



Transition to Electronic Medical Records (EMR)

CPSA Guideline

September 2004

This information is provided to assist practitioners in making decisions related to the transition to using electronic medical records in their practice. These comments are not intended to answer all questions or cover all potential situations nor should this document be interpreted as legal advice. Physicians are encouraged to consult specific references and sources for detailed guidance regarding selection of hardware, software and practice management issues. In this document electronic medical record (EMR) refers to the physician's office system for the management of their patients records as distinct from an electronic health record (EHR) which is a health system resource of widely shared clinical information.

A. Introduction

Medical records are an integral part of medical practice. The content and standards for medical records are described in a separate Policy of the College of Physicians and Surgeons of Alberta entitled **Physicians' Office Medical Records**¹. The purpose of this guideline is to address quality of care, patient safety, ethical, and medico-legal aspects of the transition of a medical practice from paper based medical records to using an electronic medical record (EMR).

Within a physician's office, the medical record performs multiple functions in that it:

- Maintains the history of patient care.
- Supports the workflow of the clinical and administrative functions within the office for physicians and staff.
- Supports the communication with external sources of medical information such as hospitals, laboratory and radiology clinics as well as consultations and referrals with colleagues.

Moving to an electronic medical record represents a paradigm change for the physician, both in the ability to manage patient information, and in the design of clinical processes. It also establishes new and/or changing responsibilities for the use, disclosure and security of the medical record. As a result, the transition from paper to electronic medical records is a complex task and must be managed from many aspects - clinically, administratively, culturally and organizationally. The transition activity must include not only the process changes inherent in the use of a new tool, but also the technical and procedural training, and the resultant changes to physician and staff roles within the office.

While the change in medical record modality from paper to electronic systems represents a major transition, care should be taken not to impact the patient-physician relationship. Nor should the integrity of the clinical processes or the continuity of care be impaired during the transition period.

Five key principles have been identified to guide the transition process:

- Patient information must be secure.
- Privacy of patient information must be maintained.
- The integrity of the medical record content must be maintained.
- The integrity of the clinical workflow supported by the medical record must be maintained.
- Continuity and quality of care must be maintained through the transition period.

Each principle has recommendations as well as considerations for their application. Note that the principles are not discrete - they are intended to work interdependently.

This document deals with a complex undertaking and has many technical references which may at first glance be overwhelming for those physicians at the beginning of the transition or contemplating a transition. External resources may be useful to assist in your understanding of these recommendations and their application to your practice.

These recommendations can be a valuable checklist before, during and after the transition to evaluate and guide your implementation.

B. Principles and Implementation

1. Patient information must be secure.

The security of paper-based medical records is primarily based on physical security while electronic medical records present many new issues and threats that must be considered (e.g. denial of service with viruses, loss of data due to corruption of computer hardware, theft of data due to intrusion, etc.). Effective security is a combination of administrative practices, physical security and technical security and should ensure the integrity, confidentiality and availability of the medical record.

Recommendations:

- Practices should undertake a formal risk assessment that considers local risk factors and dependencies, and develop a practice security policy and system management practices. Standards are available to provide guidance in these areas⁹.
 - Each practice should establish an initial assessment of the security risks including administrative practices, physical security and technical security to ensure the integrity, confidentiality and availability of the medical record.
 - Security policies and staff education should be implemented to address specific security threats.
 - Monitoring of security logs and reports should be performed on a regular basis to assess the performance of the security measures.
 - Major security events or technical changes should trigger a security review.
- Physical security measures must be implemented to prevent unauthorized access or potential loss or failure to the system. Risk factors include theft, power failure, natural disasters and deliberate tampering.
 - Access to hardware, software and storage media should be controlled, particularly to centralized data storage.
 - Hardware that is accessible by unattended patients (i.e. in an examining room) should always be explicitly locked down to prevent access.
 - Screens that are viewable by patients should not display sensitive information of other patients (i.e. scheduling information with diagnostic information).
- Access and authorization processes must be implemented to ensure only legitimate users have access to the medical record and that each user has the appropriate level of access to the medical record.
 - Every user including staff, students, and locums must have a unique identification and user-ID with appropriate password controls.
 - Audit logging must be enabled to record actions taken by each user.
 - Authorization rules are defined and implemented by user-ID (or ID's attached to security groups) to provide access to the medical record.
 - Adequate network security (such as firewalls, Virtual Private Networks, second factor authentication, etc.) is implemented to ensure that only authorized and authenticated users can access the medical record.

- The integrity and confidentiality of the medical record must be ensured.
 - Audit logs are maintained to support the authenticity of medical record additions, or updates. Access to files or databases underlying the medical record software is restricted.
 - Changes to locally created data within the medical record are by addendum or strike-through as per the medical records policy¹.
 - External documents stored in the medical record should be in read-only formats.
 - Disclosures of the medical record via email to patients or to providers must have adequate protection. The CMPA has specific recommendations for email to patients or to other health care providers¹² including that email messages that contain patient information are encrypted and are supported by a patient consent to utilize email. Other options include the use of password protected attachments within an email.
 - Adequate virus protection must be in place to ensure data is not modified or destroyed by external processes.
 - Disposal of storage media (including redundant hardware, temporary storage, back-up media, etc.) must be complete. This would include physical destruction of the media and/or re-formatting to prevent unauthorized access – deleting the information does not physically delete the data, only the indexing information.
- The reliability and accessibility of the application hardware and software must be ensured.
 - A back-up of the medical records should be performed on a regular schedule (at least daily). There should be a cycle of back-up media to minimize exposure to failed backup media.
 - Back-up media should be stored at a secure off-site location.
 - Testing of the restore process and back-up media should be done on a regular schedule.
 - A contingency plan should be in place for disaster recovery and denial of service attacks. In the event of an emergency or disruption to data accessibility, a predefined plan of action should come into play including technical and clinical resources, data recovery plans, manual scheduling and charting, follow-up on reports, etc.
 - Hardware and software (application and operating systems) should be maintained at reasonable levels of currency for support and maintenance by the vendor.
- Pearls
 - The public visibility and emotional threat of hackers are often seen as the major security threat however the vast majority of security breaches occur within organizational domains by personnel with legitimate authorization.
 - System back-ups are an integral part of system management, however the testing of the backups through a recovery process is often less rigid and may not be fully understood. It is good practice to ensure recovery testing is performed on a regular basis, especially after a system upgrade (hardware or software), and that the process is documented.
 - Enhanced security is required where networks are more exposed (i.e. those with wireless devices and remote access), or where equipment that store information on local drives which are at risk of loss or theft (i.e. portable devices such as laptops, PDA's, tablets). In these instances additional encryption or authentication processes are usually required.

2. Privacy of patient information must be maintained.

Electronic records enable a dramatically enhanced capacity for the management of patient information. This increased potential needs to be evaluated in terms of the professional/ethical responsibility to maintain patient records and also the legal responsibilities as a custodian of health information.

Recommendations:

- Physicians should establish formal protocols and procedures to ensure that patient information is documented, maintained, and disclosed in accordance with the current laws and standards set forth by the Health Information Act³. The Office of the Information and Privacy Commissioner has provided guidelines for health information custodians and the Physician Office System Program have established a reference guide which can provide guidance on specific

policies required by legislation². Note that the completion and submission of a Privacy Impact Assessment is required under the Health Information Act prior to the implementation of an Electronic Medical Record system^{2,3,5}.

- Physicians have a fiduciary and professional responsibility to collect patient information with sufficient information to allow another practitioner to assume the patient's care at any point in the course of treatment without the loss of continuity¹. This responsibility extends to disclosures for the release and transfer of medical records and the confidentiality in the intra-professional exchange of information. The Health Information Act³ defines the parameters for the disclosure and use of health information and the requirements for the collection of consent. Physicians should be prepared to advise patients what their access control policies are within the practice. Patients' requests to apply restrictions or to suppress information to one or more named clinicians should be considered carefully, although other legal or ethical factors must be considered.
- Electronic medical records dramatically increase the ability of physicians to use patient information for new purposes, based on the ability to search, aggregate, correlate and otherwise manipulate individual information. Care must be taken to ensure that any use or disclosure of health information complies with the Health Information Act and as such, appropriate measures such as patient consents and ethics reviews are undertaken when utilizing this enhanced functionality. Personal health information should only be used for the purpose it was collected unless additional consent is obtained. Release of medical information is permitted or required in certain circumstances as defined by legislation. Uses and disclosures of personally identifiable health information for the secondary purpose of research must have appropriate ethics review and approval, and patient consent if required.
- Pearls
 - A patient handout on the privacy policies of the practice may assist in the understanding and assurance of patients that their privacy is still being maintained. Some individuals may have a limited understanding of the privacy framework and information exchange that exists today in a paper-based environment (i.e. higher expectations of the information sharing than what exists today, and also misconceptions of how an EMR is used). Many may also confuse the physician's EMR with the Electronic Health Record, a shared health system tool which has had some media exposure.

3. The integrity of the medical record content must be maintained.

Managing health information in a transitional environment carries the risk that the quality of care may be adversely affected if the transition is not effectively managed. There will be a period of time within most practices where both paper and electronic records will be in use until all relevant patient data has been established in the EMR and all physicians in the practice use the electronic record.

Recommendations:

- As physicians remain the custodian of information regardless of the media in which the information is maintained, it is the responsibility of the physician to ensure that:
 - The complete medical record is accessible at all key clinical decision points.
 - The information is current, accurate and comprehensive for the purpose for which it is required .
 - There must be an audit trail to ensure that if information is altered, there will be a record of the original, the date and time of the alteration, and the identity of the person who made the change¹.
 - Changes to the EMR are made either by a new note or "addendum" or by a stroke through, or both.
- If relevant patient information is maintained externally to the electronic medical record (i.e. in a shared record such as a Provincial or Regional Electronic Health Record), the physician must:
 - Maintain procedures and documentation to support controls ensuring the receipt of result reports and other relevant orders and that appropriate follow-up actions have been taken¹⁰.
 - Ensure that defined procedures are in place to provide care in the event that the external sources of information are not accessible.

- Take adequate steps to ensure that the custodian of the external information source has, and can demonstrate an adequate policy and procedure in place regarding privacy, security, and operational integrity to ensure appropriate standards for network access.
- Ensure that the custodian can and will support the retention and subsequent access requirements as per the medical record policy as defined by the CPSA¹.
- If external electronic interfaces are integrated with the electronic medical record, adequate testing must be performed to ensure that controls are in place to ensure that all records are processed, accounted for, and that existing data cannot be corrupted or lost during the integration.
- Standards for data quality, accountability, and integrity need to be incorporated into the EMR within each practice and adopted to promote uniformity in the data for group practices. The features of quality data elements include:
 - Accessibility – data items should be easily obtainable and legal to collect
 - Accuracy – data are the correct values and are valid
 - Comprehensiveness – all required data items are included
 - Consistency – data is recorded in a consistent manner
 - Currency – the data should be up to date
 - Definition – each data element should have a clear meaning and acceptable values
 - Granularity – the attributes and values of data should be defined at the correct level of detail
 - Relevancy – data are meaningful for the purpose for which they were collected
- In the initial transition period (which could last from 6 months to two years) there will likely be a combination of electronic and paper charts. A defined process and transfer date should be identified for the EMR to become the official medical record (the source of truth) versus the paper chart or other clinical record in use, to prevent failures in the receiving or following up of medical reports¹⁰.
 - Each type of document/report that is received into the office should have a defined process and destination to either the paper chart or the electronic record, or both.
 - There must be a process in place to ensure that there are controls in place to specifically manage the changeover period of the handling of a document/report.
 - All individuals using the records must understand the content and limitations of each of the records in the period of transition.
 - Each record must be clearly identifiable as to its status as the primary medical record, parallel record, or partial record.
 - For the electronic record to be deemed the primary medical record, relevant history from the paper chart must be transferred and/or referenced directly. This is often done in conjunction with a comprehensive review of the chart (i.e. as part of a complete physical, or an insurance report) and should have a standardized process and content.
- The disposition of paper charts once transitioned to an electronic chart must still follow the parameters established in the Physician Office Medical Records policy¹.
 - If the paper chart has been transferred in its entirety in non-editable form (i.e. the entire chart has been scanned into the electronic chart), the paper chart can be disposed as per normal disposition guidelines and the electronic format becomes the clinical history.
 - If paper charts have been summarized with the relevant history transferred after a diligent ascertainment that the clinically relevant material from the past ten years (or further if deemed necessary) has been included, the paper chart may be archived or destroyed. The physician may find it useful to document the procedure used in the transfer indicating the type or rationale of material omitted from the transfer as well as any summarizations.

- Pearls
 - Be cautious of features embedded within the software application which may set default values that may create data in the medical record that was not an actual observation, or the use of a template which may limit the addition of relevant data.
 - Evaluate the requirements you may have to create reports or outgoing documents to determine the structure of your input data (i.e. defining what is text, discrete data elements, scanned reports, etc) so that future data analysis or practice review is enabled. For example, including a prescription within a textual comment in a progress note may render it inaccessible when searching the record for a specific drug based on a recall notice.
 - The Electronic Health Record is an evolving tool which in time may alter the types of information which has traditionally been held within the physician's medical record (i.e. lab results) as this information may be held in centralized source. Given the relative newness of these processes, extra diligence should be taken to evaluate the maturity of these tools, the retention of data by the custodian, and the access processes for historical and medico-legal requirements prior to making the decision to not maintain this data in the physician's medical record.
 - Conformance with Vendor Conformance and Usability Requirements (VCUR)-approved products will help to ensure that acceptable province-wide standards are achieved⁸.

4. The integrity of the clinical workflow supported by the medical record must be maintained.

There are many clinical processes directly or indirectly supported by the medical record. The transition to electronic records may alter these processes which may include important safety precautions or other critical workflow items.

Recommendations:

- The implementation of an electronic medical record will necessitate process changes in the practice workflow and often the roles that the physician and associated staff perform. Many of the workflow processes designed on the movement of the paper chart will no longer be valid and should be formally evaluated and optimized for patient safety and quality of care. The tasks assigned to individuals must fall within guidelines for professional scopes of practice and have a defined delegation of authority.
- The implementation of the technology to support electronic medical records is often accompanied with the capability for electronic mail. Email can be used for internal communication within an office, physician to physician communication, and for patient to physician communication. Emails are an explicit form of communication and therefore are part of the medical record. Care should be taken to ensure the email is attached to the medical record in the same format and location as other external communication. The CMPA has provided guidelines regarding the use of email¹² which should be consulted. At a minimum:
 - Email handling rules (including service levels and purpose limitations) should be explicit and clearly articulated to patients. Consent should be obtained from the patient to clarify the expectations and processing of emails.
 - Physicians should be aware that employers and Internet Service Providers can (and do) store and read emails. Therefore the confidentiality of emails must be taken into account, and email text and attachments should have adequate encryption.
 - Physicians should have procedures for the timely receipt, responses and an escalation process where standards for email management are not met.
 - Text based communication can lack the context and dynamic nature of personal communication therefore the physician needs to recognize the limitations of this type of communication.
- Clinical management processes and controls have traditionally been linked to the physical location and transfer of the paper chart. The lack of a physical chart necessitates the implementation of other control mechanisms to prevent follow-up failures. Specific recommendations for follow-up failures are identified in a separate guideline¹⁰, however the electronic record should at a minimum factor in the follow items:

- Follow-up appointments
 - Referral appointments
 - Reports received
 - Reports handled, signed off and filed
 - Communication attempts
- Processes should be developed to ensure the integration, inclusion, and update of multiple records as they become available at all clinical decision points.
 - Data and charting standards for shared records via networks within and between practitioners should be developed to ensure that another practitioner can assume care of the patient with full understanding of the content of the medical record.
 - Pearl
 - Planning for the implementation of an EMR provides tremendous opportunity for improvements in workflow of the practice, as well as with individual procedures. Remember to balance exploring opportunities to improve current processes, roles or timing based on the paradigm of the paper chart with the limits of the capacity for change by the people involved.

5. Continuity and quality of care must be maintained through the transition period.

The overriding issue during this period of transition is that the level of patient care cannot suffer in a manner that risks patient safety or the quality of care. First, do no harm ...

Recommendations:

- A good management strategy is essential to ensure that the implementation of the electronic medical record does not expose the patient to risk. This should include at a minimum:
 - A readiness assessment
 - Education & administrative needs
 - Clinical practice and workflow definitions
 - An evaluation of technical requirements
 - Definition of staff roles & delegation of authority
 - Design of the conversion and hybrid system processes
 - Implementation of safety and control processes
- There must be an assurance of the competency of resources in the use of the technology and of the process changes that have been implemented.
- Pearls
 - Critical for the successful implementation is the appointment of a clinical technology leader for the practice. This person must have a dedicated allocation of time to provide technical support, design and manage enhancements to workflow and to develop data and charting standards.
 - The introduction of any form of change usually is accompanied by a period of lost efficiency during the implementation period, and is also a period of high stress. Care to manage the overall workload during this period is essential.

C. Conclusion

The transition to electronic medical records (beyond the implementation of the hardware and software) represents a significant change to the clinical processes in a medical practice. These changes must be carefully considered to ensure patient safety and quality of care throughout the transition period, primarily through the continued integrity of the medical record and the clinical

processes that are supported by the medical record. In addition, changes that are inherent with the change to electronic records such as patient privacy and information security must be managed.

The transition to electronic records is a major step in its own right. However, this transition is also the beginning step in a much larger transition period both within the practice and in the health system as a whole. Once the medical record is in electronic form, there will be further opportunities to initiate clinical practice changes at an individual patient level, at the practice level as well as at the population level.

Important Reference Sources

1. Physicians' Office Medical Records. CPSA June 2003
<http://www.cpsa.ab.ca/publicationsresources/policies.asp>
2. HIA Guide to Policies and Procedures for Physician Offices. POSP February 2003
HIA Guide to Privacy Impact Statements. POSP February 2003
3. Health Information Act of Alberta. OIPC
<http://www.oipc.ab.ca/ims/client/upload/HIAResearch.pdf>
http://www.oipc.ab.ca/ims/client/upload/HIA-at-a-Glance_for_Custodians.pdf
<http://www.oipc.ab.ca/hia/>
4. Release of Medical Information: A Guide for Alberta Physicians. CPSA. March 2003
<http://www.cpsa.ab.ca/publicationsresources/policies.asp>
5. Privacy Impact Assessments.
<http://www.oipc.ab.ca/pia/template.cfm>
6. Release of Data for Research Purposes.
www.health.gov.ab.ca/system/key/research/data.html
7. CMA Health Information Privacy Code.
<http://www.cma.ca>
8. Vendor Conformance and Usability Requirements.
https://host.softworks.ca/agate/ama_posp/non_public/documents/VCUR.asp
9. COACH Guidelines for the Protection of Health Information.
http://www.coachorg.com/downloads/guidelines_order_form.pdf
10. Preventing Follow-up Failures when Caring for Patients. CPSA August 2000
<http://www.cpsa.ab.ca/publicationsresources/policies.asp>
11. The Referral/Consultation Process. CPSA June 2003
<http://www.cpsa.ab.ca/publicationsresources/policies.asp>
12. Physician-Patient E-Mail Communication: Legal Risks. Canadian Medical Protective Association Information Letter. December 2003
<http://www.cmpa-acpm.ca/>