Understanding the Legal Framework for HIFIS 4

One of the most important pre-requisites with using a shared information system is setting up the proper legal framework. While legislation and requirements are different in every province/territory, and different legal experts may have different opinions on what is required to ensure that all the bases are covered, this document should give you a pretty good overview as to what is needed.

Mandatory Agreements

Data Provision Agreement (DPA)

The entity that is overseeing the installation, hosting, and maintenance of HIFIS 4 (the Site Coordinator) must sign a legal agreement between this entity and the federal government. The entity may be the Service Manager, the Community Advisory Board (CAB), the Community Entity (CE), the municipal, county, or regional government, or a single service provider. At a very high level, this agreement states that the entity has permission to use the software, and in exchange, they will export limited, anonymous data for the federal government to use.

Data Sharing Agreement (DSA)

In addition to the DPA, if multiple organizations will be using HIFIS 4 and will be sharing data between these agencies regarding mutual clients, legal agreements must be made between participating organizations. These are referred to as Data Sharing Agreements and at a high level, outline what information will be shared and how it will be used. In most cases, Data Sharing Agreements also outline the responsibilities of the various parties involved.

Note: A Privacy Impact Assessment may also be required.

Consent Form

Any agency that is collecting personal or health information about clients must obtain informed consent from the client prior to doing so. In addition, when using a shared data system such as HIFIS 4, the client must consent to sharing their information with other agencies with whom Data Sharing Agreements are signed. Most communities adopt a new, system-wide consent form when beginning to use HIFIS 4 that states explicitly that personal information will be shared with other service providers.

Note: A Privacy Impact Assessment may also be required.

End User License Agreement (EULA)

An End User License Agreement (EULA) is an agreement made between a software developer and the user of that software. At a high level, a EULA states that the user will not try to illegally plagiarize the software itself and try to sell it, nor will the user try to sue the software developer if it doesn't work properly. All HIFIS users (staff or volunteers who have the ability to log in to HIFIS) will have to agree to the EULA before beginning to use HIFIS.

PRIVACY IMPACT ASSESSMENTS

"What are Privacy Impact Assessments?

Privacy Impact Assessments (PIAs) are used to identify the potential privacy risks of new or redesigned federal government programs or services. They also help eliminate or reduce those risks to an acceptable level.

Virtually all government institutions, as defined in section 3 of the *Privacy Act*, including parent Crown corporations and any wholly owned subsidiary of these corporations, must conduct PIAs for new or redesigned programs and services that raise privacy issues.

PIAs take a close look at how government departments protect personal information as it is collected, used, disclosed, stored and ultimately destroyed. These assessments help create a privacy-sensitive culture in government departments.

When is a PIA required?

Under the Treasury Board of Canada Secretariat's (TBS) *Directive on Privacy Impact Assessment* (effective April 1, 2010) government departments must conduct a PIA in a manner that is commensurate with the level of privacy risk identified, before establishing any new or substantially modified program or activity involving personal information.

Specifically, a PIA is generally required when a government department:

- Uses or intends to use personal information in a decision-making process that directly affects an individual;
- Substantially modifies existing programs or activities where personal information is being used, or intended to be used, in a decision-making process that directly affects an individual;
- Contracts out or transfers a program or service to another level of government or the private sector resulting in substantial modifications to a program or activity;
- Substantially redesigns the system that delivers a program to the public, or;
- Collects personal information which will not be used in decision-making process that directly affect an individual but which will have an impact on privacy."

Source: Office of the Privacy Commissioner of Canada

Optional Agreements

The following are not strictly necessary, but many communities find them advantageous to have.

Service Level Agreement (SLA)

A Service Level Agreement is made between the entity that is hosting HIFIS (the site coordinator) and all other service providers. This two-way agreement lays out the responsibilities of each party in the context of using HIFIS.

- The site coordinator promises to do their best to make sure HIFIS is running efficiently
- Service providers promise to follow policies and procedures laid out by the site coordinator

Since SLAs are not used in all communities, there is more flexibility as to its contents. Typical topics included are:

- Costs, who pays for the server
- What happens if the server experiences an outage
- Procedure for performing maintenance on the server

Oath of Confidentiality

Communities may require staff and volunteers to sign or pledge an Oath of Confidentiality. At a high level, the Oath of Confidentiality states that the person agrees not to share any information about any client that they learn about through their work.

An Oath of Confidentiality may be included as part of the Rules of Behaviour or HIFIS Use Protocols.

HIFIS Use Protocols

Various protocols surrounding the use of HIFIS are often laid out by site coordinators, particularly when there are multiple agencies involved. These protocols might cover topics such as:

- Data standards, such as mandatory data elements, entry format, accuracy, and timeliness of data entry
- Handling data access requests
- What to do if there is a data breach
- Policies on client consent
- Who trains staff, and how much training is required
- Policies on auditing and data integrity checks
- How protocols will be enforced

Rules of Behaviour (ROB)

Communities may require HIFIS users (staff or volunteers who have the ability to log in to HIFIS) to agree to particular rules surrounding HIFIS 4 use. These rules often govern things like:

- Not sharing passwords
- Using secure passwords
- Logging out when away from a computer screen
- Not accessing HIFIS over unsecured networks
- Not accessing information without authorization
- Reporting data breaches immediately

Who Signs What?

Document	Agreed to by
Data Provision Agreement	Government of Canada + Site Coordinator
Data Sharing Agreement	Site Coordinator + Service Providers
Privacy Impact Assessment	n/a
Service Level Agreement	Site Coordinator + Service Providers
HIFIS Use Protocols	Site Coordinator + Service Providers + HIFIS Users
Consent Form	Clients
End User License Agreement	HIFIS Users
Oath of Confidentiality	HIFIS Users
Rules of Behaviour	HIFIS Users

Who Develops What?

Document	Developed by
Data Provision Agreement	Government of Canada
Data Sharing Agreement	Site Coordinator
Privacy Impact Assessment	Site Coordinator
Service Level Agreement	Site Coordinator
HIFIS Use Protocols	Site Coordinator
Consent Form	Site Coordinator
End User License Agreement	Government of Canada
Oath of Confidentiality	Site Coordinator
Rules of Behaviour	Site Coordinator

Pre-Launch Checklist

- ☐ Sign Data Provision Agreement
- ☐ If necessary: conduct Privacy Impact Assessment
- ☐ Develop Data Sharing Agreement
  - ☐ Get Data Sharing Agreement signed by all participating service providers
- ☐ Develop Service Level Agreement
  - ☐ Get Service Level Agreement signed by all participating service providers
- ☐ Develop Consent Form
  - ☐ Get Consent Form signed by all clients who will be entered into HIFIS 4 as of launch date
- ☐ Optional: Develop HIFIS Use Protocols
  - ☐ Communicate HIFIS Use Protocols to all participating service providers and their staff
- ☐ Optional: Develop Oath of Confidentiality
  - ☐ Get Oath of Confidentiality signed by all staff who will be using HIFIS 4 as of launch date
- ☐ Optional: Develop Rules of Behaviour
  - ☐ Get Rules of Behaviour signed by all staff who will be using HIFIS 4 as of launch date

Ongoing Checklist

- ☐ Monitor and enforce HIFIS Use Protocols
- ☐ Get Consent Form signed by all clients prior to entering them into HIFIS
- ☐ Get Oath of Confidentiality signed by all HIFIS users prior to account creation
- ☐ Get Rules of Behaviour signed by all HIFIS users prior to account creation