Best Practices for Information Management Agreements

Section 22 of the *Personal Health Information Act* ("*PHIA*") requires custodians to enter into a written agreement with all information managers they retain. In turn, an information manager must comply with *PHIA* and the terms of the agreement in respect of the personal health information disclosed to it, including only using and disclosing information as authorized by the agreement. These agreements are commonly referred to as information management agreements ("IMAs").

Section 22 of *PHIA* states:

> *22.(1) A custodian that retains the services of an information manager for the provision of a service described in paragraph 2(1)(l) shall enter into an agreement with the information manager in accordance with subsection (2).*
>
> *(2) An agreement referred to in subsection (1) shall be in writing and shall provide for the protection of the personal health information against unauthorized access, use, disclosure, disposition, loss or modification in accordance with this Act and the regulations.*
>
> *(3) An information manager to which personal health information is disclosed by the custodian may use or disclose that information only for the purpose authorized by the agreement.*
>
> *(4) An information manager shall comply with:*
>
> *(a) this Act and the regulations; and*
>
> *(b) the terms of the agreement entered into with the custodian in respect of the personal health information disclosed to it under subsection (2).*
>
> *(5) An information manager shall not permit its employee or a person acting on its behalf to access the personal health information disclosed to it by the custodian unless the employee or person acting on its behalf agrees in writing to comply with this Act and the restrictions imposed upon the information manager referred to in subsection (4).*
>
> *(6) Nothing in subsection (4) or (5) relieves a custodian from its obligations under this Act and the regulations in respect of the personal health information disclosed by the custodian to the information manager, and the personal health information that has been disclosed to an information manager under an agreement under subsection (2) is considered to continue in the custody and control of the custodian for the purpose of this Act and the regulations.*

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

> *(7) An information manager may, in accordance with the terms of an agreement with a custodian, construct or create an integrated electronic record of personal health information comprising individual records, the custody or control of each of which may be in one or more custodians.*

Information Manager

An information manager is any third party that deals with a custodian's personal health information on behalf of that custodian in accordance with the following definition of "information manager" in section 2(1)(l) of *PHIA*:

> *a person or body, other than an employee of a custodian acting in the course of his or her employment, that:*
>
> *(i) processes, retrieves, stores or disposes of personal health information for a custodian, or*
>
> *(ii) provides information management or information technology services to a custodian.*

Examples of information managers include: an entity providing information technology services (i.e. software vendors or developers); an entity providing information management services; data storage service providers; and data destruction service providers.

Custodian Retains Obligations under *PHIA*

IMAs do not relieve custodians of their legal responsibilities and obligations under *PHIA.* While a custodian may include terms within an IMA that relate to its own obligations, for example terms requiring an information manager to adhere to certain security measures, this does not relieve the custodian from its compliance with *PHIA*. In our example, this means the custodian remains legally responsible for ensuring there are reasonable security measures in place to protect information and, therefore, a custodian will want to ensure its due diligence when selecting a service provider. It must also be remembered that personal health information handled by the information manager on behalf of the custodian is ultimately the responsibility of the custodian.

IMAs

There is no template in *PHIA* for an IMA, as each agreement will be specific to the custodian and information manager involved for the services provided. An IMA will outline the terms and conditions under which personal health information is shared between the parties and the protection of the personal health information involved by ensuring compliance with *PHIA*. When retaining an information manager, the custodian should consider the practices outlined below in creating the necessary IMA. An agreement between a custodian and information manager can be included in a broader contractual agreement as long as it includes the elements required in *PHIA* and discussed below.

Step 1: Justification

Custodians must weigh the benefits of retaining an information manager against the possible risks and consequences. Some examples of when an information manager could be used are:

- custodians using a billing service or transcription service;
- custodians using a storage service for electronic or paper records;
- custodians using an IT service provider/company; and
- custodians who use an electronic medical records service.

In making a decision to use an information manager, custodians should determine whether it is possible for the custodian to perform the services itself and, if it is not possible, a written justification should be documented (see Step 3 – Document).

Step 2: Determine Risks & Assess Impact on Privacy

Prior to drafting an IMA, a custodian must consider the risks presented by the disclosure of personal health information to the information manager. To properly identify and consider these risks, custodians should consult with their legal and privacy experts. These consultations should consider:

- the purpose of the information management agreement (i.e., what specific tasks are intended to be performed in relation to the information);
- the personal health information to be shared with the information manager, including its sensitivity, and whether it is the minimum amount of personal health information necessary;
- the necessary security measures needed to safeguard the personal health information against unauthorized access, use, disclosure, disposition, loss or modification, in accordance with the requirements of *PHIA*;
- the permitted uses and disclosures by the information manager with respect to the personal health information that are necessary for the performance of the service that is the subject of the agreement;
- the extent of the disclosure (who exactly within the information manager organization needs access to the personal health information being disclosed?);
- the location of the information after being shared: Will it be in a cloud? On a local server? Alternatively, is the information being retained at the custodian's facilities with the information manager attending?

Once the risks have been identified, the custodian should take a detailed look at the recommended privacy tools that assist in mitigating these risks including:

- conducting a Privacy Impact Assessment ("PIA");
- the possibility of using test data prior to the disclosure of personal health information; or
- consultations with a privacy, security or legal expert; the Department of Health and Community Services or OIPC.

The use of these tools may be dictated by the financial and technical constraints of the custodian. Each custodian will have to evaluate their particular circumstances to determine which of the tools is practicable.

Step 3: Document

It is best practice to document a decision to proceed with an IMA. Documentation should include, but not be limited to, the justification for the retention of an information manager, information management policies and procedures, a risk mitigation plan, and a Privacy Impact Assessment.

Step 4: Create an IMA

To the extent possible, the agreement should be specific, precise, and written in plain language to ensure that all terms are fully understood. It should also be flexible enough to allow for amendments and, where possible, the IMA should be available to patients or clients for greater transparency.

Agreements should include these key components:

- the purpose of the IMA;
- that the agreement will be governed by *PHIA*;
- details of the service offering;
- the identification of parties, including their roles and responsibilities and the fact that the custodian retains custody and control of the information;
- that the information manager must comply with *PHIA*, *PHIA*'s regulations and the IMA;
- that the information manager may only use or disclose the personal health information that is subject to the agreement as directed or authorized by the IMA;
- the timeframe of the agreement (start and end date);
- a statement that the meaning of terms used in the agreement, such as "personal health information", "information manager", or "custodian" are as found in *PHIA*;
- the identification of the specific information to which the IMA will apply;
- the identification of who will have access to the information, including how and under what conditions they will access the information;
- the legal authority to disclose and collect information, including reference to all applicable legislation;
- hardware and software requirements for both the custodian and the information manager;
- the process for compliance monitoring, including the ability to audit the information manager;

- the method for transferring the information, including the security measures used in the transfer which must be in line with section 15 of *PHIA*;
- provisions for accuracy and integrity of the information and a description of the process for ensuring same;
- the required security measures and safeguards for storing the information. Section 22(2) of *PHIA* states that the IMA shall provide for the protection of the personal health information against unauthorized access, use, disclosure, disposition, loss or modification;
- a description of the process for managing and reporting privacy breaches, complaints, and incidents that occur while the information manager is using or disclosing the personal health information subject to the IMA;
- retention periods;
- the method of secure destruction when the retention period expires;
- termination of the agreement procedures, including any costs affiliated with returning the information to the custodian or transferring to another information manager and documentation confirming all copies have been destroyed; and
- signatures and signing dates.

Step 5: Monitor and Follow Up

It is best practice to monitor the effectiveness of the agreement. This may be done through audit trails, self-assessments, verification systems, certificates of assurance or other techniques arranged by and acceptable to the custodian and the information manager related to the obligations in the agreement.

The Department of Health and Community Services *PHIA* Policy Development Manual also contains guidance on the development of IMAs and should be consulted by custodians seeking to create an IMA.

Note:

It is important to note that information management agreements (IMAs) are different and distinct from information sharing agreements (ISAs) in content and in purpose. Under an information management agreement, the information manager handles a custodian's data on behalf of the custodian for the custodian's purpose. In contrast, in an information sharing agreement, the information is disclosed by the custodian to another party for the receiving party's purpose.