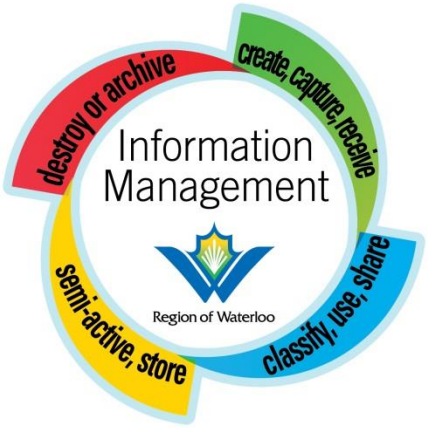


HIFIS 4 – Homeless Individuals and Families Information System

Privacy Impact Assessment

Prepared by: Brennan Hardy
Version: 1
Date: October 19, 2018

Document History

Version	Date	Author(s)	Description of Changes
V1	2018/03/21	Brennan Hardy	First Draft
V2	2018/07/27	Tracy Verhoeve	Housing Services review
V3	2018/08/08	David Thompson	ITS additions
V4	2018/09/14	Brennan Hardy	Review post Housing and ITS revisions
V5	To come		FINAL

Document Approval

Name	Title	Signature	Date
Oriana Sharp	Manager, Information Management & Archives		
Angela Pye	Manager, Housing Policy and Homelessness Prevention, Housing Services		
Tracy Verhoeve	Social Planning Associate, Housing Services		

Table of Contents

Document History ii

Document Approval ii

1. Executive Summary 5

Acronyms 6

2. Introduction 7

2.1 Background 7

2.2 PIA Purpose 8

2.3 PIA Scope 8

2.3.1 In Scope 8

2.3.2 Out-of-Scope 8

2.4 Assumptions and Limitations 9

2.5 Stakeholders 9

2.6 Methodology 9

2.6.1 The Objective of a PIA 9

3. Legislative Overview 10

4. Contractual Overview 10

5. HIFIS 12

5.1. Description of HIFIS Information Lifecycle 12

5.2. HIFIS Business Processes and Data Flows ..... **Error! Bookmark not defined.**

5.3. HIFIS Privacy Risk Assessment 23

Definition of Impact Rating 23

Definition of Likelihood Rating 23

Risk Rating Reference Table 24

Principle 1 – Accountability 14

Principle 2 – Identifying Purposes 20
Principle 3 – Consent 23
Principle 4 – Limiting Collection 27
Principle 5 – Limiting Use, Disclosure, and Retention 28
Principle 6 – Accuracy 30
Principle 7 – Safeguards 32
Principle 8 – Openness 35
Principle 9 – Individual Access 38
Principal 10 – Challenging Compliance 41
6. Conclusion 52
Appendix A: Documentation Reviewed for this PIA 53
Appendix B: Interviews Conducted for this PIA 54
Appendix C: HIFIS PIA Interview Questionnaire 55
Appendix D: HIFIS Users 62
Appendix E: Current HIFIS Retention Practices for PI 67

List of Tables

Table 1: HIFIS Stakeholders and their Roles 15
Table 2: Data Flow #1 .....
Table 3: Data Flow #2 .....
Table 4: Data Flow #3 .....

List of Figures

Figure 1: HIFIS Data Flow Chart 22

1. Executive Summary

Housing Services is in the process of implementing version four (4) of the Homeless Individuals and Families Information System (HIFIS), a program that helps service providers and their funders manage information about various types of housing services (e.g., emergency shelters, supportive housing).

The system vendor for HIFIS is the Federal government of Canada, specifically Employment and Social Development Canada (ESDC). ESDC developed the HIFIS software and owns all right, title and interest in the software. ESDC releases the software and provides on-going technical and training support at no charge to the Service Manager and provider agencies. The Region is considered to be the Application Host which refers to the entity that owns and houses the equipment on which the HIFIS application and data reside.

HIFIS 4 will replace HIFIS 3 which is currently in use by twenty local service providers in Waterloo Region. These service providers have HIFIS 3 installed at their agencies (on their servers) and data is inputted directly into the software by their staff. Service Providers run their own reports using HIFIS 3 and submit reports to the Region on a regular basis (monthly, quarterly and annually). The most current version, HIFIS 4, is web-based and will allow sharing of information across agencies. Some of the benefits to this version include:

- Better customer service for clients as they won't have to share their story multiple times
- Increases in the amount of time that service providers can spend supporting clients (high-value activities) by lowering administrative burden (e.g., time spent on manual reporting)
- Strengthens the ability to do shared service planning across agencies funded by the Region
- Gives the Region access to real-time data to monitor collective impact across the entire housing stability system

HIFIS 4 will require migration of client data from the HIFIS 3 databases of participating service providers to the central HIFIS 4 web-based program hosted by the Region and will allow for the use and disclosure of an increased amount of personal information (PI). When a program adopts a new electronic management system that involves PI a privacy impact assessment (PIA) is required to help identify and mitigate any new risks for non-compliance with privacy laws and best practices created by this change. Where risks are identified in the PIA, recommendations will be made to help mitigate those risks.

A total of 30 privacy risks have been identified in this PIA. Each risk is accompanied by a recommendation. The assessment begins on page 14 of this PIA. Housing Services has already recognized some of the risks identified in this PIA and has begun the work to implement the recommendations required to manage these risks.

Acronyms

Acronym	Definition
HIFIS	Homeless Individuals and Families Information System
ESDC	Employment and Social Development Canada
PI	Personal Information
IM&A	Information Management and Archives of the Council and Administrative Services Division, Planning, Development & Legislative Services Department operated by the Region of Waterloo
ITS	Information & Technology Services division of the Corporate Services Department operated by the Region of Waterloo
IPC	Information & Privacy Commissioner of Ontario
MFIPPA	Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56
PIA	Privacy Impact Assessment
TRA	Threat Risk Assessment
NHIS	National Homelessness Information System
ROW	Region of Waterloo
DPA	Data Provision Agreement
DSP	Data Sharing Protocol
EULA	End User License Agreement

2. Introduction

2.1 Background

Waterloo Regional Council approved the All Roads Lead to Home: The Homelessness to Housing Stability Strategy for Waterloo Region (2012) Policy Framework in March 2012 and corresponding Action Framework in November 2012. The Policy Framework was built upon:

- the housing stability framework introduced by the first Strategy (2007-2010);
- findings from a set of ten background reports released between 2008 and 2011; and
- thirty-two strategic plans or key initiatives from local organizations, groups and all orders of government.

The Strategy serves as the Region's system plan for housing stability and its implementation has been identified as an action in the Region's Corporate Strategic Plan. The Strategy is endorsed by twenty-nine organizations and groups within the region's local housing stability system. These stakeholders within the housing stability system provide broad expertise for strategy and system planning, implementation, monitoring and evaluation.

The Action Framework presents four focus areas, eight strategic directions and 40 actions towards the goal of reducing homelessness in Waterloo region. The Region holds a leading role in monitoring progress for the Strategy and serves as Service Manager for provincially funded homelessness and housing stability programs (e.g., Community Homelessness Prevention Initiative or CHPI). In doing so, Region staff consult monthly with the local Housing Stability System Planning Table.

Central to the Policy and Action Frameworks referred to above are the principles of:

- ongoing system monitoring and improvement,
- data-informed decision making, and
- the delivery of high quality services to those experiencing homelessness and those experiencing housing instability and are at-risk with the goal of ending homelessness.

As such, effective data management tools and practices have proven essential, particularly given the complexity of needs, barriers, and circumstances faced by many who access the housing stability system for assistance. For many years the Region of Waterloo, as Service Manager, has supported funded agencies in the housing stability system (namely Emergency Shelter and Supportive Housing providers) to collect and utilize client and service-delivery data by serving as local coordinator, lead, and access point for the Homelessness Individuals and Families Information System (HIFIS), a federally-developed and maintained data management system (through Employment and Social Development Canada, ESDC).

With previous and current versions of HIFIS, each applicable organization or agency has stored and operated the software within and from their own local server, with technical training and support provided from the Region in partnership with the federal agency who created the software. Local policies and procedures were developed by the Region in partnership with stakeholders to support agencies to collect data consistently and in compliance with relevant privacy legislation and, where data access was required by Region staff for quality monitoring and system planning, a data sharing protocol was employed.

There is now a new version of HIFIS (version 4) available for use within the housing stability sector, which departs from the previous versions insofar as it is web-based and can be modified to allow for shared access across organizations within a particular catchment. Given the goals and priorities set out in the aforementioned Strategy, a shared data management environment, which will allow for a more coordinated approach to service delivery, data monitoring and system improvements within Waterloo Region, is of great benefit. Personal information is also seen to be better protected under HIFIS 4 by providing centralized control of use across the system and use of standardized security principles and procedures. Service providers have a long history of sharing client information with other agencies, in accordance with the law. Since many of the clients served have complex and co-occurring disorders, client needs must be addressed by more than one service provider.

Region staff would like to work with the federal creators of HIFIS to bring version 4 to our community, and to roll out the software across an expanded group of funded housing stability programs and services (see full list of providers in Appendix B of the Preliminary Privacy Impact Assessment). The Region of Waterloo entered into a HIFIS Data Provision Agreement (DPA) with ESDC, granting the Region the rights to a registered copy of HIFIS. ESDC has developed the HIFIS software and owns all right, title and

interest in the software. ESDC releases the software and provides on-going technical and training support at no charge to the Service Manager and provider agencies. In turn ESDC requires that a Data Provision Agreement (DPA) be signed by the parties (ESDC and The Region of Waterloo) outlining roles and responsibilities including those related to privacy, security and data transfer of information. The DPA also identifies the non-identifying data to be exported to the National Homelessness Information System which is used to create a portrait of homelessness in Canada.

A HIFIS Data Sharing Protocol, HIFIS Data Entry and Administrator Guide, Data Quality Guide, Common Consent form and Security Protocol are all being developed to support the governance and guidelines for use of the system by both the Region and Service Providers.

The Region is considered to be the Application Host which refers to the entity that owns and houses the equipment on which the HIFIS application and data reside. The Region will create a backup copy of the data recorded in HIFIS on a nightly basis. The Region will create HIFIS User Templates based on defined Roles that are designed to give people in certain roles access to the information they need in HIFIS, but restricts access to information they don't need. All Users can see names and basic client information within HIFIS, therefore additional safeguards will be put in place to protect client's privacy.

The replacement of the existing HIFIS system involves the collection, use, disclosure and retention of an increased amount of personal information (PI). This privacy impact assessment (PIA) is required to make sure the use of HIFIS 4 is inline with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Housing Services Act, Personal Information Protection and Electronic Documents Act (PIPEDA) and the 10 Fair Information Privacy Principles outlined in the Canadian Standards Association's Model Code for the Protection of Personal Information.[1]

2.2 PIA Purpose

The purpose of this PIA is to identify the risks to the privacy of clients within the Housing Stability sector and the confidentiality and security of their PI that may result from Housing Services' implementation of HIFIS 4 and to provide recommendation on how these risks can be managed.

2.3 PIA Scope

2.3.1 In Scope

Included within the scope of this PIA is the analysis and risk identification of:

- HIFIS data flow;
- system technology requirements;
- system software;
- legislative analysis; and
- policies, procedures, governance of information, and technical services as they relate to HIFIS 4.

Phase 1 of this implementation with involve use of the following modules by Emergency Shelters (ES) and Transitional Housing (TH):

- Client Vitals/Information
- Admissions
- Assessments
- Service Restrictions
- Turn Aways
- Goods and Services
- Communications
- Reports

2.3.2 Out-of-Scope

The following matters are out-of-scope of this PIA:

- broadened scope of use by other external organizations;
- assessment of service providers/ stakeholders privacy practices and policies; and
- Threat Risk Assessment (TRA).

[1] CAN/CSA-Q830-96.

Updates to the existing HIFIS 4 PIA in the form of an addendum will be done in conjunction with implementation of additional phases of HIFIS 4, for example use of additional modules by additional service providers not covered in the initial scope of this PIA.

2.4 Assumptions and Limitations

In order for this PIA to be successful, IM&A assumed that:

- architecture exists for all applications;
- the necessary policy, procedure and governance documents exist to provide the appropriate controls over the process under assessment;
- all related documentation was provided as input to the PIA;
- key persons attended interviews as required by the agreed work plan; and
- appropriate members of Housing Services reviewed and commented on all draft documents.

2.5 Stakeholders

The table below describes the stakeholders and their roles in HIFIS 4:

Stakeholder	Description/Role	Access to HIFIS 4 data
Clients	Client PI is collected, used and disclosed in HIFIS 4. Clients are involved in the following data flows: • Service registration; • request for correction or updating PI; • request for security restrictions related to access to PI; and • complaints.	No (may request access to their own PI)
Housing Services	Authorized Housing Services staff are accountable for maintaining the privacy of clients within the Housing Stability sector, and the confidentiality and security of the PI that they access/ enter into HIFIS 4. User Templates based on defined Roles will be used within HIFIS 4 to limit the level of access to client PI. De-identified, aggregate data will be pulled from HIFIS 4 to inform housing planning.	Yes
Information Technology Services (ITS)	Authorized ITS staff will administer and maintain the HIFIS 4 infrastructure, network and hardware devices to ensure they are functioning properly.	Yes
Service Providers	Accurate and up-to-date collection, use and disclosure of client data as documented within the HIFIS 4 system for providing service and case management	Yes
ESDC	ESDC developed the HIFIS software and owns all right, title and interest in the software. ESDC releases the software and agrees to provide ongoing technical and training support at no charge to the Service Manager and the provider agencies.	Yes, however data is exported and reported to ESDC rather than accessed through HIFIS 4 (see Appendix A of DPA for required export fields)

Table 1: HIFIS 4 Stakeholders and their roles

2.6 Methodology

2.6.1 The Objective of a PIA

A PIA is a structured process which helps to determine if new or re-designed programs or services meet legislated privacy standards. The PIA examines proposed information handling processes and assesses them for technical compliance with privacy requirements. The PIA process is designed to ensure that privacy is considered throughout the project. The PIA is a living document that ensures:

- fair information practices are used in the handling of PI of clients;

- collection, use, disclosure, security, retention and disposal of PI complies with MFIPPA and other relevant laws;
- an increase in the efficiency of the program or service design by making sure that appropriate information handling methods are incorporated from the outset and not applied retroactively to completed processes;
- a reduction in the risk of mishandling PI, security breaches, and client complaints; and
- staff take more responsibility for applying privacy supportive practices in their activities.

The PIA was developed by reviewing documentation related to HIFIS 4, as well as conducting formal interviews and informal discussions with Housing Services and ITS staff. The documents reviewed and staff interviewed are listed in Appendices A and B respectively. A written questionnaire based on the 10 Fair Information Privacy Principles was used as the basis for obtaining necessary information. The questionnaire and the responses to the questions posed are included as Appendix C.

The PIA was conducted using an analytical framework based on the privacy requirements of MFIPPA, 10 Fair Information Privacy Principles, and best practices. According to the risk standard adopted by the Region, the target privacy risk level should be "no risk identified" to "low" to indicate that the potential exposure of an individual's PI to risk is kept to a minimum.

3. Legislative Overview

The authority for this initiative is derived from the Region's role as Service Manager as per the Housing Services Act, 2011 (2011, c. 6, Sched. 1, s. 11 (1).), and the requirement as Service Manager to develop a 10 year Housing and Homelessness Plan.

The authority is also derived more specifically in accordance with the provincial Community Homelessness Prevention Initiative and funding provided to Service Managers to develop local strategies for preventing and addressing homelessness - http://www.mah.gov.on.ca/Page9183.aspx

A Data Provision Agreement has been entered into by Region and Employment and Social Development Canada (ESDC).

The Region is subject to MFIPPA and subsection 28(2) states that an institution can only collect PI if:

- the collection is expressly authorized by statute;
- the PI is used for the purposes of law enforcement; or
- the collection is necessary to the proper administration of a lawfully authorized activity.

The authorities within the aforementioned Housing Services Act and provincial initiative confirm the permissions to move forward with this initiative.

Protecting personal information adheres to those Principles cited in Schedule 1 (Section 5) of the Personal Information Protection and Electronic Documents Act (PIPEDA). This is an Act to support and protect electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances.

The collection of PI in HIFIS is necessary for the proper administration of the housing stability system in Waterloo Region, a lawfully authorized function under the Housing Services Act and the Data Sharing Protocol includes a section that Service Providers must adhere to all applicable legislative authorities as defined.

4. Contractual Overview

Housing Services signed a Data Provision Agreement with ESDC to obtain a license to use the full version of HIFIS software and to facilitate its use by participating service providers. The purpose of the Agreement is to outline the terms and conditions related to the licence that ESDC will grant in return for certain non-identifiable Personal Information; and the collection and disclosure of Personal Information by the Region and participating Service Providers in such a manner as to protect the privacy and dignity of their clients. As background the agreement outlines:

- ESDC owns all right, title and interest in the HIFIS SOFTWARE and related Documentation and all of the files and intellectual property associated with it, including trade secrets and copyright;

- The Region wishes to obtain a licence to use the full version of the HIFIS SOFTWARE and ESDC is willing to grant such licence in return for non-identifiable personal information related to the Service Providers and their clientele ("Personal Information").
- The Region and participating Service Providers, are providing services to homeless individuals and families, and have the authority to collect, use and disclose personal information related to their clients;
- ESDC has the authority under the Department of Employment and Social Development Act (the "DESD Act") and the Privacy Act to collect the Personal Information for the administration of the Homelessness Partnering Strategy where the information will be used for the purpose of improving services to the homeless population, enhancing the Government of Canada's ability to respond to homelessness in Canada and policy analysis, research or evaluation purposes of policies and programs respecting homelessness in Canada.

Roles and Responsibilities:

The Region and participating service providers will:
a) collect the Personal Information using the HIFIS SOFTWARE, and ensure compliance with your applicable provincial or territorial legislative standards respecting personal information;
b) ensure that individuals are informed that their Personal Information will be provided to ESDC for the purposes of policy analysis, research and evaluation of policies and programs respecting homelessness in Canada;
c) designate a representative to review, verify and clean the Personal Information on a quarterly basis;
d) export the Personal Information listed in Appendix A to this Agreement quarterly to ESDC using the tools provided by ESDC;
e) use best efforts to ensure the completeness and accuracy of the Personal Information provided to ESDC;
f) create a back-up of electronic data on a regular basis, and store all Personal Information in a secure location; and
g) maintain the security of the Personal Information in your custody, by protecting it against such risks as unauthorized access, collection, use, disclosure or disposal.

And ESDC will:
a) only use the Personal Information for the purposes of policy analysis, research and evaluation of policies and programs respecting homelessness in Canada. Any reports emanating from this policy analysis, research and evaluation will contain only aggregate, non-identifiable information. These reports may also be shared with federal institutions and other stakeholders;
b) inform the Service Provider of any quality issues that are discovered in the Personal Information;
c) implement and maintain a secure storage system for the Personal Information collected under this Agreement and inform the Service Provider of any changes related to the collection, use, disclosure or retention of this Personal Information.
d) ESDC agrees to facilitate the sharing of technical information about software, functionality and security requirements, as required for use of the HIFIS SOFTWARE.

Termination/ Data Retention:
The Agreement states that either Party may terminate the DPA for any reason upon 60 days written notice and in the event of this occurring:
a) all Personal Information exported and shared with ESDC will be retained by ESDC in accordance with the *Library and Archives of Canada Act*, SC 2004 c.11.
b) the Region agrees to destroy all copies of the **HIFIS SOFTWARE** and Documentation in its possession, except for those copies made for archival or back-up purposes.

The process has not been defined or documented in terms of how service providers will be directed to obtain their site specific data upon termination of their use of HIFIS 4 or the termination of HIFIS 4 as a whole.

Participating Service Providers agree to follow the principles outlined in the HIFIS Data Sharing Protocol and individual users agree to the terms within the End User License Agreement upon first login to the system and the Attestation upon first access to each client. The Protocol outlines principles related to, but not limited to, service provider requirements to have client consent and a legal authority for collection, use and disclosure of their personal information; only accessing client information when there is a "need-to-know" and ensuring they follow the requirements within the HIFIS Data Entry and Administrator Guide and the HIFIS Data Integrity Guide. The Protocol also outlines the Region's responsibility to provide training and technical support while ensuring the ongoing security of the system and leveraging the data to plan for meaningful improvements within the HSS.

The impacts of these agreements made with EDSC and the participating service providers on the privacy risks related to Housing Services implementation of HIFIS are assessed in Section 5.3 of this PIA.

5. Homeless Individuals and Families Information System

5.1. Description of HIFIS Information Lifecycle

The HIFIS information flow processes involve:

- Client registers (intake) at service provider;
- Client requests for correction or updating PI;
- Funded service providers manage client data;
- Housing Services planners/analysts generate reports from HIFIS;
- ITS administrators maintain HIFIS infrastructure

The data flows involved in HIFIS include collection, use, disclosure, and final disposition.

Collection

HIFIS client information is collected and entered into HIFIS through the following methods:

- Service Providers collect information directly from the client using the HIFIS 4 Data Collection Form (General or Dependent versions) or they may record information directly into HIFIS 4 by adding a new client profile or updating an existing profile.

Use

The data collected in HIFIS is used for providing client intake services; case management; for housing stability system planning and for Federal homelessness tracking.

Disclosure

The identifiable client data held within HIFIS 4 may be disclosed across service provider sites as clients move from provider to provider with the HSS. Reports generated from HIFIS 4 with de-identified data will be used to inform housing planning at the municipal, provincial and federal levels.

Final Disposition

The retention for PI is outlined in the *Region of Waterloo Retention and Disposal Schedule By-Law No. 93-076 as amended* (DOCS# 888044v2) however at this time there is no plan to apply retention to this system. Once client data is entered into HIFIS 4 it will reside there until the system itself is terminated.

The process has not yet been defined or documented in terms of how retention will be applied upon termination of HIFIS 4 as a whole or termination of use of HIFIS 4 by an individual service provider in terms of access to their own site specific data. It appears individual service providers may be able to export a copy of their data and make the original files remaining in HIFIS 4 inactive or un-viewable however this will be a manual undertaking by the individual sites. The de-identified information required for reporting purposes will remain in HIFIS 4.

5.2. HIFIS Data Flows

Figure 1: HIFIS Data Flow Chart

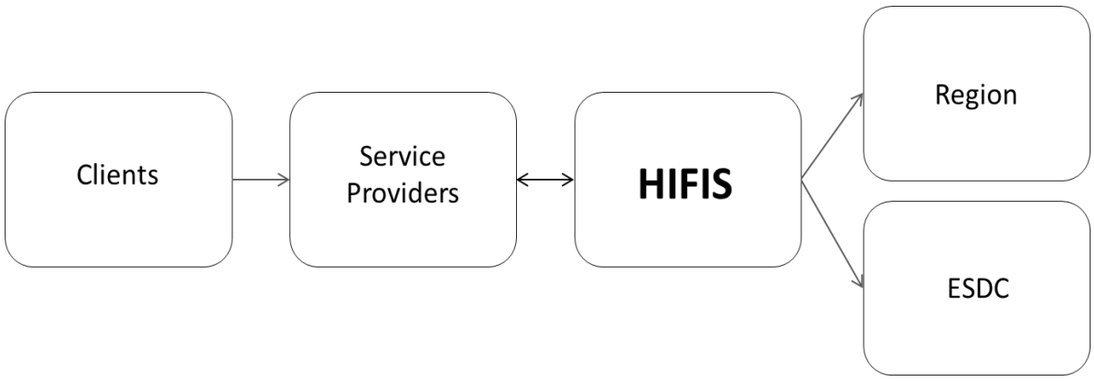
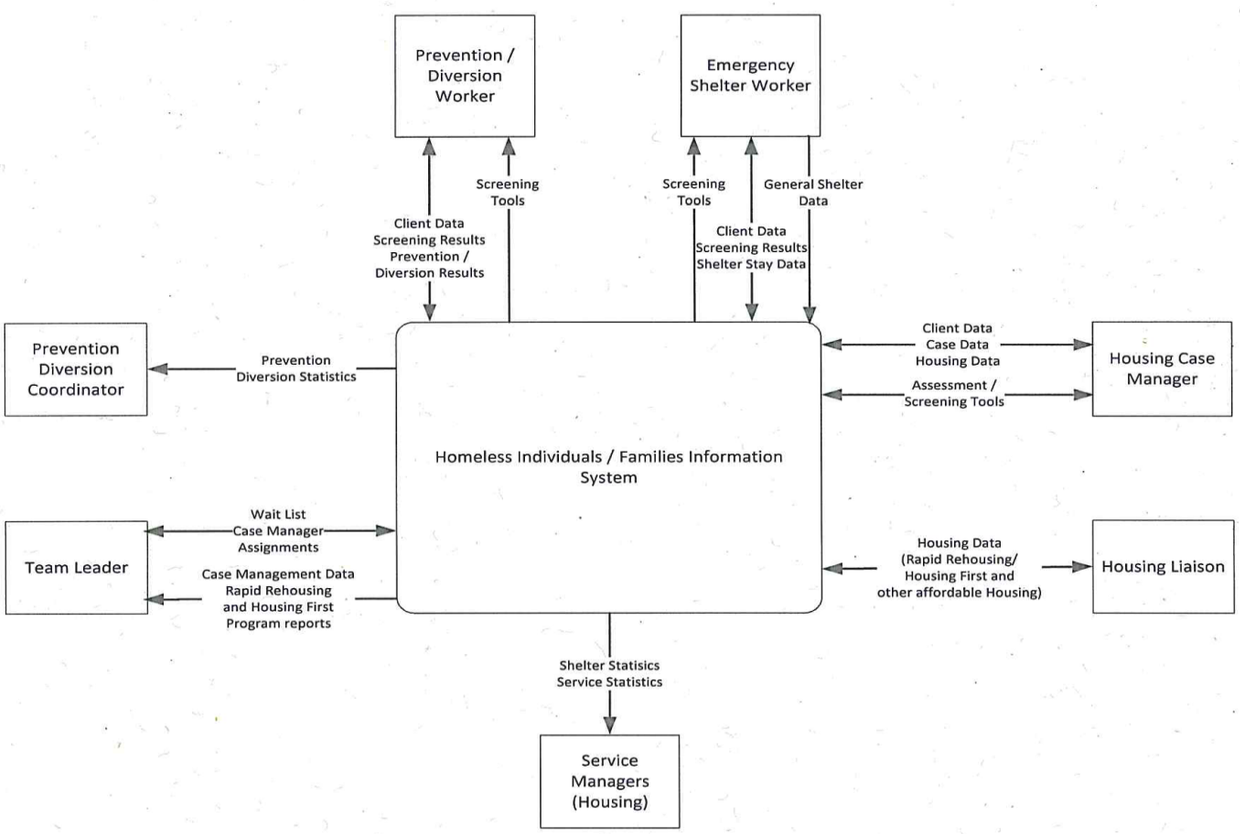


Figure 2: HIFIS Data Flow Chart



5.3. HIFIS 4 Privacy Risk Assessment

The risks identified in the privacy risk assessment below are colour coded according to the following levels:

Definition of Impact Rating

Very High	A major risk with the potential to lead to long-term damage to the Region's ability to meet its objectives. The consequences would cause serious, long-term regulatory, reputational, financial or operational problems to the Region and require top-level management intervention. It could cause significant reputational, financial and/or emotional distress to the individual as the subject of an information privacy breach.
High	A critical risk, which with proper management, can be endured by the Region. The consequences could include significant regulatory, reputational, financial or operational concerns for the Region, and require top-level management intervention. It could cause significant reputational, financial and/or emotional distress to the individual as the subject of an information privacy breach.
Medium	A significant risk that can be managed under normal circumstances by the Region. The consequences could cause regulatory, reputational, financial, or operational problems but could be managed internally by the Region. It could result in a moderate consequence to the individual, such as exposure of some financial information. The impact to the individual has the opportunity to be contained within the Region and further exposure is limited.
Low	A risk where consequences can be absorbed by the Region, but management effort is required to minimize the impact. The consequences might threaten regulatory, reputational, or operational standards but would be dealt with internally. This would be of low consequence for the Region. The impact to the individual has the opportunity to be contained within the Region and further exposure is limited.
Very Low	A risk where the consequences can be absorbed through normal activity. The consequences might threaten regulatory, reputational, or operational standards but would be dealt with internally. This would be of low consequence for the Region. The impact to the individual has the opportunity to be contained within the Region and further exposure is limited.

Definition of Likelihood Rating

Very High	The risk has occurred regularly or often, or will almost definitely occur.
High	The risk has occurred more than once, or has occurred in similar circumstances, or it is highly likely to occur.
Medium	The risk has previously occurred, or has been observed in similar circumstances, or it may occur.
Low	The risk has occurred infrequently to others in similar circumstances, but it has not occurred previously in the Region and it is not likely to do so.
Very Low	The risk has almost never or has never been observed, it may occur only in exceptional circumstances, or is it highly unlikely.

Risk Rating Reference Table

Impact	**Risk Reference Table**				
Very High	Medium	High	Very High	Very High	Very High
High	Medium	Medium	High	High	Very High
Medium	Low	Medium	Medium	High	High
Low	Very Low	Low	Medium	Medium	Medium
Very Low	Very Low	Very Low	Low	Medium	Medium
Likelihood	Very Low	Low	Medium	High	Very High

Principle 1 – Accountability

An organization is responsible for PI under its custody and control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

MFIPPA Obligations

25. (1) A head shall cause to be made available for inspection and copying by the public information containing,

(a) a description of the organization and responsibilities of the institution;

(b) a list of the general classes or types of records in the custody or control of the institution;

(c) the title, business telephone and business address of the head; and

(d) the address to which a request under this Act should be made

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of PI.	The Manager, Housing Policy and Homelessness Prevention, is accountable for the privacy components of HIFIS 4 and is the contact person for service provider privacy concerns. The Administrators of the individual service provider organizations are accountable for client privacy concerns.	No risk identified.	-	-	In compliance with Principle 1.
1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.	Service Provider Administrators and staff are provided information regarding who the contact person is at the Region of Waterloo.	No risk identified.	-	-	In compliance with Principle 1.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
1.3 An organization is responsible for PI in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.	The responsibility for collection of information is with the service providers and their staff when providing direct service to clients. This responsibility will remain with collection of data within HIFIS 4 however the Region will assume responsibility for protecting the data while stored at rest within HIFIS 4, hosted on the Region's server. These responsibilities are outlined in the HIFIS DSP.	Service Providers are in control of the PI of their clients collected in HIFIS 4 and thus retain legal responsibility for the way in which it is managed within the hosted system. The hosting duties assumed by the Region creates a conflict related to "custody and/ or control" of the collected data, especially in light of the absence of privacy provisions related to data retention/ destruction. This exposes the data to risk as the custody and control is not shared by one party, and is retained for the life of the database. The DSP documents responsibilities related to data collection, confidentiality and security but it is unclear who will be required to review this protocol.	Low / Low **Low**	1	Ensure that all of the responsibilities listed in the DSP are addressed with all users given access to HIFIS 4.
1.4 Organizations shall implement policies and practices to give effect to the principles, including					
(a) implementing procedures to protect personal information;	Procedures related to protection of personal information are outlined in: Privacy and Consent FAQs for Service Providers; the User Attestation upon login; and the DRAFT Security Protocol.	The Security Protocol is still in draft and has not been implemented.	Low / Low **Low**	2	Complete the draft Security Protocol and ensure users are educated on its contents.
(b) establishing procedures to receive and respond to complaints and inquiries;	The Region has organizational procedures in place to respond to PI complaints and inquiries. Service	The Security Protocol is still in draft and has not been implemented.	Low / Low **Low**	3	Complete the draft Security Protocol and ensure users are educated on its contents.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
	Providers will follow their own internal complaints/ inquiries processes. Complaints related to privacy breaches will be addressed in the DRAFT Security Protocol.				
(c) training staff and communicating to staff information about the organization's policies and practices; and	Service Providers: A representative from each participating Service Provider must be part of the "Training and Technology Working Group" – attending training themselves, training other users and reporting training given to Housing Services. Training is based on the content of the "Privacy and Consent FAQs for Service Providers". In addition an online training was created in VideoScribe for staff of participating service providers to view before gaining access to HIFIS 4. Region Staff: Since 2000 new Regional employees sign a Promise of Confidentiality Form HR15 at the time they are hired. This process still occurs but is now completed via online review and attestation through the Region's Learning Management System (LMS). Staff must also review HR Policy I-04 Confidential Information at this time. Since 2013 new staff members haven't received additional access and privacy	With the increased amount of PI being shared across service providers and from the service providers to the Region there is a heightened importance in relation to training of all those with access to the system. Ensuring all staff have received privacy training via one of the options available and that they are aware of the policies and practices governing appropriate use of the system before gaining access will be difficult to ensure compliance with due to the fact that it is manually administered and tracked.	Low / Med **Medium**	4	It is recommended that a procedure be implemented that requires mandatory privacy training and commitment by staff before they are given a login/ access to the system. It is recommended that re-training/ renewed commitment to follow the policies and practices for use of the system occur on an annual basis. It is also recommended that current and new Housing Services staff accessing HIFIS 4 be encouraged to complete the online privacy training module once complete.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
	training through the Learning at Work program. An online learning module is in development.				
(d) developing information to explain the organization's policies and procedures.	A common consent form was developed for clients that outlines policies and practices related to access, use, and sharing of their information within HIFIS 4. Additional information is documented in the Privacy and Consent FAQs for Service Providers should additional questions come up related to consent modifications, legal issues, etc.	There is a risk of increased privacy complaints, breaches and questions with the launch of the HIFIS 4. Although the consent form and FAQ document have been provided the completion of additional protocols eg. Privacy Complaint/ Breach Protocol will limit the risk of misinformation regarding how to handle specific situations.	Low / Low **Low**	5	It is recommended that the additional draft protocols to be developed are completed and incorporated within the current information available to both clients and users of the system.

Principle 2 – Identifying Purposes

The purposes for which PI is collected shall be identified by the organization at or before the time the information is collected.

MFIPPA Obligations

29. (2) If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection. R.S.O. 1990, c. M.56, s. 29 (2).

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
2.1 The organization shall document the purposes for which PI is collected in order to comply with the Openness principle (8) and the Individual Access principle (9).	The participating service providers request intake related information at the time a client presents for service. The purpose for this collection is explained verbally at this first point of direct contact with the client. The purpose for collection of personal information from HIFIS 4 by the various participating service providers is documented in the Common Consent to Release Information Form. The form includes a Notice of Collection as well as an attachment titled "Important Information About Consent" that detail the legislative authority, purpose, contact information for questions and detailed information related to who may collect their information, why they need it and the	No risk identified.	-	-	In compliance with Principle 2.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
	client's ability to limit this consent. sharing of information, consent, who may collect data.				
2.2 Identifying purposes for which PI is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (4) requires an organization to collect only that information necessary for the purposes that have been identified.	The available fields within the system for the collection of intake and case management related information, collected when clients present for service at a service provider location, would have been jointly identified by the Government of Canada and the service provider community based on the purpose of research, reporting requirements and the requirements and/ or needs of the providers to provide temporary shelter and case management. Staff users are directed by by the DPA to not collect any information in HIFIS that is outside of their legal authority and the purposes for the collection of PI by ESDC is described in detail in the DPA – "for the purpose of improving services to the homeless population and enhancing the Government of Canada's ability to respond to homelessness in Canada. It may also be used for policy analysis, research or evaluation purposes of policies and programs respecting homelessness in Canada."	The direction for staff users in the DPA is one line and does not clearly direct that they must limit their collection of PI to only that which is necessary for their purposes. It has also been identified that past practice allowed the individual service providers to collect additional information at the request of their clients as a "service" to them, for example copies of their identification. HIFIS 4 was built with the capacity to collect more information within the various modules than what has been clearly mapped to a legitimate, legislative authority through the PIA, as with the example above there is now an "Identification" module where information related to ID can be stored. The list of collected information identified in the Master HIFIS Planning Worksheet is extensive and while it identifies what can be shared, edited and exported, it does not identify the legal authority for each data element as the PIA List of Collected Information template requires. Due to this it is unclear what pieces of information would be considered unnecessary or	Low / Med **Medium**	6	It is recommended that fields or modules within HIFIS 4 that are not mapped to a legally authorized purpose be made unavailable for use and that the DPA be amended to include more clear direction related to limiting collection of PI to only that which is necessary/ legally authorized. If fields/ modules cannot be customized or providers insist on their use ensure they are not "shareable" or "exportable".

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
		outside of the legal authority for collection but as was identified with the issue of collecting ID it is understood there are examples of this yet the service providers feel the collection is important for their clients.			
2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the PI is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purpose.	See 2.1	No risk identified.	-	-	In compliance with Principle 2.
2.4 When PI that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose.	The PI collected in HIFIS will only be used for the purposes stated in the Common Consent for clients and the DPA for ROW/ ESDC. If a new purpose is developed clients will be notified to obtain consent prior to use.	No risk identified.	-	-	In compliance with Principle 2.
2.5 Persons collecting PI should be able to explain the purpose for which the information is being collected.	See 2.1	No risk identified	-	-	In compliance with Principle 2.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of PHI, except when inappropriate.

MFIPPA Obligations

14. (1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,

(a) upon the prior written request or consent of the individual, if the record is one to which the individual is entitled to have access

31. An institution shall not use personal information in its custody or under its control except,

(a) if the person to whom the information relates has identified that information in particular and consented to its use

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
3.1 Consent is generally required for the use and disclosure of PI. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use.	The HSS Common Consent form is completed in person by the client at the point of admission along with any other additional intake documentation.	No risk identified.	-	-	In compliance with Principle 3.
3.2 The principle requires "knowledge and consent." Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.	The Appendix of the HSS Common Consent Form provides detailed information related to the use and disclosure of the client's PI. The Privacy and Consent FAQs for Service Providers may also serve as a resource to staff when prompted with additional questions.	No risk identified.	-	-	In compliance with Principle 3.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purpose.	Individuals will not be required to consent to the collection, use, or disclosure of information beyond that which is required to fulfill the explicitly specified and legitimate purposes. Clients also have the option to be entered into the system with an anonymous code rather than personal identifiers.	No risk identified.	-	-	In compliance with Principle 3.
3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information.	All clients are provided the same Common Consent form and must provide express consent but the consent can be signed or confirmed verbally (script included in Privacy & Consent FAQs) and documented in the Consent Type field in HIFIS 4.	No risk identified	-	-	In compliance with Principle 3.
3.5 In obtaining consent, the reasonable expectations of the individual are also relevant.	The reasonable expectations of the individual have been considered.	No risk identified.	-	-	In compliance with Principle 3.
3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative.	See 3.4. The Privacy & Consent FAQs provide direction that incapable persons may have express consent provided on their behalf by an authorized individual or they can be entered into HIFIS 4 as “anonymous” until they can provide consent themselves. (see 3.3)	No risk identified.	-	-	In compliance with Principle 3.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
3.7 Individuals can give consent in many ways. For example: • an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information; • a check-off box may be used to allow individuals to request that their names and address not be given to other organizations; • consent may be given orally when information is collected over the telephone; or • consent may be given at the time that individuals use a product or service.	See 3.1.	No risk identified.	-	-	In compliance with Principle 3.
3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.	Clients have the ability to remove their consent on a go forward basis – the process for which is described in the Privacy & Consent FAQs document. The consent field is end-dated and staff can no longer make updates to the client's file however the information already shared within HIFIS will continue to be viewable. If the client re-presents at a later date staff will be prompted to modify the consent on the original file or a new file can be created with an "anonymous" code (see 3.3). In extreme cases a request can be made to have the file made un-viewable but this	Although client's may remove their consent, their information remains in HIFIS indefinitely and despite any limitations to sharing and masking that may be done, their name, age and gender will permanently appear on the full client list.	Low - Low **Low**	7	It is recommended that an update be made to the Privacy & Consent FAQs to outline the options for clients wishing to fully mask their information within HIFIS 4, for example, in a risk situation, etc.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
	has not been clearly documented.				

Principle 4 – Limiting Collection

The collection of PI shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

MFIPPA Obligations

28. (2) No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. R.S.O. 1990, c. M.56, s. 28.

29. (1) An institution shall collect personal information only directly from the individual to whom the information relates

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
4.1 Organizations shall not collect PI and PHI indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information handling policies and practices, in accordance with the Openness principle (8).	See 2.2	See 2.2	Low - Med **Medium**	8	See 2.2
4.2 The requirement that PI be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.	See 3.1 and 3.2. Consent will not be obtained through deception. If a client is incapable of understanding the consent they will be entered as “anonymous” so they may still receive service.	No risk identified.	-	-	In compliance with Principle 4.

Principle 5 – Limiting Use, Disclosure, and Retention

PI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. PI shall be retained only as long as necessary for the fulfillment of those purposes.

MFIPPA Obligations

30. (1) Personal information that has been used by an institution shall be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information.

31. An institution shall not use personal information in its custody or under its control except,

(b) for the purpose for which it was obtained or compiled or for a consistent purpose

32. An institution shall not disclose personal information in its custody or under its control except,

(c) for the purpose for which it was obtained or compiled or for a consistent purpose;

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
5.1 Organizations using PI for a new purpose shall document this purpose.	If changes are made to the purpose for collecting PI they will be communicated to clients before the new purpose is implemented.	No risk identified.	-	-	In compliance with Principle 5.
5.2 Organizations should develop guidelines and implement procedures with respect to the retention of PI. These guidelines should include minimum and maximum retention periods. PI that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after	Housing Services is subject to the Region's Information Retention and Disposal By-law 93-076 as amended (DOCS# 868731v1); current retention rules are set out in Appendix F. As stated in the Summary of HIFIS 4 Data Privacy and Security Features draft document, while service providers have	The Region's Retention By-law, as well as the individual retention obligations of the service providers, cannot be applied in the HIFIS system. Directions for the alternative actions available, details related to the circumstances of a service provider choosing to leave HIFIS 4 and/or the termination of the use of HIFIS 4	Low - High **Medium**	9	It is recommended the Retention Protocol be drafted, finalized and communicated as mentioned, including planning and consideration of applying retention to any exported data.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.	primary ownership over their client's data, the Region has shared ownership of the data in their role as Community Coordinator. This document also dictates that it is the responsibility of the Region, as Application Host, to develop retention policies which to date have not been drafted but are said to be in the process of development in the Privacy & Security FAQs document. Files are never destroyed once entered into HIFIS 4 but they can be made inactive or un-viewable.	completely to date have not been documented (referred to as a "Retention Protocol" in the Privacy & Consent FAQs document). Some of the risks associated with the retention of PI for a time that is not consistent with a legitimate retention period are inappropriate access, unintended loss, inappropriate disposal, and denial of access.			
5.3 PI that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of PI.	See 5.2	See 5.2	Low - High **Medium**	10	See 5.2

Principle 6 – Accuracy

PI must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

MFIPPA Obligations

30. (2) The head of an institution shall take reasonable steps to ensure that personal information on the records of the institution is not used unless it is accurate and up to date.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
6.1 The extent to which PI shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-do-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.	Service Providers are responsible for ensuring that client PI which is collected, used, and disclosed is as accurate and complete as possible, updating and verifying information with each presentation for service as directed in the draft Data Entry and Administrator Guide. The guide goes on to explain the importance of the data remaining current for service but also for reporting requirements within the organization, the region, and beyond, and requests daily updates for each participant and for every stay or period of service use. The DSP for users of HIFIS 4 indicates that the protocols above in the draft guide must be complied with. The DPA entered into with ESDC in order to use HIFIS 4 states that service providers and the Region must "ensure the completeness and accuracy of the PI" which is then provided to ESDC.	The DSP references compliance with the Data Entry and Administrator Guide however this document remains in draft; it is unclear when it will be finalized/ shared with the service providers. There does not appear to be a documented 'request for correction/ access' process. The closest reference is in the Common Consent form's attached "Important Information About Consent" document which identifies that clients may request to see what PI has been collected about them. There is also reference within the Privacy & Consent FAQs document to the development of a policy/ procedure on requests for HIFIS 4 data (see Subpoena and Media sections).	Very Low - Med **Medium**	11	It is recommended that the draft Data Entry and Administrator Guide be finalized and communicated to all users, perhaps requiring sign-off to ensure compliance. It is recommended that the Privacy & Consent FAQs document be updated to include instructions related to client access/ correction requests and that the policy/ procedure related to access to data include access requests by clients to their own PI and the process to request corrections. This could also be included in the Requests for HIFIS data Policy/ Procedure which should be drafted.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
6.2 An organization shall not routinely update PI, unless such a process is necessary to fulfil the purposes for which the information was collected.	See 6.1. Regular/ routine updates to PI are required for this type of service.	No risk identified.	-	-	In compliance with Principle 6.
6.2 PI that is used on an ongoing basis, including information that is disclosed to third parties, should be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.	See 6.1.	See 6.1.	-	-	See 6.1.

Principle 7 – Safeguards

PI shall be protected by security safeguards appropriate to the sensitivity of the information.

MFIPPA Obligations

30. (4) A head shall dispose of personal information under the control of the institution in accordance with the regulations. R.S.O. 1990, c. M.56, s. 30.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
7.1 The security safeguards shall protect PI against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect PI regardless of the format in which it is held.	The Region is the Application Host for HIFIS 4. Data is stored on Regional servers behind the Region's firewall. The data is backed-up nightly with the back-up stored on a separate server. Additional details related to the technical security have not been provided however a Security Policy/ Protocol is said to be in development.	The data is currently not encrypted within the database nor is it encrypted in transmission therefore there is a risk to inappropriate access, disclosure, copying or use. The Region's own "Use of Information Technology" policy states that personal information being accessed externally via the web must be encrypted using a Regionally approved encryption solution. There may be additional technical risks but complete details have not been provided.	High - Med **High**	12	It is recommended that SSL encryption be enabled to ensure secure transmission of data in transit and encryption at rest be considered for the database itself based on Region policy for databases housing PI. It is recommended that the Security Policy/ Protocol referenced in the PIA Interview Questionnaire (see Appendix C) be drafted and include all details related to administrative, technical and physical safeguards employed as outlined in this section of the PIA.
7.2 The methods of protection should include:					

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
(a) organizational measures (e.g. security clearance);	All HIFIS users require an operating system login to initiate a session with any server or workstation. Based on user group account permissions, users will receive access to perform allowed tasks, and will not allow any administrative work, such as changing system configuration or installing/removing applications. Every user account is assigned to a user group. Each user group in turn is assigned a specific set of functionality based on service site and data elements. This group to functionality assignment is configurable and can be specified on a very fine level of detail. Each account contains the user's name and password, plus the allocation to a user group. For specific details related to the 12 defined user roles see the User Templates tab within the Master HIFIS 4 Planning Worksheet.	While user roles/ groups have been defined in detail, individual users have access to a significant amount of PI of all clients within HIFIS 4, regardless whether they are servicing them at their site or not. Due to this there is a risk of inappropriate access, use or disclosure. There is the expectation set out that all staff will receive training concerning appropriate access/ use of the system and that the Attestation requirement for first time access to each client will provide added protection. (see Principle 1)	Low - Med **Medium**	13	See Principle 1 recommendations re training. It is recommended that user access be audited on a routine basis. See next section.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
(b) technological measures (e.g. passwords, auditing); and	Administrators are responsible for account and password maintenance – the Region Super User for Region staff and the Service Provider Admins at each site for service provider staff. There is some question as to whether or service provider users will all have individual, unique logins/ passwords or if they will share generic logins. The HIFIS software does not currently have password requirements. It has been suggested that this can be configured through a membership element in the web configuration but it is unclear if this has been done.	Accounts must be unique to individual users in order to validate appropriate access to client PI and the ability to individually attest to appropriate access. HIFIS 4 does not currently enforce minimum password length and character requirements or mandatory password changes and it is unknown at this time if changes will be made. This could leave the system vulnerable to unauthorized access.	Low - Medium **Medium**	14	It is recommended that the Security Policy/ Protocol be drafted to include account and password maintenance rules. Accounts must be unique and passwords should follow Corporate practices which requires at least one number and uppercase letter; expires after 90 days; and locks after 3 attempts.
	HIFIS 4 tracks all user activity and is fully auditable via built in audit reports. The Region intends to use the Audit Log feature within HIFIS and will draft a monthly "Privacy and Security Audit Report" to identify possible concerns eg. after hours use of HIFIS, unusual remote access, users access to individuals outside of scope of work, which service providers will run and review for their users. It is also referenced in the Privacy & Consent FAQs that a Privacy Breach Protocol will be developed, including additional reports to be used for	The reports and protocols for auditing have not been developed to date therefore there is currently no auditing taking place. This created a risk of an undetected invasion of client privacy or breach.	Low - Medium **Medium**	15	It is recommended that the Administrator set up reports and assign responsibility to appropriate individuals to perform the following audits: identification and review of usage patterns; review of user access and roles; random auditing; and reactive auditing based on triggered events. The roles for auditing HIFIS and taking any necessary actions should also be clearly described in Security Policy/ Protocol and/or Privacy Breach Protocol.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
	monitoring access for privacy breaches.				
(c) physical measures (e.g. restricted access to offices).	Physical security measures in terms of server room and building, protection from natural and environmental hazards, unauthorized intrusion, and so on was not shared therefore it is difficult to assess however there is a general understanding that systems hosted by the Region are well protected.	Missing information related to physical security measures – potential for risk.	Very Low -Very Low **Very Low**	16	It is recommended that additional information related to physical security be obtained from ITS.
7.3 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.	See 5.2	See 5.2	Low - High **Medium**	17	See 5.2

Principle 8 – Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of PI.

MFIPPA Obligations

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
8.1 Organizations shall be open about their policies and practices with respect to the management of PI. Individuals shall be able to acquire information about an organization's policies and practices	Any individual whose PI is handled by Housing Services will be able to obtain information about the organization's information practices by using reasonable and ordinary effort.	No risk identified.	-	-	In compliance with Principle 8.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
without unreasonable effort. This information shall be made available in a form that is generally understandable.					
8.2 The information made available shall include:					
(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;	Clients are directed to Housing Services for questions on the Common Consent form and will also have a direct contact at each service provider. This process could be formally documented along with a Complaints process within the Requests for HIFIS data policy/ procedure and/ or Privacy Complaint/ Breach Protocol that are still to be drafted.	The formal process has not been documented therefore there is a chance clients would be misdirected/ misinformed or receive inconsistent information.	Very Low-Very Low **Very Low**	18	It is recommended that the Requests for HIFIS data policy/ procedure and Privacy Complaint/ Breach Protocol be drafted to include this information.
(b) the means of gaining access to personal information held by the organization;	See 8.2(a)	See 8.2(a)	Very Low-Very Low **Very Low**	19	See 8.2(a)
(c) a description of the type of personal information held by the organization, including general account of its use;	An open data set of the Corporate classification system is available on the Region's website. Access to the Housing Services classification manual will be given upon request.	No risk identified.	-	-	In compliance with Principle 8.
(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and	See 8.2(a)	See 8.2(a)	Very Low-Very Low **Very Low**	20	See 8.2(a)
(e) what PI is made available to related organizations.	No PI is made available to related organizations.	No risk identified.	-	-	In compliance with Principle 8.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations.	See 8.2(a)	See 8.2(a)	Very Low-Very Low **Very Low**	21	See 8.2(a)

Principle 9 – Individual Access

Upon request, an individual must be informed of the existence, use and disclosure of his or her PI and must be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

MFIPPA Obligations

36. (1) Every individual has a right of access to,

(a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution; and

(b) any other personal information about the individual in the custody or under the control of an institution with respect to which the individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution.

(2) Every individual who is given access under subsection (1) to personal information is entitled to,

(a) request correction of the personal information if the individual believes there is an error or omission;

(b) require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and

(c) require that any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required be notified of the correction or statement of disagreement. R.S.O. 1990, c. M.56, s. 36.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
9.1 Upon request, an organization shall inform an individual whether or not the organization holds PI about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third party to which it has been	As outlined in the Common Consent form clients may request information on what information has been collected about them, whom it has been shared with and what is has been used for. Again it would be beneficial to have this formally documented in the Requests for HIFIS data policy/ procedure. Individuals who prefer to request information from the Region may use their right of access as set out in MFIPPA and make a written	See 8.2(a)	Very Low-Very Low **Very Low**	22	See 8.2(a)

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
disclosed.	request to the Region's Privacy Office.				
9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of PI. The information provided shall only be used for this purpose.	These requirements should be included in the documented formal process. Clients using their right of access through MFIPPA are required to make the request in writing using the MFIPPA Request Form.	See 8.2(a)	Very Low-Very Low **Very Low**	23	See 8.2(a)
9.3 In providing an account of third parties to which it has disclosed PI about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.	See 9.1.	See 9.1.	Very Low-Very Low **Very Low**	24	See 9.1.
9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.	See 9.1.	See 9.1.	Very Low-Very Low **Very Low**	25	See 9.1.
9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of PI, the organization	Requests for the correction can be made directly to the service providers. See 6.1.	See 6.1.	Very Low-Very Low **Very Low**	26	See 6.1.

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.	Clients who prefer to use their right for correction as set out in MFIPPA must make the request in writing using the MFIPPA Request Form. Corrections may be requested for errors and omissions only.				
9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence to the unresolved challenge shall be transmitted to third parties having access to the information in question.	Direction for service provider response needs to be documented to guide the process. See 9.5 The Region's process states that a client may request a statement of disagreement be attached to the record in question if correction is not granted but the process has not been documented.	See 9.5	Very Low-Very Low **Very Low**	27	See 9.5

Principal 10 – Challenging Compliance

An individual has the right to be able to address a challenge concerning compliance with the above to the designated individual or individuals with regard to the organization's compliance.

MFIPPA Obligations

39. (1) A person may appeal any decision of a head under this Act to the Commissioner if,

(a) the person has made a request for access to a record under subsection 17 (1);

(b) the person has made a request for access to personal information under subsection 37 (1);

(c) the person has made a request for correction of personal information under subsection 36 (2); or

(d) the person is given notice of a request under subsection 21 (1). R.S.O. 1990, c. M.56, s. 39 (1).

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
10.1 organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of PI. The complaint procedures should be easily accessible and simple to use.	See 8.2(a) Complaints about Region information practices may be directed to the Manager of IM&A as the Acting MFIPPA Contact Person.	See 8.2(a)	Very Low-Very Low **Very Low**	28	See 8.2(a)
10.2 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the PI handling practices of the companies they regulate.	See 8.2(a) Clients are to be made aware that they are entitled to address Region privacy complaints and concerns to the Information & Privacy Commissioner (IPC) of Ontario.	See 8.2(a)	Very Low-Very Low **Very Low**	29	See 8.2(a)
10.3 An organization shall investigate all complaints. If a complaint is found to be	All complaints will be investigated through a structured process to be	See 8.2(a)	Very Low-Very Low	30	See 8.2(a)

Privacy Requirement	Current Practice	Risk(s)	Risk Score (Likelihood/Impact)	#	Recommendation
justified, the organization shall take appropriate measures, including, if necessary, amending its policies and procedures.	documented in the Privacy Complaint/ Breach Protocol to be drafted. See 8.2(a)		**Very Low**		

6. Conclusion

Housing Services has conducted an extremely thorough review of the practices related to use of HIFIS 4, as they relate to the identification of risks to the privacy of clients and the confidentiality and security of their PI, as they implement HIFIS 4 for the Housing Stability System in the Region of Waterloo. By virtue of participating in the PIA, Housing Services as well as the service providers affected were made aware of the identified risks and related recommendations. It is understood that they have already begun the process of addressing the risks related to privacy requirements including the development of a number of important policies/ protocols related to privacy, including access, retention, complaints/ breaches, and security governance including development of auditing reports and governance for their use.

There are a significant number of low level risks that can be addressed through development of these policies and procedures and updates to the various guides and tools that already exist for users of the system, perhaps combined in one HIFIS User Manual. The manual should outline user accountability, roles and privacy responsibilities; ROW Super Administrator and Service Provider Administrator user account management; consent management; auditing; data integrity and troubleshooting procedures. Ideally, users would confirm they have read the manual and understand their privacy responsibilities before they are given access to the system. The medium and high level risks will be more difficult to address as they relate to the way to system operates, including the lack of retention, broad access to data and lack of encryption.

The recommendations in this PIA put Housing Services in a good position to implement solutions to address many of the risks identified as the continue to move forward with full implementation of all phases of HIFIS 4.

Appendix A: Documentation Reviewed for this PIA

Category	Reference
Project Plan	• HIFIS 4 Project Binder (DOCS #2626246v1) • HIFIS 4 Implementation Checklist (DOCS #2623106v1)
Contracts	• Data Provision Agreement (DOCS #2604108v2) • Data Provision Agreement – Briefing Note (DOCS #2605847v1)
System Specifications	• Waterloo Data Components (DOCS #2599173v1) • HIFIS 4 Data Migration Plan (DOCS #2579110v2) • Data Entry and Administrator Guide (DOCS #2626071v1) • Data Quality Guide (DOCS #2626075v1)
Legislation	• Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56 • Housing Services Act, 2011, S.O. 2011, c. 6, Sched. 1 • Municipal Act, 2001, S.O. 2001, c. 25. s.69
Privacy/ Other Policies and Procedures	• HIFIS 4 Data Sharing Protocol (DOCS #2626070v4) • HIFIS Working Group Terms of Reference (DOCS #2626076v1) • Housing Stability System Common Consent form (DOCS #2633513v7) • HIFIS 4: Privacy and Consent FAQs for Service Providers (DOCS #2669900) • Human Resources Policies Section No. I Policy No. 4 Confidential Information (DOCS #41657v2) • Human Resources Policies Section No. I Policy No. 6 Use of Information Technology (DOCS #41658v12)
Staff Confidentiality Agreement	• Promise of Confidentiality (DOCS #240497v1) • Attestation (DOCS #2791392) • EULA (DOCS #2791384) • VideoScribe Privacy Training script (DOCS #2782035)
Current fields of information collected	• HIFIS 4 PIA List of Collected Information (DOCS #2567552)
Staffing positions that will access the information collected	• HIFIS 4 PIA Users of Personal Information (DOCS #2567552v1) • Local Rights Template Configuration (DOCS #2634436v1)
PIA documents	• Preliminary Privacy Impact Assessment (DOCS #2102489v6)

Appendix B: Interviews Conducted for this PIA

Interview	Date	Participants
Introduction to revived project (initial meetings took place March 2016)	2017/04/11	Angela Pye, Manager, Housing Policy and Homelessness Prevention Marina Sloutsky, Student Brennan Hardy, Information & Privacy Analyst
Start-Up Meeting with new Social Planner assigned to project	2017/12/12	Angela Pye, Manager, Housing Policy and Homelessness Prevention Tracy Verhoeve, Social Planning Associate Brennan Hardy, Information & Privacy Analyst
Various PIA completion meetings	12/2017 – 09/2018	Tracy Verhoeve, Social Planning Associate Brennan Hardy, Information & Privacy Analyst

Appendix C: HIFIS 4 PIA Interview Questionnaire[2]

Y (Yes): You know the privacy protection requirement either has been met by existing measures or will be met by action planned before implementation.
N (No): You know nothing has been done or is planned to address this privacy protection requirement, that is, there is a possible privacy risk in the project's compliance.
IP (In Progress): You do not know the answer to the question at this time, that is, more information or analysis is required and until such time, there is a potential privacy risk.
NA: You know this privacy protection requirement is not applicable to the project.

Number	Question	Y	N	IP	NA	Enclosed Reference/Comments
Accountability						
1	What legal authority is there for this business activity? Is the collection of personal information authorized under MFIPPA or another act?	Y				The authority for this initiative is derived from the Region's role as Service Manager as per the Housing Services Act, 2011 (2011, c. 6, Sched. 1, s. 11 (1).), and the requirement as Service Manager to develop a 10 year Housing and Homelessness Plan. The authority is also derived more specifically in accordance with the provincial Community Homelessness Prevention Initiative and funding provided to Service Managers to develop local strategies for preventing and addressing homelessness - http://www.mah.gov.on.ca/Page9183.aspx The collection of PI by Housing Services from within HIFIS 4 is authorized under MFIPPA as collection is expressly authorized by statute (s.28(2)), once again the Region's designation as 'Service Manager' within the Housing Services Act (Part III).
2	Will this program ever collect any personal health information?	Y				Housing Service Providers evaluate a client's mental and physical abilities to as part of their assessment for appropriate housing needs, supports and accommodations. Implementation of HIFIS 4 is not changing this process.
3	Has responsibility for the collection been assigned to program staff or third party service providers?	Y				Collection of PI/ PHI will take place via third party housing service providers in the community. Region staff will collect data required from within HIFIS 4.
4	Who is accountable for the privacy component of this project?	Y				The Manager of Housing Policy and Homelessness Prevention is the contact person for service provider privacy concerns. Service Providers are the contact for client concerns.
5	Are there any privacy policies and procedures applicable to this program?	Y				Current corporate privacy policies and procedures are applicable to Region staff. Service Providers will adhere to Data Sharing Protocol (2626070v4) as well as other guides related to

[2] Questionnaire based on the Privacy Analyst Checklist in Appendix C of the Planning for Success: Privacy Impact Assessment Guide published by the IPC

						consent and privacy.
6	Have/will employees working in this program area received privacy training?	Y	N			Service Providers will receive training on privacy and consent roles and responsibilities before using the system (DOCS #2670236). Region employees do not receive specific privacy training.
7	Will employees sign a confidentiality agreement?	Y				Human Resources policy I-04 Confidential Information states that Regional staff will maintain the confidentiality of the information they gain through work (DOCS #41657V2). New Regional employees sign a Promise of Confidentiality Form HR15 (DOCS #240497V1). Service Providers electronically review and agree to an End User License Agreement at time of first login. (2791384) In addition, when a client is accessed in the system for the first time by site an attestation will appear (2791392) requiring the user to attest that they have a reason to view the information of that particular client. In the future the preference is for this to happen for each user the first time they access a client rather then per site.
8	Do contracts with external service providers contain privacy provisions?	Y				The Data Provision Agreement with ESDC contains privacy provisions (DOCS #2604108).
Identifying Purposes						
9	Has the purpose of the collection been defined? What is the purpose of collection?	Y				The purpose is to provide housing stability services and supports to those within the housing stability sector. A shared data management environment will allow for a more coordinated approach to service delivery, data monitoring and system improvements within the Region. The HIFIS Project Team completed a list of Collected Information (#2567552). Service providers follow our data collection requirements in addition to their own operational needs.
10	Will notice of collection be provided to the individual(s)? Explain timing, method, and exemptions from notice, where authorized.	Y				Notice of collection is a written statement on the HSS Common Consent form. Service Provider staff will also be able to explain the purpose for collection during in person registration. The notice will be given before collection begins.
11	Who determines what personal information is required and how was this determined?	Y				See question 9
12	Has each piece of personal information collected been mapped to a legitimate purpose? For Example, if birthdate is collected, has it been determined that this information is necessary?	Y				Information is collected based on the Region's mandated data collection requirements and the service providers own operations needs. (#2567552)
13	Will personal information be used for other purposes? If so, do you have a process in place to update the relevant notifications?				NA	De-identified/ aggregate information will be used for planning and reporting purposes.

14	Is any personal information collected from a source other than the individual? Explain authority for indirect collection.	Y				All collection by Region staff where required is collected from within HIFIS 4 rather than from the individual directly. This collection and purpose is outlined within the HSS Common Consent form.
15	Is there a procedure in place that would inform the supplier of information about another individual that the information would belong to that other individual and subject to the right of access to that individual?		N			No procedure in place.
Consent						
16	What is the method of requesting consent? Please outline the process involved and provide any forms that may have to be filled out.	Y				The HSS Common Consent form is completed in person by the client at the point of admission. (DOCS #2633513)
17	Does an individual have an opportunity to change their level of consent? If so, is each staff member aware of what information must be collected in order to act on the request?	Y				This process is described in the Appendix of the HSS Common Consent Form (2633513) and the Privacy and Consent FAQs (2669900).
Limiting Collection						
18	Is all the personal information collected necessary for the project to proceed? Why or why not?	Y				Providers were collecting info with v 3 so needed to remain consistent to their operational needs as well as the Region's data collection requirements.
19	Will the staff collecting the information be trained to ensure that the individual provides only the personal information that is required? For Example, do they know that if the individual does provide more personal information than required, they only need to collect the required information?	Y				Staff are provided with training before accessing HIFIS 4. Many of the fields are indicated as mandatory (with a red star) in HIFIS. Staff are also provided with a Data Entry Guide to indicate which additional fields must be entered to meet the Region's reporting requirements.
Limiting Use, Disclosure, and Retention						
20	What procedures are in place to make sure the personal information is accessed by only those who need to know?	Y				Well defined user templates were created to be able to restrict access to various areas/ fields within the system to those personnel that have a need to access the data. See PIA Users of Personal Information (DOCS #2567552).
21	Has the manner of disclosure been defined, for example, oral, mail, email, etc.?	Y				PI is communicated verbally by clients and entered into HIFIS 4 by Service Provider staff at admission. Some Providers may also record the information on the HIFIS 4 Data Collection Form.

						Any required disclosures between service providers will take place within HIFIS 4 based on the user's level of access.
22	Will the disclosures be documented and how?	Y				An audit trail of users views, edits, additions, deletions, searches along with time and IP address associations can be tracked within HIFIS 4.
23	Would personal information that is collected ever be disclosed to a third party? Will the disclosure be documented and controlled by information sharing agreements or other means?	Y				Non-identifiable personal information related to the Service Provider and its clientele with be collected and used by EDSC in accordance with the Data Provision Agreement (DOCS #2604108). ESDC has the authority under the Department of Employment and Social Development Act (the "DESD Act") and the Privacy Act to collect the Personal Information for the administration of the Homelessness Partnering Strategy. The Personal Information will be used for the purpose of improving services to the homeless population and enhancing the Government of Canada's ability to respond to homelessness in Canada. It may also be used for policy analysis, research or evaluation purposes of policies and programs respecting homelessness in Canada.
24	Is it reasonably likely that personal information will need to be disclosed for research purposes?	Y				Only de-identified information will be used for planning and research purposes.
25	How and where is the personal information in the program stored? For example: on a server and location. Provide details, including the rationale, for any access, storage and disclosure outside of Canada.	Y				Data is stored on Regional servers maintained in the Regional data centre. These are maintained behind Regional firewalls. The data is not currently encrypted in the data centre. HIFIS National indicates that the data could be encrypted but no organization has done this to date.
26	Have retention periods been set on the types of personal information collected in the program?		N			HIFIS 4 does not have the ability to apply data retention rules. Files are never destroyed in HIFIS 4, but they can become inactive or made un-viewable. De-identified information remains in HIFIS 4 for reporting purposes. Retention rules/ policies may be developed.
27	How is the information going to be destroyed at the end of the retention period? Is there a procedure in place for accomplishing this?			IP		The Project Team is currently developing a procedure to document secure destruction of PI at end of life. Low level of risk related to agencies that may lose their funding and choose to leave HIFIS.
28	Will procedures be defined and documented for disposal of devices and equipment containing personal information?		N			
29	Will details of the disposal of personal information be recorded?			IP		See question 27

Accuracy						
30	Will there be measures in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of measures.	Y				ROW does not own the data and it is entered by the service providers therefore not within ROW's ability to enforce any measures. Updates to client info at sites with each new visit. Also service providers are provided with the HIFIS 4 Data Quality Guide which addresses data integrity and maintenance.
31	Will controls be in place to ensure that only authorized personnel will be able to add, change or delete personal information?	Y				Well defined user templates were created to be able to restrict access to various areas/ fields within the system to those personnel that have a need to access the data. See PIA Users of Personal Information (DOCS #2567552).
Safeguards						
32	Will measures be used to secure the personal information? Explain each physical, technical and procedural measure.			IP		Data is stored on Regional Servers behind the Regional firewall. The data is not currently encrypted in the database however HIFIS national indicates this is possible although no organization has done so. Data is currently not encrypted in transmission to and from the data centre although HIFIS national indicates it is possible to enable Transport mode security (done when configuring the application for SSL/TLS) and data will be encrypted in transit. Data is backed-up on a nightly basis and data is stored in two locations. Based on defined user templates (see DOCS#2567552) with account permissions, users will receive the appropriate level of role-based access from their Administrator. Administrators at each service provider site will receive their user access from the ROW site Administrator in Housing Services. OS account maintenance for Administrators is centralized, and under full control of Housing Services who will assign administrative access to authorized and qualified personnel. These administrators become responsible for account and password maintenance for the users at their individual sites. The HIFIS software does not have password requirements; however, password best practices will be recommended in the HIFIS 4 Security Protocol. HIFIS is accessed from a web browser and requires a userid and password. In the application it is possible to set-up rules on password configuration. It can be configured through the 'membership' element in the web.config. See: https://msdn.microsoft.com/en-us/library/system.web.security.membership(v=vs.110).aspx The defined user accounts are assigned to unique individual users. Each user is assigned a

						specific set of functionality based on their role. This group to functionality assignment is configurable and can be specified on a very fine level of detail. Each account contains the user's name and password, plus the allocation to a user group. Access within the system is tracked and fully auditable, tracking the time, IP address and user name for all activity. The Region will use the Audit Log feature within HIFIS and will draft a monthly "Privacy and Security Audit Report" to identify possible privacy and security issues (e.g., after hours use of HIFIS, users reviewing information outside their own scope of work, unusual remote access). The Region will also draft a monthly Privacy and Security Audit Report for CHAC Users. Note, although remote access of HIFIS 4 will be permitted, the Privacy and Security Audit Report will be used to assess "unusual" remote access activity.
33	Is there a process in place for access or role change for system users?	Y				Region Super Administrator sets up new Administrators and new Region staff user accounts. Service Provider level administrators can set up accounts for new staff at their own organization. Service Providers are trained on HIFIS Administration and can refer to the Service Provider Administration Manual for reference.
34	How is the data backed up?	Y				Data is backed-up on a nightly basis and data is stored in two locations.
35	Are network devices, such as routers and switches password protected?			IP		ITS to inform
36	What are the password rules and how are they managed / implemented?			IP		Will the same password standards as that used by Information Technology Service to manage network access be set up? The HIFIS software does not have password requirements; however, password best practices will be recommended in the HIFIS 4 Security Protocol. ???? In HIFIS 4.0 it is possible to set-up rules on password configuration. It can be configured through the 'membership' element in the web.config. See: https://msdn.microsoft.com/en-us/library/system.web.security.membership(v=vs.110).aspx
37	Will security policies and procedures be defined and documented to protect the confidentiality, integrity, and availability of personal information?			IP		A HIFIS 4 Security Policy/ Protocol is under development.
38	Will all actions relating to the collection, use, disclosure, retention, correction, copying or disposal be logged and subject to auditing and monitoring?		N			ROW will audit ROW staff; service provider Administrators will audit their staff with built in auditing reports that are under development. User access/ actions within the system are tracked and fully auditable, tracking the time, IP address and user name for all activity. The

						Region intends to use the Audit Log feature within HIFIS and will draft a monthly "Privacy and Security Audit Report" to identify possible privacy and security issues (e.g., after hours use of HIFIS, users reviewing information outside their own scope of work, unusual remote access). Note, although remote access of HIFIS 4 will be permitted, the Privacy and Security Audit Report will be used to assess "unusual" remote access activity. Will there be automated audit reports? No.
39	Will procedures be defined and documented on how to identify, report, investigate and address the unauthorized access, collection, uses, and/or disclosures of personal information?			IP		
40	Will the data collected for this program ever be anonymized for analysis purposes?	Y				Yes, de-identified data extracted from HIFIS 4 will be used for housing stability system planning by ROW and will be exported to the NHIS to create a portrait of homelessness in Canada.
41	Will any personal information ever be printed? If so, are there safeguards in place to ensure it's protected?	Y				The HIFIS software does not feature a print function except for the purposes of printing HIFIS 4 Reports. However, users may choose to print their browser screen if desired and there is no mechanism to restrict this behaviour.
42	Is there a process for managing a privacy breach?			IP		ROW is developing a protocol.
Openness						
43	Will there be awareness on the privacy aspects of this program and will this PIA be made public?	Y				Yes service providers are aware of the privacy aspects of the system and are involved in coordination, planning, and communication around the project through membership on the HIFIS Working Group. Other working groups may be established to address specific needs/ topics for example Consent. The HIFIS Project Team are open to sharing the final PIA with other municipalities upon request.
Individual Access						
44	Will the management of personal information change or restrict individuals' right of access to their personal information?		N			HIFIS 4 is a new version of an existing database therefore clients may still request their I personal information from service providers as they could previously. The new version does not change this process or place any restriction on access.
45	Is there a process for individuals to request their personal information?	Y				Service providers will have established processes based on their own operations as they are the owners of the data.

46	Are there any procedures in place, other than a MFIPPA request, for someone to access and request correction to their information?	Y				Requests for personal information will go directly to the service providers as they are the owners of the data.
Handling Complaints						
47	Is there a process in place to respond to privacy complaints? If so, what is it?			IP		Brennan – do you think it would make sense for this to go into the Security Protocol or elsewhere?

Appendix E: Current HIFIS Retention Practices for PI

File Code	Record Series	OPR	Active	Semi Active	Final Disposition
S13-40	• Regional Homelessness Program Files	CSD	CY+2Y	3Y	SR
S13-80	• Homelessness Program Planning Reports and Studies	CSD	SO+1Y	3Y	SR
S13-90	• Homelessness Program Planning Resource and Reference Files	CSD	SO	--	D
D26-02	• Access and Supply Client Files	CSD	UT+1Y	6Y	DC