal health information, regardless of how that information is maintained. The CMPA continues to work collaboratively to address this and other emerging issues. In the interim, physicians should ensure they are aware of the provisions that apply in their jurisdiction.

Physicians are encouraged to monitor CMPA publications on this topic and contact the Association if they have questions or concerns about the adoption and implementation of EMRs or EHRs.
Appendix A – Glossary

Audit trail
Information concerning the history of an electronic document, often including details of insertions, deletions, or other alterations to the data as well as details of access to the data.

Agent/affiliate
An individual to whom the responsibilities of a health information custodian can be delegated. In a hospital setting, physicians, nurses, and other clinical care providers are often considered to be an agent or affiliate of the custodian hospital or regional health authority. In a physician’s office, an office assistant and other staff members who are required to access the medical records for business or clinical purposes often do so as an agent of the custodian physician. Despite being an affiliate of the hospital or regional health authority that has legal custodianship over the record, a physician will generally be subject to similar obligations regarding the protection of patients’ personal health information.

Core data set
A subset of health-related information required for treatment of a patient which is created for the purpose of sharing specific data between healthcare professionals. (Also referred to as “clinical data set, “client data set,” “continuity of care record,” “electronic medical summary,” “shareable patient health profile,” “cumulative patient profile,” and “master patient index.”)

Custodianship (of eRecords)
Duties associated with collecting, using, and disclosing information (in an eRecord).

Data integrity
Preservation of information so that it remains unaltered and is authentic.

Data sharing agreement
An agreement between a healthcare provider, or a group thereof, on the one hand, and an institution, health authority, or service provider on the other hand, that sets out the terms for the sharing of electronic health information.

Data stewardship
Responsibility for the appropriate management and protection of the data contained in an eRecord.

Digital signature
A secure form of electronic signature where the identity of the signatory and the authenticity and integrity of the document can be verified (e.g. a digitized image of a manual signature entered via a digital signature pad, use of a digital signature certificate with a private key).

eDiscovery
The production of electronic data in legal proceedings.

Electronic health record (EHR)
A compilation of core health data submitted by various healthcare providers and organizations, accessible by numerous authorized parties from a number of points of care, possibly even from different jurisdictions.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic medical record (EMR)</td>
<td>An electronic version of the paper record that doctors have traditionally maintained for their patients and which is typically only accessible within the facility or office that controls it. A “simple EMR,” which refers most often to an electronic record created and maintained by a single physician in an office-based practice, must be distinguished from a “shared EMR” (see below) or “EHR” (see above).</td>
</tr>
<tr>
<td>eRecords</td>
<td>Term used to refer to both EMRs and EHRs.</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>A generic term referring to a wide variety of non-manual signature options. An electronic signature may consist of letters, characters, numbers or symbols in digital form, attached to or associated with an electronic document.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The process of transforming information into a form that is unintelligible to those not possessing the required knowledge or authorization to decrypt it, such as a muddled stream of seemingly random symbols.</td>
</tr>
<tr>
<td>Inter-physician agreement</td>
<td>An agreement between physicians, such as in the context of a group of physicians or as part of a physician organization, dealing with how the information contributed to a shared EMR will be managed.</td>
</tr>
<tr>
<td>Licence</td>
<td>A legal agreement governing the use and distribution of copyright-protected software, including imposing restrictions on who can use the software and the legal obligations on the software designers and end users.</td>
</tr>
<tr>
<td>Lockbox</td>
<td>A security feature that allows access to a patient’s personal health information, or portions thereof, to be restricted to certain users at the specific request of the patient. (Often used interchangeably with the concept of a “masking,” below.)</td>
</tr>
<tr>
<td>Masking</td>
<td>The concealing of a patient’s personal health information, or portions thereof, at the specific request of the patient in order to limit or control the information that is disclosed to other healthcare providers. (Often used interchangeably with the concept of a “lockbox,” above.)</td>
</tr>
<tr>
<td>Metadata</td>
<td>Electronic background information generated in the course of creating and maintaining an electronic record e.g. dates and times of insertions/deletions, details of user access.</td>
</tr>
<tr>
<td>Privacy audit</td>
<td>A periodic review and assessment of privacy controls to ensure their effectiveness.</td>
</tr>
<tr>
<td>Optical character recognition (OCR)</td>
<td>A technology process that converts an image of handwritten or typewritten text into machine editable text that can be changed, searched, or otherwise manipulated.</td>
</tr>
<tr>
<td>Ownership (of eRecords)</td>
<td>The concept of legal custody and control of an eRecord system and the data within it, even though a number of users may have rights to contribute and draw information from it.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Patient health record (PHR)</td>
<td>(Also referred to as “personal health record”) An electronic record typically created and maintained by the patient, sometimes using a third-party online service. Unlike eRecords, which are typically created and maintained by a healthcare professional or facility, the term PHR commonly refers to a compilation of information personally gathered and maintained by patients regarding their health. The patient controls access and information inputted into the PHR.</td>
</tr>
<tr>
<td>Privacy impact assessment</td>
<td>A risk management process by which actual and potential privacy risks associated with implementing an information system are identified.</td>
</tr>
<tr>
<td>Portable data storage device</td>
<td>Any portable electronic device that allows the storage of data such as a laptop, cell phone, personal digital assistant (PDA), USB flash drive/memory stick, or portable hard drive.</td>
</tr>
<tr>
<td>Secondary use</td>
<td>The use of personal health information for purposes other than the provision of healthcare, for example, for research or health system planning.</td>
</tr>
<tr>
<td>Shared EMR</td>
<td>A centralized electronic medical record of a patient that permits a number of users (e.g. treating physicians, other healthcare providers, information managers, etc.) to access all or a portion of the record.</td>
</tr>
</tbody>
</table>
Appendix B – Additional Resources

The following is not intended as an exhaustive list, but merely gives physicians some suggestions for further references on eRecords. (Revised 2013)

**CMPA MATERIALS**

The privacy issue, Special edition, *CMPA Perspective*, October 2013

Electronic Health Records: A medical liability perspective, August 2008

Minimizing medico-legal risk when using technology, June 2008

Medico-legal issues arising from new healthcare technologies, December 2007

Protecting sensitive electronic health information — think encryption, September 2007

How do you protect privacy?, April 2008

Safeguarding your patients’ privacy when data is stored on computers, March 2008

Using email communication with your patients: legal risks, June 2013

Transitioning to electronic medical records, June 2010

Using social and professional networking websites can breach confidentiality, June 2010

Encryption just makes sense, April 2013

Privacy and a wired world — Protecting patient health information, December 2011

Technology unleashed — The evolution of online communication, June 2012

**OTHER RESOURCES**

**Canada**

*Canada Health Infoway*

www.infoway-inforoute.ca

Federal not-for-profit corporation created to accelerate Canada’s EHR development and implementation efforts.

*Canadian Medical Association*

cma.ca

See Advocacy section for guidelines on social media use and research reports and resources on health information technology, including guidance on EMR adoption.

*Canadian EMR*

www.canadianemr.ca

Private resource site for physicians, staff, vendors and others regarding EMR systems.

*The College of Family Physicians of Canada*

http://www.cfpc.ca/

Included in the CFPC’s Primary Care Toolkit for Family Physicians is a section dedicated to “Information Technology,” which includes information and resources on eRecords.

*Office of the Privacy Commissioner of Canada*

www.priv.gc.ca

Monitors and enforces the Personal Information Protection and Electronic Documents Act. Provides privacy resources including fact sheets on cloud computing and protecting personal information on mobile devices.
British Columbia

College of Physicians and Surgeons of British Columbia
www.cpsbc.ca
See Professional Standards and Guidelines for guidance on electronic medical records, data stewardship, and social media/online networking.

British Columbia Medical Association
www.bcma.org
See Privacy Toolkit and policy statements on health information management and technology and on email communications with patients.

Physician Information Technology Office
www.pito.bc.ca
Joint initiative by BCMA and BC Ministry of Health to support physicians implementing EMRs in their practices.

Society of General Practitioners of BC
www.sgp.bc.ca
Library section includes material on IT issues, including material on EMRs/PITO.

Office of the Information and Privacy Commissioner for British Columbia
www.oipcbc.bc.ca
Monitors and enforces the Personal Information Protection Act and E-Health Act, and includes resources for physicians, such as the BC Physician Privacy Toolkit.

British Columbia Ministry of Health — eHealth
www.health.gov.bc.ca/ehealth
Overview of B.C.’s eHealth projects.

Alberta

College of Physicians and Surgeons of Alberta
www.cpsa.ab.ca
See section on Data Stewardship, including CPSA Data Stewardship Framework and CPSA Data Stewardship Principles—Information Sharing Agreements, and section on EMR and Physicians, which includes EMR resources.

Alberta Medical Association
www.albertadoctors.org
See section on Practice Help – EMRs, including information about transitioning to EMRs, EMR choices and Alberta’s EHR initiative.

Physician Office System Program
www.posp.ab.ca
Joint initiative by Alberta Health & Wellness, AMA and Alberta Health Services to support physicians implementing EMRs in their practices and provide integration and interoperability with the provincial health information management infrastructure.

Office of the Information and Privacy Commissioner of Alberta.
www.oipc.ab.ca
Monitors and enforces the Health Information Act. Provides information on compliance for custodians and guidance for conducting privacy impact assessments.

Alberta Netcare
www.albertanetcare.ca
Responsible for implementation of province-wide EHR.

Saskatchewan

College of Physicians and Surgeons of Saskatchewan
www.quadrant.net/cpss/
See Regulatory By-laws on medical records and Privacy Toolkit jointly produced with the Saskatchewan Medical Association.

Saskatchewan Medical Association
www.sma.sk.ca
See sections on EMR Program and Privacy for resources concerning EMR adoption and related privacy issues.

Office of the Saskatchewan Information and Privacy Commissioner
www.oipc.sk.ca
Monitors and enforces the Health Information Protection Act and includes resources on mobile device security and conducting privacy impact assessments.
E-Health Saskatchewan
www.health.gov.sk.ca/ehealth-saskatchewan
Responsible for implementation of province-wide EHR.

Manitoba
College of Physicians and Surgeons of Manitoba
www.cpsm.mb.ca
See statements and guidelines on medical records, medical computer systems, and transmission of health information by electronic means and by cellular and cordless phones.

Manitoba eHealth
www.manitoba-ehealth.ca
Includes section on Community Physicians, with resources for community-based specialists and primary care providers.

Manitoba Ombudsman
www.ombudsman.mb.ca
Access and Privacy Division is responsible for ensuring compliance with The Personal Health Information Act and resources include guidance about eChart Manitoba, emailing personal health information, protection of personal health information when working outside the office.

eChart Manitoba
www.connectedcare.ca/echartmanitoba
Overview of Manitoba’s province-wide EHR initiative.

Ontario
College of Physicians and Surgeons of Ontario
www.cpsso.on.ca
See policy on medical records, including section on eRecords.

OntarioMD
www.ontariomd.ca
Subsidiary of Ontario Medical Association that provides physicians with information and support with respect to the adoption of information technology. See section on EMR Adoption Program, including information on EMR offerings and specifications, and resources for transition support.

eHealth Ontario
www.ehealthontario.on.ca
Government agency responsible for implementing information technology in healthcare.

Information and Privacy Commissioner of Ontario
www.ipc.on.ca
Responsible for monitoring and enforcing the Personal Health Information Protection Act. Resources include privacy toolkit, guidance on privacy impact assessments and transitioning to eRecords, and fact sheets on secure destruction and transfer of personal health information, “lockboxes,” and encryption for mobile devices.

Québec
Collège des médecins du Québec
www.cmq.org
See practice guides on medical records, including eRecords and electronic communication, and Code of Ethics of Physicians.

Dossier Santé Québec
www.dossierdesante.gouv.qc.ca
Responsible for development of the Québec Electronic Health Record.

New Brunswick
College of Physicians and Surgeons of New Brunswick
www.cpsnb.org
See regulations and guidelines on medical records, electronic prescribing, and Facebook.

New Brunswick Department of Health
www.gnb.ca/0051/acts/index-e.asp
Includes resources for custodians of personal health information and lists designated EHRs.
Nova Scotia

College of Physicians and Surgeons of Nova Scotia
www.cpsns.ns.ca
See guidelines on medical record-keeping, including section on eRecords.

Nova Scotia Department of Health and Wellness
www.gov.ns.ca/health/ehealth
Includes information on the Primary Health Care Information Management Program to implement EMR systems and information on SHARE, Nova Scotia's EHR initiative.

Prince Edward Island

College of Physicians and Surgeons of Prince Edward Island
www.cpspei.ca
See policy on privacy principles.

Newfoundland & Labrador

College of Physicians and Surgeons of Newfoundland & Labrador
www.cpsnl.ca
See by-law and guidelines on medical records.

Newfoundland & Labrador Centre for Health Information
www.nlchi.nl.ca
Responsible for developing and implementing a province-wide EHR. Includes section on privacy and security.

Newfoundland and Labrador Department of Health and Community Services
www.health.gov.nl.ca/health/PHIA
Includes resources for custodians, including a PHIA Risk Management Toolkit.
Appendix C — Data Sharing Principles for Electronic Medical Record/Electronic Health Record Agreements (reviewed 2013)

Introduction

This document provides some interim guidance on 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 or 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 predefined access rights. Each provider of healthcare 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 or 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 or EHR system. Physicians will want to assess the risks and benefits in the context of their individual circumstances. As the custodians of very sensitive information, physicians need to carefully consider the extent to which patient information will be disclosed in an EMR or EHR system. When that sensitive information is shared in an EMR or 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 and disclosure of health information through an EMR or 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 or 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 or 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
   c. a family health team or family health network

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 or 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”)

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.

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).
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

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 or 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 or EHR system.

1.2 Why it is important:
The historical approach to medical record ownership is being outpaced by EMR and 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 and EHR are 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 physicians have appropriate access to the personal health information, and that physicians have the ability to provide their 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
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 and EHR could be considered assets 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 or civil 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 the civil 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, healthcare providers need to rely upon information maintained in the EMR/EHR. The importance of accuracy is increased where the healthcare 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 or civil 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 physicians 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, backup 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 healthcare 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 Recommendations:
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 backups;
(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 whom 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 practise 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 healthcare 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 that 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.
Appendix D — Contractual Provisions for Data Sharing in Electronic Medical Record/Electronic Health Record Agreements

Purpose of this document
The CMPA (together with the Canadian Medical Association) published “Data Sharing Principles for Electronic Medical Record/Electronic Health Record Agreements” (“Data Sharing Principles”) to provide guidance with respect to the implementation of an agreement for an electronic medical record (EMR) or electronic health record (EHR) system. The CMPA has also prepared sample contractual provisions that reflect each of the principles identified in the Data Sharing Principles document.

How to Use
These sample provisions are intended to be used as a guide when a physician is entering into an agreement for an EMR/EHR system or where sharing patient information in electronic form. The principles and related contractual provisions will vary depending upon the circumstances. Consideration will need to be given to intended use, the system(s) in operation, the information to be shared, the parties and the type of agreement being developed. Due to data sharing complexities, physicians are encouraged to engage legal counsel to assist them in using these sample provisions to develop an agreement that suits their context. It will be necessary to select the sample provisions that apply and to adapt them to the particular circumstances in which patient information is being shared.

The contractual provisions within this document are generally intended for an arrangement where the physician is relying upon the services of another party (e.g. health region, hospital, service provider) to maintain an EMR/EHR system and to maintain patient information in the system on behalf of the physician. In some jurisdictions, the contractual provisions for data sharing within a health region or network may be determined at the provincial/territorial level with assistance from the provincial/territorial medical association. The sample provisions are intended to assist physicians in circumstances where no data sharing framework has been developed at the provincial/territorial/regional level. The provisions could also be modified for use in an Inter-Physician Agreement where a physician will be contracting with other physicians.

It must be emphasized that the information contained in this document should not be considered a replacement for a legal agreement prepared in consultation with legal counsel.

Definitions
The appropriate list of definitions to be included in the agreement will depend upon the contracting scenario, which may include, but not be limited to, the following:

- Parties
- Physician [Comment: The parties will also want to consider whether the definition of physician should include the physician’s employees and agents.]
- Service Provider
- Personal Health Information (“PHI”) [Comment: The definition of PHI may not be limited to patient information, but may include audit trails and other data.]
- Patient
- Applicable Law
- Applicable Privacy Legislation
• Applicable College Policies
• Users and Designated Users
• System [Comment: The system may be a complex EHR or a simple one-way flow of patient information in electronic form, but should be defined in any case.]
• Health Services
• Data Stewardship Committee
• Quality Assurance Information

Each of these terms should be defined in a manner that reflects the particular contracting scenario.

1. Ownership of Personal Health Information/Data Stewardship

SAMPLE PROVISIONS:
• The Parties acknowledge that for the purposes of applicable privacy legislation, all PHI collected by the Physician remains in the custody of the Physician. [Comment: This may not always apply in hospital-based systems.]
• The Service Provider acknowledges and agrees that it shall not acquire any ownership of any PHI, and the Service Provider’s use of the PHI is solely for the purposes of providing the EMR/EHR System and for no other purpose.
• In collecting, using, or disclosing PHI, the Parties shall comply with all applicable law and any provincial/territorial regulatory authority (College) policies dealing with the creation, maintenance, or destruction of medical records.
• Notwithstanding any other provision of this Agreement, nothing in this Agreement nor any liens, claims, and encumbrances granted to any third party by the Service Provider or otherwise shall prevent the Physician from complying with applicable law and any provincial/territorial regulatory authority (College) policies, including without limitation the Physician’s: (i) obligations regarding the creation, maintenance, and destruction of patient medical records; (ii) ability to use patient medical records; and (iii) ability to transition medical records to another service provider in the event of a termination or expiry of the Agreement.
• A Party may disclose PHI in response to a subpoena, warrant, order, demand, or request by a Canadian court or other competent authority with jurisdiction to compel the disclosure, or as otherwise required or permitted by Canadian law. A Party shall promptly notify the other Party if it receives any such order so that the Parties can jointly determine whether to seek a protective order or other appropriate remedy. The Parties shall cooperate with each other as appropriate to help obtain a protective order. If a Party does not obtain a protective order, the Party subject to the subpoena, warrant, order, or demand shall: a) furnish only that portion of the PHI which is legally required; b) exercise reasonable efforts to obtain reliable assurance that the PHI will be accorded confidential treatment; and c) promptly provide to the other Party, copies of the PHI that was disclosed, as well as the request made for the PHI.

2. Confidentiality and Privacy

SAMPLE PROVISIONS:
• The Physician may provide the Physician’s patients with access to their own PHI in accordance with applicable law.
• The collection, use, and disclosure of PHI will be undertaken in accordance with applicable privacy legislation on a “least information necessary to achieve the purpose” principle, with the highest degree of anonymity that is practical in the circumstances. Collection and use of PHI will be on a “need to know” basis.
• In collecting, using, or disclosing PHI, Users shall comply with applicable law and any provincial/territorial regulatory authority (College) policies dealing with the creation, use, maintenance, or destruction of medical records. [Comment: In a sophisticated system, the Parties may wish to establish a Data Stewardship Committee to assist in making decisions regarding the use of PHI in the System, including the use of Data for purposes other than the provision of health services.]
• The Data Stewardship Committee shall be responsible for determining whether and how PHI may be used or disclosed for purposes other than the provision of health services where such uses or disclosure are permitted by applicable privacy law.

3. Security and Access to the EMR/EHR

SAMPLE PROVISIONS:

• The Physician may use PHI on the System for the provision of health services where the use of such information is permitted under applicable law and any provincial/territorial regulatory authority (College) policies. The Physician may use PHI on the System when:
  (a) the Physician is in a clinical relationship with the individual who is the subject of the PHI;
  (b) the Physician is providing health services to the individual;
  (c) the Physician’s use of the PHI is necessary for the provision of health services or for making a determination for a related health service; or
  (d) the PHI is related to and necessary for the current session of care.

• The Service Provider will manage, in a secure manner, any devices, codes, or other security measures it creates for enabling user access to the System.

• The Service Provider will develop, implement, operate, and manage a mechanism, which may include processes and technology, to detect and monitor unauthorized access to the System, and unauthorized use or disclosure of PHI.

• The Service Provider will develop, implement, operate, and manage an incident response process to deal with breaches or suspected breaches of the System or PHI access security.

• The Service Provider will immediately investigate any suspected breach of the System or PHI security where:
  (a) the suspected breach is identified by the Service Provider, or
  (b) such investigation is requested by a participant in its own investigation of a suspected breach.

• Where the Service Provider determines that a breach of the System or PHI security has occurred, it will immediately inform the Physician impacted by or likely to be impacted by the breach.

• With respect to any breach of the System or PHI security, the Service Provider will immediately act to:
  (a) remedy the breach;
  (b) manage and mitigate effects of the breach; and
  (c) develop a strategy for the prevention of a future breach under a similar circumstance.

• The Parties will not allow any person to use PHI in the System unless that person has been authorized as a designated User by the Service Provider.

• The Parties will use all reasonable efforts to protect the System and the PHI against any unauthorized access, use, disclosure, or modification. This obligation shall survive termination of the Agreement.

• The Service Provider shall, in accordance with the terms of this Agreement:
(a) comply with applicable law and any provincial/territorial regulatory authority (College) policies with respect to the security and protection of the PHI. More specifically, the Service Provider agrees to implement and maintain reasonable safeguards for the security and protection of the PHI and shall report regularly on its security measures and activities;

(b) ensure that its employees, agents, and those for whom it is otherwise in law responsible, use the PHI solely for the purposes of and as described in the Agreement;

(c) be fully and solely responsible for the actions of its employees, agents, and those for whom it is otherwise in law responsible respecting the use or disclosure of the PHI and for any unauthorized disclosure or use of the PHI as a result of carrying out its obligations under the Agreement;

(d) regularly monitor access to the System to ensure that only designated Users are permitted access; and

(e) provide the Physician with audit logs of the Physician’s designated Users’ activity in the System upon the Physician’s request, and cooperate with the Physician’s investigations of inappropriate System use by the Physician’s designated Users.

• The Parties shall only permit use of PHI if it is necessary to carry out a collection, use, or disclosure contemplated under this Agreement. Except as otherwise required in the Agreement, wherever possible the parties shall de-identify PHI before using or disclosing.

• The Parties agree that every User of the System shall use and disclose the minimum PHI that is essential to enable the User to carry out one or more of the purposes authorized by the Agreement. The Parties agree that PHI shall only be collected, stored, used, and disclosed as contemplated by this Agreement.

• The Service Provider will utilize technological practices and standards, such as encryption technology, that incorporate reasonable security measures, to protect confidentiality.

• The Service Provider shall ensure that the System can accommodate patient requests to limit access to PHI to specific Users.

### 4. Accuracy and PHI Quality

**SAMPLE PROVISIONS:**

- Corrections or amendments can be made to PHI by the Physician as required, including in response to a request from a patient for a correction to his/her PHI.

- Where a correction or amendment to the PHI the Physician has entered into the System is required after the Physician’s access to the System has been terminated or suspended, upon written notice to the Service Provider, the Service Provider shall forthwith make the correction or amendment and give written notice to the Physician that such correction or amendment has been made.

- The Service Provider shall promptly notify the Physician if the Physician has accessed any erroneous or outdated information.

- The Parties shall ensure that the PHI that is collected, used, or disclosed is accurate and not altered, modified, or enhanced except in accordance with this Agreement.

- Each of the Parties agrees, and shall ensure that the PHI that it has collected and makes available for disclosure to and use by the other Parties under this Agreement, should be accurate and no Party shall alter, modify, or enhance that PHI except in accordance with this Agreement.

### 5. Record Maintenance Requirements

**SAMPLE PROVISIONS:**

- A Physician may access the System and use PHI on the System for conducting practice self-audits as follows:

  (a) to determine whether the requirements of an applicable professional regulatory body are being maintained and its guidelines adhered to;
(b) to determine whether the requirements of any other governing or overseeing body are being maintained;
(c) to determine whether the practice’s claims submissions are accurate and their claims practices are compliant with applicable requirements;
(d) to determine whether the practice’s own written standards and procedures are being effectively and efficiently executed; and (e) for any other purpose essential to the practice’s effective operation in the provision of health services to individuals.

- The Service Provider shall not access records relating to a Physician’s self-practice audit or use or disclose the records relating to a self-practice audit without authorization from the Physician.
- PHI may be provided to a health professional body at the Physician’s request where:
  (a) the Physician has complied with any other legislation authorizing or requiring the Physician to disclose that information for that purpose;
  (b) the PHI is required with respect to an investigation, discipline proceeding, or practice review; and
  (c) the PHI,
    i. has been entered by a member of the requesting health professional body, or
    ii. pertains to an activity of a member of the requesting health professional body.
- The Service Provider shall establish a data stewardship committee (“Data Stewardship Committee”) which shall have oversight of the collection, use, disclosure, management, and retention of PHI in the System. The Data Stewardship Committee shall include Physician representatives. [Comment: The Agreement should define the composition of the Committee and how/whether the Committee will have access to the PHI in the System.]
- The Data Stewardship Committee shall periodically assess compliance with this Agreement by the Parties and shall create policies and procedures to facilitate such compliance.
- The Data Stewardship Committee shall conduct periodic and/or random audits of access to the System and use or disclosure of PHI including assessments of levels of access; the identity of individuals or entities accessing, using, or disclosing PHI; and the purposes of access, use, or disclosure.
- The Service Provider shall ensure that with respect to all PHI, PHI will be created, maintained, or retained with a view to satisfying a Physician’s legal requirements for authenticity and integrity of both the PHI and the process by which it was created. The System shall provide for an audit trail to supply a record of collection, use, access, disclosure, and corrections made to the PHI. [Comment: Agreement may specify additional requirements of audit trail.]
- In the event that the Physician becomes involved in a medico-legal matter, the Service Provider shall ensure that the Physician will have access to the PHI required by the Physician with respect to care provided by the Physician to the patient. PHI shall be created, maintained, or retained with a view to satisfying applicable requirements regarding the integrity of the PHI and the process by which the PHI was created. The PHI should be maintained for a period that is consistent with applicable record retention requirements, and the PHI shall be made available to the Physician in the event of a medico-legal matter.
- When, in accordance with applicable law and any provincial/territorial regulatory authority (College) policies, PHI is required to be destroyed, the Service Provider shall ensure that the PHI has been destroyed in an appropriate manner consistent with applicable law and any provincial/territorial regulatory authority (College) policies.
- The Service Provider shall ensure that the System can accommodate the storage of PHI such that the content and form of the PHI complies with applicable law and any provincial/territorial regulatory authority (College) policies or electronic record maintenance requirements.
6. Quality Assurance

SAMPLE PROVISIONS:

- The Service Provider shall ensure that any PHI designated as “quality assurance information” shall be segregated in the System and made accessible only to specified Users who are involved in the quality assurance/quality improvement review.

7. Services and Functionality

SAMPLE PROVISIONS:

- **SERVICES**: The Service Provider shall provide the electronic medical record/electronic health record and related services, functions, as set forth and described in Schedule “A” attached hereto (the “EMR/EHR Services”). [Comment: The specific EHR/EMR services will need to be described in detail in a service schedule.]

- **SERVICE LEVELS**: The Service Provider’s performance of the EMR/EHR Services shall comply with the terms and conditions of this Agreement; shall meet or exceed the service levels, response times, and other performance criteria set forth in Schedule “B” attached hereto (the “Service Levels”); and shall at all times be in compliance with applicable law and any provincial/territorial regulatory authority (College) policies. [Comment: The service level schedule will define specific service levels which must be met by the Service Provider. This may include an availability requirement and the schedule would detail how such a requirement would be calculated. Sample language is provided as an example.]

SERVICE LEVELS

- **HOURS OF OPERATION; RESPONSE TIME**: Physician support calls will be responded to by the Service Provider’s appropriate call centre on business days during the call centre’s normal hours of operation which are [•]. The Service Provider will use reasonable efforts to respond to a service call promptly after the call is received by the Service Provider’s call centre representative. The Service Provider shall respond to support calls and remedy any and all problems within the time frames set forth in this Agreement.

- **MAINTENANCE**: The Service Provider shall provide scheduled maintenance (“Scheduled Maintenance”) for the purpose of general maintenance and upkeep of the System, including, without limitation, general adjustments to the System, the installation of bug fixes and patches, and the implementation of updates, upgrades, revisions, and new versions of software and hardware. The Service Provider shall also provide remedial maintenance (“Remedial Maintenance”), including responding to problems encountered by the Physician when the Physician reports problems to the Service Provider. The Service Provider shall give the Physician no less than [72] hours’ notice of any Scheduled Maintenance. Scheduled Maintenance shall be limited to no more than [8] hours per calendar month, unless the Physician requests additional Scheduled Maintenance or the parties otherwise agree additional Scheduled Maintenance is appropriate, and Scheduled Maintenance shall be conducted whenever practicable during non-peak hours.

- **SYSTEM AVAILABILITY**:
  
  (i) “System Availability” means the ratio of minutes that the System is available (excluding Scheduled Maintenance) in any rolling three (3) calendar month period to the total number of minutes in that three (3) month period. Problems or outages caused by systems or providers outside of the Service Provider’s control shall not be included in the calculation of System Availability. [Comment: There are numerous ways of measuring “system availability,” this Section is given as an example.]

[Comment: Remedies of some sort are typically necessary for the Service Levels to have any real consequence. The types of consequences specified in an agreement for a failure to meet service levels need to be tailored to the particular agreement. In agreements where the Physician pays the Service Provider for the Services, it may be appropriate to
provide for some sort of refund or service credit associated with a failure to meet service levels. Service Providers are generally more willing to provide credits than refunds. Such a provision can be more or less detailed depending on the needs of the Physician.

• **THIRD PARTY LICENCES:** The Service Provider, at its sole cost and expense, shall obtain any and all third party licences on behalf of the Physician that are required for the provision of the Services and use of the System. At the Physician’s request, the Service Provider shall promptly provide written confirmation to Physician that all third party software licensors are aware that the Physician is a beneficiary of such third party software licences.  

  [Comment: The Physician wants assurance that the Service Provider has obtained all necessary rights in connection with the operation of the EMR/EHR System.]

• **BACKUPS:** The Service Provider shall use storage media to perform a backup that involves nightly incremental and periodic full backups of the electronic medical record/electronic health records. The Service Provider shall store all backup storage media in a fire-proof area in the Service Provider’s facility. Backup storage media shall rotate to an offsite storage facility periodically.

• **DISASTER RECOVERY:** The Service Provider shall at all times implement and maintain the following disaster recovery measures:

  (a) **Fire.** The Service Provider facility shall contain an automated fire suppression system that will not affect any of the equipment or systems but will immediately extinguish a fire.

  (b) **Power.** The Service Provider shall use multiple power sources to ensure an uninterrupted power supply to the Service Provider facility in the event of a power failure.

  (c) **Server Failure.** All Service Provider servers shall be either redundant or load balanced to allow for any system to go down and not in any way interrupt use of the System nor affect the functionality, capacity, availability, or performance of the System.

• **SECURITY:**

  (a) The Service Provider shall use appropriate best practices for security access control technology for all access to the System, with access restricted to authorized persons. The Service Provider shall provide adequate firewall protection and intrusion detection systems in order to secure the PHI from unauthorized access, alteration, or destruction by third parties, and shall use appropriate, industry best practice security technology to ensure the security of all transmissions to and from the System and to prevent the corruption, loss, destruction, or misdirection of such transmissions. The Service Provider shall immediately notify the Physician of any security or system integrity breaches or holes and shall take all reasonable steps to remedy the situation.  

  [Comment: Agreement may specify appropriate levels of protection required, including encryption requirements.]

  (b) The Service Provider shall employ system security measures which meet or exceed any and all applicable standards required by applicable law and any provincial/territorial regulatory authority (College) policies for Physicians operating electronic medical record or electronic health record systems. The Service Provider shall keep all such systems maintained and current, and shall install all updates, upgrades, enhancements, new versions, and required patches in a timely manner. The Service Provider will promptly notify the Physician of any security breaches or known security vulnerability of the System.

• **TRANSITION ASSISTANCE SERVICES:** In the event this Agreement is terminated, regardless of the reason for such termination, or upon the expiration of this Agreement, the Service Provider shall cooperate in good faith with the Physician to assist the Physician and another service provider selected by the Physician in the orderly transition of the Services from the Service
Provider’s System to the new service provider’s system. Such assistance will, upon the Physician’s request, include, without limitation, the following:

(i) promptly developing with the Service Provider and its new service provider a transition plan setting forth the respective tasks and timetable to be performed by each party;

(ii) backing up the Physician’s PHI and other information and data;

(iii) assisting the Physician or the new service provider with the loading or transmission of the database;

(iv) assisting the Physician or the new service provider in resolving any connectivity or configuration problems;

(v) rendering such assistance as is reasonably necessary to enable all necessary or appropriate conversions of Physician PHI, and other information and data to the new system; and

(vi) providing any and all other assistance to the Physician until the service is transitioned to the new service provider’s system.

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

SAMPLE PROVISIONS:

- Upon the termination or expiration of this Agreement:
  (a) the Data Stewardship Committee shall assume responsibility for the interim maintenance of the Data;
  (b) within sixty (60) days of termination, the Data Stewardship Committee shall ensure that all Physicians who have contributed PHI receive copies of such PHI, together with copies of all other PHI contributed subsequently that has altered, modified, enhanced, or is otherwise related to such PHI in such format as that the Physician requires; and
  (c) the Data Stewardship Committee shall not otherwise alter, modify, enhance or destroy the EMR without the approval of the Physician.

9. Termination for Convenience

SAMPLE PROVISIONS:

- Termination for Convenience: The Physician may terminate [this Agreement] or [its participation in the System] without cause by providing [thirty (30)] days written notice:

- Termination for Bankruptcy/Insolvency: Either Party may terminate this Agreement, upon written notice to the other Party, if the other Party is subject to proceedings in bankruptcy or insolvency, voluntarily or involuntarily; if a receiver is appointed with or without the other Party’s consent; if the other Party assigns its property to its creditors or performs any other act of bankruptcy; or if the other Party becomes insolvent and cannot pay its debts when they are due.

- Termination for Breach: In addition to any other rights and remedies available to it, the Physician may immediately terminate this Agreement in the event of a breach of this Agreement by the Service Provider provided that such breach is not cured.
within [# of days (e.g., seven)] days of notification by the Physician of such breach.

10. Indemnification

SAMPLE PROVISIONS:

• The Service Provider agrees to be liable to and to indemnify and hold the Physician, its employees, subcontractors, agents, and suppliers harmless from any and all claims, demands, suits, actions, causes of action, or liability of any kind whatsoever for damages, losses, costs, or expenses (including legal fees and disbursements), or other amounts that may arise, directly or indirectly, as a result of:
  (a) any breach of applicable law;
  (b) any breach of the Agreement;
  (c) any unauthorized collection, use, or disclosure, or alteration of PHI;
  (d) any unauthorized exchange of PHI;
  (e) any unauthorized access to the System;
  (f) any breach of the security or privacy of PHI the Physician has entered or has provided access to through the System; or
  (g) any unauthorized alteration (including, without limitation, unauthorized access) of the PHI the Physician has contributed to the System, or caused by the Service Provider, its employees, agents or others for whom the Service Provider is legally responsible.

• INDEMNIFICATION PROCESS: The indemnifying party will defend and settle, at the indemnifying party’s own expense, all such claims and will pay all awards, damages, costs, and other amounts awarded to the claimant or agreed to in a settlement, including the indemnified party’s reasonable legal fees and expenses prior to the indemnifying party assuming control of the defence to such claims and the reasonable and necessary expenses relating to cooperation requested by the Indemnifying Party under Section [ ].

• INDEMNIFICATION CONDITIONS: The indemnified party shall have control over the defence, final award, or settlement of such claim, provided that the indemnifying party shall not compromise or settle a claim in the name of the indemnified party without the indemnified party’s prior consent. The indemnified party shall cooperate with the indemnifying party in such defence and settlement.

11. Limitation of Liability

SAMPLE PROVISION:

In no event shall any provision of this Agreement limit or exclude the Service Provider’s liability for any unauthorized or unlawful collection, access, use, or disclosure of PHI.

12. Representations and Warranties

SAMPLE PROVISION:

• The Service Provider represents and warrants to the Physician that:
  (a) it has the full power and authority to enter into and perform its obligations under this Agreement;
  (b) there are no outstanding contracts, commitments, covenants, or agreements to which the Service Provider is a party which conflict with this Agreement or which may limit, restrict, or impair the rights of the ability of the Service Provider to provide the Services and perform its obligations hereunder;
  (c) all of the Services to be performed by it hereunder shall be rendered in a competent, professional, workmanlike manner by knowledgeable, trained, and qualified personnel;
  (d) the Services shall at all times be provided in conformance with the Service Levels and other performance criteria set forth in this Agreement and in any documentation and other materials provided by the Service Provider;
  (e) the Service Provider’s technology does not and shall not violate any applicable law, or any provincial/territorial regulatory (College) policies;
(f) the Services do not and shall not violate, infringe, or misappropriate the patent, trade-mark, copyright, trade secret, or other intellectual or proprietary right of any third party; and the Service Provider owns or otherwise has the right to use the System in connection with providing the Services hereunder;

(g) it will comply with all applicable law and any provincial/territorial regulatory authority (College) policies in the performance of its obligations hereunder; and

(h) it shall remain primarily responsible for the performance of its obligations under this Agreement.

13. Dispute Resolution
SAMPLE PROVISIONS:
• **DISPUTE RESOLUTION**
  (a) *Escalation Procedure:* If the Parties are unable to settle a dispute arising from this Agreement, then notice shall be provided to the Physician and the Service Provider. In the event the Parties are not able to resolve the dispute within five (5) Business Days of the receipt of such notice, then either Party may request that the matter proceed to arbitration in accordance with the laws of [province/territory of the Physician] then in effect. The decision of the arbitrator, which may include an award of costs in the matter, shall be final and binding upon the Parties.

  (b) *Continued Performance:* Subject to the provisions of this Agreement and other than the specific subject matter of the dispute, the Parties shall continue the performance of their obligations during the resolution of any dispute or disagreement, including during any period of arbitration, unless and until this Agreement is terminated or expires in accordance with its terms.

  (c) *Injunctive Relief:* Notwithstanding the provisions of this Section, each Party shall retain the right and nothing shall prevent either Party from seeking immediate injunctive relief if, in its business judgment, such relief is necessary to protect its interests prior to utilizing or completing the dispute resolution processes described in Section [], including without limitation, in respect of a claim by a Party based on a breach of the confidentiality obligations herein.

14. Governing Law/Forum
SAMPLE PROVISION:
• **GOVERNING LAW/FORUM:** The Parties hereby agree that their relationship and the resolution of any and all disputes arising therefrom, including any issues related to this Agreement, shall be governed by and construed in accordance with the laws of the Province or Territory of and the laws of Canada applicable therein.

• **JURISDICTION:** The Parties hereby acknowledge that the Services will be provided in the Province or Territory of [insert province or territory where Physician is located] and that the Courts of the Province or Territory of [insert province or territory where Physician is located] shall have exclusive and preferential jurisdiction to entertain any complaint, demand, claim, or cause of action whatsoever arising out of this Agreement. The parties hereby agree that if either of them commences any such legal proceedings they will only be commenced in the Province or Territory of [insert province or territory where Physician is located] and hereby irrevocably submit to the exclusive jurisdiction of the Courts of the Province or Territory of [insert province or territory where Physician is located].

15. Funding [Comment: Each Physician will want to ensure that the funding and support infrastructure meets the Physician’s needs. No funding provision is recommended given the variability in which funding might be offered.]
CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

During my employment with the __________________________, I acknowledge that I will be given access to patient information that is deemed sensitive and/or confidential.

I agree that:

a) I shall not share this information, material, or documents (information) with persons within or outside of the __________________________ who are not authorized to have this information.

b) I shall not publish such information.

c) I shall not communicate such information without authority.

d) I shall not use or disclose any such information for other than authorized official purposes.

e) I shall not remove any such information from the premises without permission.

f) Should I receive any such information, I will accept full responsibility to ensure the confidentiality and safe-keeping of this information.

g) I shall take every reasonable step to prevent unauthorized parties from examining and/or copying and such information.

I understand that these rules apply both during and after my employment with __________________________ and that any infringement by me of these rules may be grounds for the termination of my employment and/or legal action.

______________________________  ______________________________
Name (print)   Signature

______________________________  ______________________________
Witness  Date