

Data Sharing Agreement Outline for Physician Group Practices For Discussion

The development and use of a shared Electronic Medical Record is complex. The primary purpose of the EMR is to document the care provided to the patient. In order to ensure that this information is maintained in a confidential and secure manner in a method that is retrievable for continued care and meet physician's fiduciary and statutory obligations requires communication and understanding amongst the EMR users.

This Data Sharing Agreement Outline is meant to provide a framework for constructing practical solutions for your unique circumstances. I hope that you will use the Outline to document agreements and expectations that will facilitate smooth implementation and maintenance of your EMR. 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 Vendor and participating physicians are for illustration purposes only and must be confirmed or edited by the participants of the Shared EMR solution.

Privacy Officer, is responsible for information privacy and security, including ensuring that appropriate administrative, technical and physical security features are in place to protect health information. His position as Privacy champion will ensure that there will always be someone at the Clinic who is able to respond to patient and clinic staff questions about privacy and information security, and to fulfill any of the other Privacy Officer responsibilities outlined in Privacy Officer Responsibilities.

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 Initiative 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.

Introductory Matters

Custodians (physicians) 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.

Each physician who documents in the EMR is the custodian of that information. It is important that each physician use his uniquely identifying user login and password to record each entry in the record. This consistently identifies the author of the notation. If the author is the physician, the physician is the custodian of this encounter. If the author is an affiliate (employee) of the physician, the physician is the custodian of this encounter. Physicians' rights and duties as custodians will apply to all records that they have access to in the group. This may mean that there could be 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 is it the intent of the participating physicians that

1. The remaining physicians of the clinic will assume the ongoing management of the records?
2. If the exiting physician intends to establish a practice elsewhere and requests access to his patient's records, how will this be accommodated?
 - a. In what media? Hard copy, electronic, etc
 - b. At what cost?
 - c. Who will assume the cost? The departing physician, the patient, 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 the way a screen display is made available by the vendor, who will make the decision on behalf of the participants?

3. 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.
4. Data elements standards will be documented by the EMR System Administrator. The System Administrator will monitor and may suggest to the Vendor changes to improve or maintain data integrity.

Access Authorization

5. Each participating physician authorizes their employees and affiliates access to the shared EMR. The EMR System Administrator creates the unique user login account with role based privileges. (See Shared EMR Access Request Form)
6. Physicians and authorized clinic employees and vendors may be granted access to wireless network and/ or remote access to the Clinic EMR.
7. The participating physician may choose to permit other shared EMR 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.
8. If a physician chooses to restrict view access to other EMR users,
_____ (what message on the EMR do other users see that indicates that there is a clinic note for the patient that the user does not have permissions to access?)
9. Confidentiality and security of information are addressed as part of the conditions of employment for Clinic staff, and that staff must be made aware of, and appropriately trained with regard to, policies and procedures for safeguarding information.
10. The Vendor assists the custodian participating in the Shared EMR in training their new employees to the EMR and related applications.

Privacy and Security Breaches

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

11. Notify the primary custodian (physician lead) of the breach.
12. Notify the Privacy Officer of the Clinic
13. May require notification to the OIPC, POSP, Netcare, other information sharing partners.

Access Requests

14. Each participating physician maintains its responsibility to receive access requests (including release of information requests) from their patients and respond to them appropriately. This role may be delegated to a clinic employee for the purpose of centralized release of information function.

15. A patient 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 view 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.
- a. Detail the EMR field and data standards

Monitoring and Audit

To properly track events of access and verify compliance with privacy and confidentiality policies and procedures and this Data Sharing Agreement, the System Administrator will be responsible for routine auditing of access to the EMR and appropriate role based, need to know access amongst the users of the Shared EMR. Where possible, these audits will be automated.