Data Sharing Agreement Outline for Physician Group Practices

The development and use of a shared Electronic Medical Record (EMR) is complex. The primary purpose of the EMR is to document the care provided to the patient. The maintenance of these records, particularly when more than one user (or custodian) has access to them, is even more challenging and requires proactive communication amongst the EMR users. **Each user must ensure the following:**

- The information is maintained in a confidential and secure manner
- The data is easily retrievable for continued care
- The use must meet the physician's fiduciary and statutory obligations

This Data Sharing Agreement Outline is meant to provide a framework for constructing practical solutions for your unique circumstances. We recommend that you use this outline to document your agreements and expectations in order to facilitate smooth EMR implementation and maintenance. The Data Sharing Agreement will often be a parallel document with Information Manager Agreements, Service Agreements, etc. **Statements made in this document** regarding the roles and responsibilities of vendors and participating physicians **are for illustration purposes only,** and must be confirmed or edited by the participants of the shared EMR solution.

Your privacy officer is responsible for information security throughout your clinic. In particular, he or she is accountable for ensuring that appropriate administrative, technical and physical security features are in place to protect confidential information. By filling this important role, you are ensuring there is someone at your clinic who can respond to staff and patient questions about privacy and information security. **For more information about privacy officers, please see the article: "Privacy Officer's To Do List."**

This Document Management Tip is intended to help you along your journey by guiding you through a series of questions and providing resources to get started.

It is expected that you will review and refine these documents to meet your needs.

For further assistance, contact us:

Jean L. Eaton, B Admin, CHIM
The Practical Privacy Coach and Practice Management Mentor
INFORMATION MANAGERS LTD.
www.informationmanagers.ca
Email: jean@informationmanagers.ca
LinkedIn ca.linkedin.com/in/jeaneaton/
Twitter @InfoManLtd

author of the forthcoming books, "*Privacy Breach Management Resource Package*" and *"Practice Management: Easy to Follow Steps to Start a New Clinic and Improve Your Established Clinic".*

Privacy Impact Assessments

All custodians of health information are required to submit a Privacy Impact Assessment (PIA) to the Office of the Information and Privacy Commissioner (*HIA* sections 62, 63, 64). Each participating physician (or clinic) must have a PIA accepted by the Office of the Information and Privacy Commissioner (OIPC).

Ownership of the patient records

When a physician documents information in the EMR, he or she becomes the custodian of that specific data. Therefore, it is necessary for each physician to use his or her unique user login and password to record each entry in the record. This signature consistently identifies the author of the notation. If the author is the physician, he or she becomes the custodian of this encounter. Even if the author is an affiliate (employee) of the physician, the physician is still the custodian of this encounter. Physicians' rights and duties as custodians apply to all records to which they have access in the group. **This may mean that there are multiple custodians for each record, if more than one physician was involved in the care of the patient.**

If a physician leaves the shared EMR solution, the remaining physicians must decide:

- Will the remaining physicians assume the ongoing management of the records?
- If the exiting physician intends to practice elsewhere and requests access to his or her patients' records, how will this be accommodated?
  - In what media? Hard copy, electronic, etc
  - At what cost?
  - Who will assume the cost? The departing physician, the patient, or the remaining physicians?

Data Governance

The shared EMR uses a common database structure. **To ensure consistent and accurate information for patient care** (and other business reasons), **it is important that key data elements are defined and maintained.** For example, how will 'user defined fields' in the EMR application be used? How will 'patient alerts' be used? When options for screen display are made available by the vendor, who will make the decision on behalf of the participating users?

- **The clinic physician lead will make decisions on data governance issues.** Where appropriate, consultation will be made with physicians and other users of the EMR application. These decisions will be communicated to all participating physicians by the EMR system administrator.
- **Data elements standards will be documented by the EMR system administrator.** The system administrator will monitor and make suggestions to the vendor in order to improve or maintain data integrity.

Access Authorization

- **Each participating physician will provide shared EMR access to their employees and affiliates.** The EMR system administrator will create unique user login accounts with role-based privileges. (See Shared EMR Access Request Form)

- Physicians, authorized clinic employees and vendors may be granted access to the clinic's wireless network and/ or remote access to the clinic EMR.

- **A participating physician may choose to permit other authorized users view-access to his clinic group's entries in the patient record.** This shared access facilitates continued care and treatment for the patient amongst the participating physicians.

- If a physician chooses to restrict view-access from other shared EMR users, how do other users see that there is a clinic note for the patient which the user does not have permission to access?

- **Confidentiality and security of information are addressed as part of the conditions of employment for clinic staff.** Staff must be appropriately trained in regard to policies and procedures for safeguarding information.

- The vendor will assist the participating custodians in the training of their new employees in the shared EMR system and related applications.

Privacy and Security Breaches

A privacy breach can take place when there is unauthorized access, collection, use, disclosure or disposal of personal or health information. In the event of a (suspected) privacy or security breach:

- Notify the primary custodian (physician lead) of the breach
- Notify the clinic's privacy officer
- Notification to the OIPC, POSP, Netcare, other information sharing partners may be required

Access Requests

It is each participating physician's responsibility to receive and respond to access requests from his or her patients. This function may be delegated to a clinic employee for the purpose of centralized release of information.

Some patients may specifically request that their information not be shared or further disclosed. To ensure that this request is documented in a manner that permits all authorized users access to this request, all users of the shared EMR will use the following 'patient alert fields' in the EMR. Prior to

any disclosure of information, the custodian or his affiliate will ensure that this field is viewed prior to disclosing patient information.

- Detail the EMR field and data standards

Monitoring and Audit

To properly track events of access, verify compliance with privacy policies and procedures, as well as compliance to this Data Sharing Agreement, the System Administrator will be responsible for:

- routine auditing of access to the EMR
- ensuring appropriate role-based, need-to-know access amongst the shared EMR users
- automating these audits, where possible

This publication provides general guidance for a medical office in Alberta. Consultation with your information systems, health records, and privacy office is recommended. For additional assistance, contact Information Managers Ltd.

Additional References for your consideration:

Alberta Medical Association. Shared EMRs Information Management Agreement Working Paper. February 19 2008.

Alberta Medical Association. Shared EMRs Discussion Paper. February 19 2008.

College of Physicians and Surgeons of Alberta. Physicians' Office Medical Records CPSA Policy. Revised August 2005.

College of Physicians and Surgeons Medical Informatics Committee. Data Stewardship Framework version 1.2. December 1 2006.

Foundation of Research and Education of American Health Information Management Association. State Level Health Information Exchange Intiative Development Workbook. 2006

Information and Privacy Commissioner Ontario. Model Data Sharing Agreement. Tom Wright, Commissioner. December 1995. http://www.ipc.on.ca/english/Resources/Best-Practices/Best-Practices-Summary/?id=30 retrieved July 17 2009

Canada Health Infoway Inc. White Paper on Information Governance of the Interoperable Electronic Health Record (EHR). March 2007.