Information Sharing Agreements for Disclosure of EHR Data within Canada

Prepared for the Pan Canadian Health Information Privacy (HIP) Group

Authored by: Elaine Sawatsky, January 2010

Table of Contents

Purpose of the Document 3
Methodology: Sources of information 3
Observations 4
Titles of Agreements 4
Purpose of Agreements 4
Content of Agreements 5
Approach to Agreements 11
Structure of the Agreements 15
On-going work: Enforcement & Agreement Maintenance 16
Summary 16
Samples 17

Introduction: The interoperable EHR - iEHR

The vision for a pan-Canadian EHR or interoperable EHR (iEHR) is one in which personal health information is available to support patient care no matter where in Canada the person is receiving care, as well as health system administration. The iEHR will make available to the caregiver, in a privacy-protective manner, the information needed to treat a patient from another jurisdiction -- and to also make available to caregivers in the home jurisdiction the information they need for the patient's follow-up care. Data has always been disclosed on an ad-hoc basis when needed for care and in the existing environment, data disclosure also takes place routinely for administrative uses such as billing, with supporting agreements. While these arrangements are not new, it is the scale and scope of the disclosure which changes in the EHR context. Mitigating the risk associated with disclosure outside the jurisdictional boundary, while ensuring that data is available is the objective of the EHR and the participating parties.

Legislation and requirements for sharing information within and across jurisdictions differ in Canada. Some jurisdictional legislation requires a written agreement for information to be disclosed outside the province, but does not describe what sort of agreement is required. Other jurisdictions specifically require Information Sharing Agreements (ISAs) for any disclosures from their health information banks, whether within or outside the province. Some other jurisdictions which share among custodians or trustees, set out rules in policy

Purpose of the Document

The purpose of this document is to support the work of the Health Information Privacy (HIP) Group by describing the types of agreements in place and their common features.. It also provides an inventory of elements and effective processes, as well as templates and samples, to help jurisdictions define what should be in an ISA to support the disclosure of information in an appropriate manner across jurisdictional boundaries. The document will look at the purpose of ISAs and what they are intended to achieve. It will also describe issues associated with information sharing.

Methodology: Sources of information

The consultant reviewed material from federal, provincial and intra-provincial bodies, private bodies, professional associations, and organizations in Europe and New Zealand. Information was acquired by web searches and direct contact with members of the HIP Group and others.

Contact with EuroRec and the European Federation of Medical Informatics and its special topics conferences on trans-border data flows provided contact and information with European Commission (EC) representatives[1] and other international sources. The sources represented a variety of jurisdictions, business purposes and contexts.

Observations

Titles of Agreements

Many types of agreements are currently in use. Titles include Data Sharing Agreements (DSAs), Data Access Agreements (DAAs), Information Sharing Agreements (ISAs), Memoranda of Understanding (MoUs), Letters of Understanding (LoUs), Service Level Agreements (SLAs) and Contracts. Privacy Schedules or Service Schedules are often attached to contracts. There is little consistency in the terms used to describe the agreements. Titles do not necessarily have a standard meaning nor do they necessarily reflect the agreement content. For example, one *Service Level Agreement* included elements of many types of agreements but little about services. Some organizations call an agreement a *Data Sharing Agreement* if the disclosure is in both directions and a *Data Access Agreement* if the data is disclosed by one organization to another. Some call a *Data Access Agreement* that which controls direct access to another's information, while others use it to mean disclosure without direct access. One interprovincial agreement references law and describes objectives, exceptions and procedures at a very high level but contains little detail. Some agreements are based on principles rather than specific legal authority.

Observation #1: ***In respect of the wide variety of terms used, it may be valuable to consider using a standard term for the agreements required to manage trans-jurisdictional disclosures of EHR information. Alternatively, standard definitions of the terms can be agreed. The term "responsibility agreement" could be used to describe the group of documents used by parties to set out the business relationship and the controls that will be applied.***

Purpose of Agreements

It can be expected that once the Pan-Canadian EHR is in place there will be increased disclosure of information for care and treatment as well as for other uses. Agreements are

[1] Further contact with interviewees including EC representatives is possible.

one of the tools available to jurisdictions to help manage disclosures of personal health information across borders in Canada. Such agreements set out legislative authority and obligations, manage risk, undertake due diligence and to manage service expectations. iEHR partners wish to ensure that the transfer of information across jurisdictional borders is legitimate and carried out securely. Legitimacy is established through law and security through the application of physical, technical and organizational controls, while trust is gained by open and transparent communication, but also may require extensive policy and process design.

Observation #2: ***Agreements tend to be more successful if the business partners know what it is they wish to do, what they agree upon and how they would like to approach their information sharing, before they attempt to draft the agreement.***

Content of Agreements

- The agreement templates reviewed control disclosures for different data purposes and between different types of parties. Data uses included billing, research, data warehousing/linking and clinical uses; the agreement templates were employed between public, private and foreign bodies.

- The agreements and templates ranged widely in complexity and formality. Some address only confidentiality and controls to support it. Some directly state permitted data use while others do not. Some include business objectives and some do not. In one case a "*Letter" of Understanding* was more than forty pages – much longer than its name implies.

Observation # 3: ***One of the foremost principles of the CSA Model Code and fair information management is the requirement to define the purposes for which the data will be used. However, the data purpose was not always explicitly stated in the agreements reviewed, and doing so is important in order to clarify expectations and apply appropriate controls to the various purposes.***

- Some agreements make use of statements of general principles while others use contract clauses or consent.

- Some agreements hold that once data is disclosed, it is under the legal control responsibility of the recipient while others maintain that the disclosing organization retains control.

- Some jurisdictions require a comparable level of data protection available by law in the receiver's jurisdiction before data is disclosed.

- Some agreements prohibit onward disclosure and/or use for other purposes while others do not mention it at all.

- Some agreements control outsourced IT services, but others do not.

- Some agreements were designed to retain tight control over personal records while others control only the financial aspects of a relationship[2].

Observation #4: ***There is little consistency on some very key clauses or issues such as permitted purpose, onward disclosure, and security and confidentiality.***

Current activities in Canada and internationally to develop agreements or agreement templates

- Some jurisdictions are working on agreements for specific internal initiatives while in a few cases agreements for trans-border flows within Canada are underway. Some examples of current work can be found at the federal level in one of the first Canadian inter-jurisdictional EHR initiatives - Panorama, Canada's national public health surveillance and disease outbreak system. Discussions are taking place between the Public Health Agency of Canada (PHAC) and jurisdictions for collection of Panorama-related information from all jurisdictions and it is assumed agreements will be required. In addition, BC and Yukon are currently discussing trans-border disclosure of data and are working on an information sharing agreement to support it.

- The Federal Treasury Board Secretariat (TBS) is currently working on Information Sharing Agreement content and structure. Past work by the TBS in this area, including its guidance documents, is widely used.

- The Alberta College of Physicians and Surgeons has recently published a paper on data stewardship and information sharing agreements. Newfoundland provided some

general agreement examples and Yukon provided specific examples as well. Interviews in BC provided background and context. In addition the BC Government CIO's office is currently working on process and methodology for managing information sharing agreements.

- Canada has formally adopted ISO 22857:2004 Guidelines on data protection to facilitate Transborder flows of personal health information[3]. The standard outlines principles for adequacy of data protection, describes context and sets the stage for international data sharing activities. It describes Principles (Why), Stipulations (What) and Measures (How). (An information sharing agreement is an example of a Measure[4].) Because the standard must be principles-based and usable by many countries it does not make reference to specific legislation. Although the standard speaks about international transfer it can be applied in the domestic setting.

- In the European Union (EU) a large-scale EHR interoperability project[5] known as epSOS (European Patients Smart Open Services) is underway. The project is a large scale Europe-wide pilot of patient summary and electronic prescription information, organized by twelve EU member states including ministries of health, national competence centres and numerous companies, clustered in practical cooperation. The overarching goal is to develop a practical eHealth framework and ITC infrastructure to enable secure access to patient information between different European healthcare systems. The project is facing similar, but even more difficult issues than is Canada's EHR due to the number of EU countries and their close proximity, which results in a large degree of patient mobility. Consequently the project has been designed to include legal analysis which follows the project design and implementation in order to drive out specific legal issues. Project representatives have stated that it is obvious that Canada is facing similar challenges and that they feel international cooperation is important.

- Transfers of personal data outside EU borders may take place where the recipient country ensures an adequate level of protection in law. However an exemption

[2] In this case while the public body retains the right to audit financial records personal information does not fall under their control.
[3] The standard is based on consent which is not an absolute requirement under law in Canada
[4] The standard requires some updating to make it clear that some clauses are variable depending upon the laws of the jurisdiction in which it is used, and compensating controls which may be added to increase protection where certain clauses cannot be applied, as well as consideration of cultural differences.
[5] http://www.epsos.eu/

authorizes transfer to a 'non-adequate' country if there are adequate privacy protection safeguards in contracts.

- The starting point for assessing adequacy includes a series of basic data protection principles set out below, together with the three further requirements: 1) that in practice there is a good level of compliance with the principles, 2) that support and help are available to individuals in the exercise of their rights, and 3) that a means of redress is available in the event of non-compliance. The principles are: (It is valuable to note that the principles are applied in the EU/USA Safe Harbour framework)

  1. purpose limitation;
  2. data quality and proportionality - data should be accurate and up to date, adequate, relevant and not excessive in relation to the purposes;
  3. transparency - individuals should be provided with information as to the purpose of the processing[6] and other information insofar as this is necessary to ensure fairness;
  4. security - technical and organisational security measures must apply;
  5. rights of access, rectification and opposition accrue to the data subject; and
  6. restrictions are placed on onward transfers.

  In some situations additional principles must be applied:

  1. sensitive data - where 'sensitive' categories of data are involved, additional safeguards should be in place;
  2. direct marketing - for direct marketing, the data subject should be able to 'opt-out';
  3. automated individual decision – in the case where an automated decision is made about a person, the individual should have the right to know the logic involved in this decision; and
  4. other measures should be taken to safeguard the individual's legitimate interest.

- In the EU environment while agreements may vary in detail and formality, parties are required to implement privacy and security measures commensurate with the nature

[6] Processing means any operation which is performed on personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use disclosure, dissemination, alignment or combination, blocking, erasure or destruction.

of the work, the amount and sensitivity of the information, and the number and nature of individuals who have access to it.

Observation #5: ***There is considerable work underway in Canada and elsewhere on agreements to control disclosure of data across borders.***

Observation #6: ***In addition to a suitably relevant title, names of the parties and signing pages, the following is a list of subject headings that templates set out by ISO, the EU, COACH and others suggest should be included.***

1. Facts about the business environment:
    a. the purpose of the agreement;
    b. authority for the agreement
    c. authority for the disclosure and subsequent data collection;
    d. a general description of the nature of the data to which the agreement applies, or detailed descriptions as required by the nature of the data and the setting;
    e. the purposes for which the data are processed, including descriptions of secondary uses;
    f. the transfers that are covered by the agreement both inside and outside of Canada;
    g. if there are any onward transfers authorized or prohibited, including ad-hoc transfer;
    h. governing law and a dispute forum[7];
    i. an accountable person or body, data steward or data custodian;
    j. independent authority or data stewardship group for decision making;
    k. clear separation of stewardship from operations, in order to reduce conflict of interest;
    l. provisions of other agreements to be respected; and
    m. liability
2. Controls[8] to which the data is subject including:

[7] When considering a liability regime it is important that individuals are provided with means to exercise their rights and receive appropriate compensation. A process and principle to this effect is needed.

a. fair information management principles, transparency and fairness to data subjects;

b. individual rights of access, rectification and objection to processing (as applicable);

c. ensuring data quality – accuracy, integrity and timeliness of data;

d. consent requirements or requirements for notice;

e. privacy policies and procedures that describe how the organization adheres to each fair information practice, and mechanisms for review and update;

f. retention schedules and disposal procedures based on business purposes;

g. a security program including physical, technical and administrative measures;

h. access control procedures – identification, authentication and authorization;

i. requirements for a Security Threat and Risk Assessment;

j. secure transfer procedures;

k. human resources policies including clearly defined roles and responsibilities, appointed contact persons for privacy and security standards, professional standards, confidentiality agreements and disciplinary procedures;

l. ongoing privacy and security education and training programs;

m. control over third party agreements;

n. designated responsibility for internal and/or external privacy audits;

o. privacy and security crisis management protocols;

p. data linkage protocols;

q. procedures or standards for de-identifying data;

r. requirements for inventories of data holdings of personal health information with the relevant characteristics of the data and possible transfers in an accurate, specific and comprehensive manner;

s. protocols for reviewing proposals in terms of their privacy impacts;

t. requirement for, and management, of audit trails including the right to examine audit logs should be included;

u. disaster recovery plans;

[8] Security control mechanisms should be specified at a technology neutral level to allow for variations in implementation and future technological improvements.

v. standards to be applied, mandated or suggested;

w. references to risk management programs, structures and concepts;

x. mechanisms for reporting and recording changes, including processes for informing other parts of the organisation of changes to the rules;

y. right to ask for relevant policies;

z. communication materials related to privacy such as brochures available to the public; and

aa. monitoring, enforcement and evidence of application of the rules in general.

3. Process requirements which affect the life and content of the agreement:

    a. reference to a program of services;

    b. program changes which trigger agreement review;

    c. other triggers and process for review;

    d. term of the agreement;

    e. agreement oversight process and redress, and

    f. reference to supporting documentation: Program Charters, PIAs, STRAs, SLAs and policy.

Approach to Agreements

A number of characteristics were identified in the review which were key to the success of both the process of creating an agreement, and the implementation of the agreement itself:

1. Clarify and document the reasons for the agreement: identify and communicate the basis for the initiative or program and the basic rules, business requirements and assumptions related to data sharing. The business of healthcare is complex, with many players and perspectives. However, to create an adequate agreement all of these perspectives must be considered. It is important to understand the rationale for the initiative, its objectives, and business requirements which the agreement will control, before beginning to draft the details.

    For example, one jurisdiction characterised their success as being due to the fact that key project people responded to questions raised by the Conceptual PIA thus using

the Conceptual PIA as an input to design. The questions raised required responses to privacy issues as well as business and technological issues, and so created a convergence of interests where each learned from the others.

2. Decide how to apply the law: Organizations must decide if they are going to take the approach of allowing all disclosures which are not *specifically prohibited*, or whether they will only allow disclosures which are *specifically authorized*. When a public body is either a source or recipient of personal health information, privacy legislation, health information legislation and other law applies to its collection, use and disclosure. An agreement can enable information sharing which might otherwise require authorization for each disclosure. Agreements set out the arrangement to ensure disclosures don't contravene law and to formalize the control mechanisms.

3. Decide who has control responsibilities for the disclosed data: two models are available for control of data once disclosed:

    a. The disclosing party may by virtue of the agreement retain control of the disclosed copy of the data and thus its permitted uses, and responsibility for its protection, or

    b. the disclosing party may transfer control of the disclosed copy of the data to the recipient who must have the authority to collect it and who then becomes the trustee or custodian, allowing their legislative and ethical responsibilities to apply.

    In the case where a disclosing party transfers control of the data copy to the recipient, the disclosing party has a basic ethical and sometimes legal, requirement to ensure that the transfer is done securely, with appropriate authority, and that the data is required for the business purposes of the collecting party. Providing more or different data than the receiver requires creates a privacy risk, and in some cases, a legal risk for both parties. In either case there remains a requirement for both parties to have in place a structure to investigate and rectify security breaches and to adapt their arrangements and agreements to reduce recurrence of similar incidents.

4. Comply with applicable law: Jurisdictions cannot agree to be bound by rules that differ from their legislation nor can the legislative requirements of one jurisdiction apply to another; however agreements can be used to limit collection, use and

disclosure beyond what is required in legislation. For example, BC law explicitly prohibits disclosure of personal information outside Canada, without consent of the individual, except in specific circumstances. This prohibition does not exist in many other Canadian jurisdictions but the requirement must be met in support, outsourcing or other contracts. It is required by BC law that the recipient agree to notify the BC public body discloser of any foreign demands for the data. Although this can mean significant change to the recipient's processes, privacy schedules which meet this requirement have been successfully negotiated in vendor agreements. This would likely require greater flexibility in negotiation where the parties to the agreement are equal bodies with differing legal requirements.

5. Consider Risk: Information Sharing Agreements must be designed to address the full spectrum of risks: legal, financial, public relations, patient safety, privacy, security – they must all be taken together to define the composite risk of the initiative or program. The parties to the agreement must determine their acceptable level of risk within the whole of the business environment. The rights and expectations of the data subject are also considered but done so within the context of all the business risks. Based on the review it was clear that bringing together different perspectives was key to success. There is never a complete absence of risk and focussing on one risk area to the detriment of others does not lead to a balanced agreement and can lengthen the negotiation process. Privacy experts focus on sound ethical and legal principles. Computer scientists focus on technology mechanisms to implement policy and policy specialists focus on overall business objectives, without which it is difficult to know what technology is necessary. The most successful initiatives combine these and other perspectives into a set of business requirements in order to create an effective agreement.

   Privacy Analytics has recently created a tool that considers the spectrum of risks associated with disclosure of large data sets. This work has blended the activities of risk assessment with the creation of controls over disclosed data. The agreement created by the tool considers all of the risk variables as well as conditions related to the security and privacy practices of the collecting party.

Observation #7: ***In the EHR context with the potential for higher volumes of data disclosure, in the absence of an agreement there is a higher risk of***

misunderstanding, misinterpretation, accidental or inappropriate disclosures and disputes.

6. Agree on and Maintain Consistent ISA Content: Individual parties will typically negotiate the content of an agreement. Partners in an exchange can agree on aspects that concern them exclusively but there may be a need for nationally agreed principles to address recurring aspects and common cross-border interoperability issues.

7. Organizational Culture: Entirely new programs or new ways of doing business may require time in order to understand their potential impact. For example, in the European Union issues are often addressed from the top down in a formal manner, and work on formal data protection for trans-border data flow has been going on for some time. Where that has occurred too quickly the proposed technical solutions have sometimes been misunderstood from a social perspective. The degree of authoritativeness, complexity, formalism, detail and openness relates to the parties' cultural approach to risk. For example, some time back the Ontario Information Privacy Commissioner identified some of the common elements of data sharing success stories. One of the most striking was the importance of a "positive access mind-set" or a "corporate-wide attitude of openness". A characteristic of success was leadership that endorses positive and active ways to communicate and meet objectives and the necessary staff to develop and implement strategies.

8. Communication and collaboration: Increased collaboration and data integration requires communication between the administrations involved. Although jurisdictions are responsible for the interoperability of their own systems, program interoperability is needed in order to meet common priorities and implement common solutions. Organizational processes supporting the iEHR require agreement on how to structure interactions and define the "business interfaces". An approach which demands that the highest standard among the parties be met by all, is not likely to be considered reasonable by all parties. The *ep*SOS project has taken the approach of identifying the minimum requirements for safe legal trans-border disclosure and is moving forward from there.

9. Consistency in Terminology: In standards, policies, legislation and other human communication using the same term to mean the same thing is key. In all sample

agreements, definitions play a major role. Semantic interoperability means ensuring that the meaning of information is not lost in the exchange, that it is retained and understood by people, applications and institutions. Semantic consistency can support communication.

Structure of the Agreements

The review also revealed situations where a hierarchy of tools were employed. In one instance a Program Charter was first written to set out the basic business requirements and assumptions of the program or initiative. This document provided the foundation information and business requirements for the ISAs and allowed the parties to understand the initiative which the agreement was to control. This allowed the agreement specifically describing data protection, i.e. the ISA, to rely upon the Program Charter to describe the business context within which to interpret its rules. The most basic of these rules and assumptions were translated into the 'whereas' statements found at the beginning of the ISA, sometimes referred to as recitals.

This is analogous to the case for complex health services delivery programs where a program charter is written to set the program context for which the information sharing is required. The Program Charter describes the business objectives, program and legal authority, information required and the principles and governing structure under which the program, and thus the information collection, use and disclosure operates. When designed this way the ISA fits into a framework of law, context documents, and policy and is a tool which gives effect to the business and legal requirements described in the Program Charter. The ISA becomes a control mechanism supporting risk assessments such as Privacy Impact Assessments and Security Threat and Risk Assessments.

Expanding upon this approach, a set of 'agreement' documents each with its own special purpose may be employed: 1) a program description or charter, 2) a general contract, 3) a Services Level Agreement (SLA), and 4) an ISA, as well as separate schedules for description of data elements and applicable policies, thus providing an environment in which changes can be made Once the basic clauses or requirements of an agreement have been identified and agreed to, the degree of formality and detail used in their construction can vary.

On-going work: Enforcement & Agreement Maintenance

Once agreements are in place they must be updated regularly to maintain their applicability and compliance with law. This is typically a process and governance issue which can be important to the operation of the program or initiative.

Summary

In all a few common themes were identified:

- It has been suggested a shift is coming in the need for legal tools and a more structured approach to manage the risk associated with information disclosure. As jurisdictions must assure themselves that other jurisdictions conform to functional requirements it may become important that certification statements relating to systems, organizations and people are included in agreements.

- Based on comments made by EU sources it has been suggested that more functional control will be demanded of the technology. However until that is the case, as long as controls must be applied by administrative means, tools such as information sharing agreements will remain important.

- As well as the necessity for common terms and principles, another common theme is the value of communication and the importance of including a broad group of stakeholders to combine the risk assessment perspective each brings to the table.

- The importance of context documentation including descriptions of principles and agreed approach was a key element of success.

Approaches and steps which may be considered include:

- *It is helpful to have the policy and business stakeholders agree on their common basic values, general approach to privacy protection and legal issues before engaging legal experts to write detailed agreements.*

- *It is important for the parties to decide if they are going to take the approach of allowing all disclosures which are not specifically prohibited, or whether they will only allow disclosures which are specifically authorized.*

- *A multi-perspective, top down approach including business, legal, ethical, technical, people and process requirements can help ensure that gaps in an agreement do not create opportunities for risk, by agreeing and documenting the business initiative, its goals and objectives, its program of services and the data needed for service delivery and the data protection controls.*

- *Awareness of and adherence to commonly agreed guidelines, whether written by the business and policy stakeholders or adapted or adopted from other sources, can support more effective business interoperability.*

- *Using simple language and consistent terminology will make agreements effective and easier to understand.*

Samples

The objective was to create a report with examples of agreements and related instruments in order to better understand the types and features of agreements and the attributes of successful implementation. However at this time it is difficult to provide specific examples because of the lack of implemented agreements dealing with trans-border data flow. Consequently the samples provided are not a comprehensive set, nor are they chosen based on what might be considered 'best practice'. Rather they reflect what was made available and represent different approaches based on different business context and data purpose. Neither the EHR nor the iEHR is specifically reflected in the samples although in some the iEHR characteristics of the disclosure include ongoing, open access rather than one-time disclosures.

- TBS tools apply to a wide range of jurisdictions and may include approaches which could be reused.

- The BC Government CIO's office is currently working on a process and methodology for managing information sharing agreements. That work could be examined for its adaptive possibilities.

- The Public Health Agency of Canada will require agreements and processes for Panorama. The existing structure of trusted bodies may be considered for steering and operating committees.

The Canadian standard on trans-border data flow may be helpful in forming a foundation of principles, scope and depth of detail. Clauses to uphold legislative requirements can be negotiated.

Samples templates include:

1. A generic template which includes basic requirements
2. An example of a specific privacy and security schedule for attachment to a contract
3. An example specifically tailored for disclosure of data for research
4. An example which is tailored to outsourcing of data processing
5. An 'lighter' ISA example for sharing within a trusted group
6. An example based on ISO 22857:2004 *Guidelines on data protection to facilitate Transborder flows of personal health information* ***Note:** the international standard which this standard is based upon is strongly consent driven. Where those same consent requirements are not required in Canadian jurisdictions an analogous reference to notification requirements can be substituted.

For all samples see Appendix B.