CALGARY HOMELESS FOUNDATION

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

HMIS

PRIVACY IMPACT ASSESSMENT

VERSION 2.1

Prepared with the assistance of

Excela
Associates Inc.

April 2011

Table of Contents

TERMS AND ABBREVIATIONS

Term or Abbreviation	Definition
CHF	Calgary Homeless Foundation
Custodian	An organization or individual that is subject to the *Health Information Act*.
Employee	"Employee" is used in its FOIP context, which includes paid employees, contractors, agents, volunteers and others who provide service for a public body. The term is technically limited to individuals, but for simplicity we apply it to organizations as well. Such use does not alter its FOIP implications for CHF and HMIS.
FOIP	*Freedom of Information and Protection of Privacy Act* of Alberta
FOIP agency	An HMIS agency that is subject to the FOIP Act by virtue of a funding agreement or other agreement with a FOIP public body.
HIA	*Health Information Act*
HMIS	Homeless Information Management System
HMIS agency	An agency that is an authorized HMIS user undwer the terms of an HMIS Agency Participation Agreement
HUA	Alberta Housing and Urban Affairs
OIPC	Office of the Information and Privacy Commissioner
PI	"Personal information" as defined in the FOIP Act
PIA	Privacy impact assessment
PIPA	*Personal Information Protection Act* of Alberta
PIPEDA	*Personal Information Protection and Electronic Documents Act* of Canada
Public body	An organization that is subject to the *Freedom of Information and Protection of Privacy Act*.
Subject (of PI)	The identifiable individual to which personal information relates.

1 PROJECT DESCRIPTION

1.1 INTRODUCTION

Calgary's 10 Year Plan to End Homelessness was created by the Calgary Committee to End Homelessness. Calgary Homeless Foundation (CHF) is moving forward on implementing the Plan in partnership with government partners, homeless-serving agencies, the private sector, the faith community and other foundations.

Alberta Housing and Urban Affairs (HUA) is providing conditional grant funding to CHF to assist homeless individuals to obtain housing and provide the support services and referrals required to maintain long-term housing stability. CHF will implement a city-wide Homeless Management Information System (HMIS) to support this initiative and the implementation of Calgary's 10 Year Plan to End Homelessness.

As the recipient of conditional grant funding from HUA, CHF is deemed to be an "employee" under the *Freedom of Information and Protection of Privacy Act* (FOIP Act). As such, CHF's personal information collection, use and disclosure activities described in the Outreach and Support Services Initiative Conditional Grant Funding Agreement (Grant Funding Agreement) with HUA and the use of HMIS to manage this information are subject to the protection of personal information provisions of the FOIP Act.

CHF wishes to identify and mitigate any potential privacy risks that may be associated with the implementation and use of HMIS. A Privacy Impact Assessment (PIA) is a due diligence exercise, in which CHF can identify and address potential risks to individual privacy that may occur in the course of its operation of HMIS. A completed PIA will provide documented assurance to CHF board members and staff, HUA, participating agencies and to the public that privacy requirements have been identified and addressed.

1.2 RESPONSIBLE PUBLIC BODY

HUA, as the Outreach and Support Services Initiative funder, and as described in the Grant Funding Agreement with CHF, maintains control of all personal information collected in support of the funded services.

CHF, by virtue of conditions in the Grant Funding Agreement, maintains custody of all personal information collected in support of the funded projects during the life of the agreement.

1.3 CONTACT PERSONS

The following individuals can answer questions about personal information collected, used, disclosed and managed in HMIS. Alberta Housing and Urban Affairs contacts have been included because HUA is the sponsoring FOIP public body for HMIS.

Calgary Homeless Foundation	**Alberta Housing and Urban Affairs**
Alina Tanasescu VP Strategy Calgary Homeless Foundation Phone: 403.237.6456 Email: alina@calgaryhomeless.com	Barry Bezuko Director Homeless Cross Ministry Initiatives Housing and Urban Affairs Phone: 780.643.0757 Email: barry.bezuko@gov.ab.ca
Chantal Hansen Manager Calgary HMIS Initiative Calgary Homeless Foundation Phone: 403.237.6456 Email: chansen@calgaryhomeless.com	Holly Simpson Privacy and Information Advisor Strategic Services Housing and Urban Affairs Phone: 780.638.2979 Email: holly.simpson@gov.ab.ca

1.4 PROJECT OVERVIEW

The Grant Funding Agreement enables CHF to work with community partners in Calgary to deliver services necessary to meet the unique needs of the homeless. Under the Agreement, CHF has contracted with service providers for service delivery and case management. CHF has also contracted with Bowman Systems to provide application and database services through HMIS to handle and manage the information collected, and to provide case management capability and outcomes measurement tools to address the day-to-day operations of CHF and its contracted service providers.

The Calgary Homeless Management Information System (HMIS) is a web-based, electronic client management information system that provides a standardized assessment of client needs, individualized service plans and service records. HMIS will provide real-time data on the number of homeless people, demographic and biographical information, their needs, what the causes of homelessness are, how people are interacting with our systems of care, and how effective its interventions are. A web-based application makes this type of client management information system easily available and more secure, since no client information entered into HMIS will be stored on local computers. The intake and assessment process has been standardized so that information gathered and entered into the HMIS has a standard format. At the service provider level, the assessment and information gathered will be used by case managers to provide support and by emergency shelter providers for rapid re-housing programs.

HMIS will also produce service provider-specific reports as well as aggregate information and reports that will be used by CHF and HUA to identify and address the needs of Calgary's and Alberta's homeless respectively, and to make informed decisions about their respective programs.

1.5 HMIS BENEFITS

For HUA:

Provide consistent, real-time data to assess the flow of homeless persons through services rather than within a particular program.

For CHF and service providers:

Enable the:

- development of unduplicated counts of clients served at the local level.
- analysis of patterns of use of people entering and exiting the homeless assistance system.
- evaluation of the effectiveness of these systems towards meeting ending homelessness targets.

Provide easier accessibility to client information and case files by caseworkers.

Eliminate duplication of efforts in data entry.

For clients:

Better evaluation and referral to the most appropriate support service providers through the creation of a cohesive and comprehensive case file.

2 DESCRIPTION AND ANALYSIS OF PERSONAL INFORMATION FLOWS

2.1 PERSONAL INFORMATION FLOW

The diagram in Figure 1 below depicts the service delivery process that HMIS is intended to support, with the associated flows of personal information to and from HMIS. A discussion of each numbered step and its associated PI flows follows.

1. The client initially seeks services from the agency. The client may have approached the agency individually or may have been referred by another agency. (See Agency B line.)

2. The agency requests client consent to record client PI on HMIS. This PI will only be available to the agency that collected it, unless the client consents to release to a specific other agency (see step 9).

3. If the client consents to the collection of identifiable personal information, the agency records HMIS universal data elements and selected agency-specific data elements in HMIS.

4. If the client does not consent to the recording of identifiable personal information in HMIS, the agency may record the information anonymously, using a pseudonym and false birthdate, for reporting purposes. Alternatively, the agency may choose not to record any information about the client in HMIS. In either case, service to the client will be unaffected.

5. If the agency collects identifiable or anonymous personal information in HMIS, HMIS will create a record for that client. Subsequent access to the record by other agencies will only be possible if the record is released by the initial agency (see step 9).

6. In any case, the agency will deliver services to the client. If the client is otherwise eligible for service it will not be affected by the provision or refusal of HMIS consent.

7. The agency may wish to refer the client to another agency for service as well.

8. If no such referral occurs, the agency will complete its service to the client and the process will conclude. Another, separate service process may begin if the client subsequently approaches another agency, but that service process will be unrelated to this one. If the agency involved in the second service is a HMIS agency, the process will begin again at step 1.

9. If the agency determines that a referral to another HMIS agency would benefit the client, it will request the client's consent to make client personal information in HMIS available to the other agency.

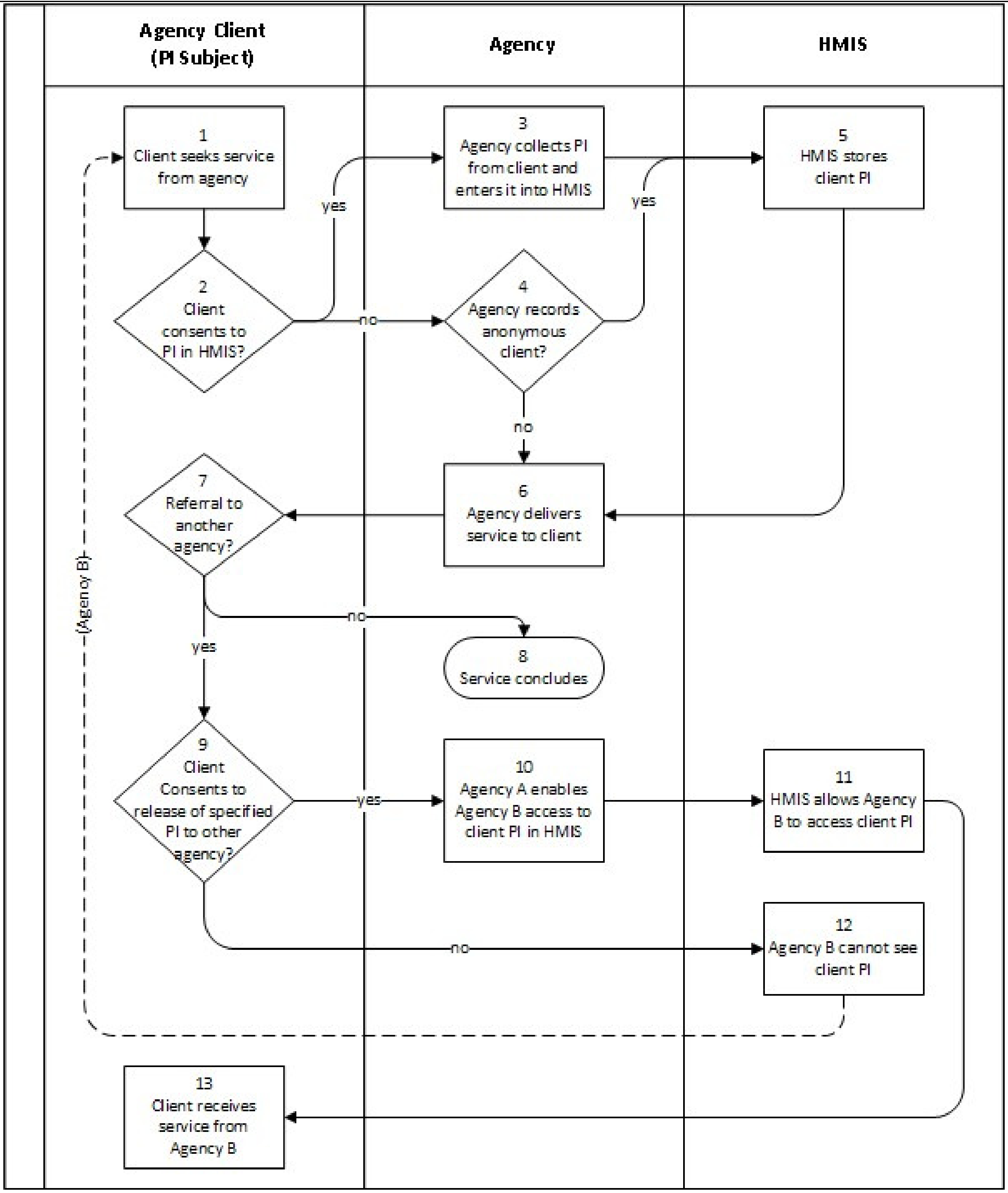

Agency Client (PI Subject)
Agency
HMIS
1 Client seeks service from agency
2 Client consents to PI in HMIS?
yes
no
3 Agency collects PI from client and enters it into HMIS
4 Agency records anonymous client?
yes
no
5 HMIS stores client PI
6 Agency delivers service to client
7 Referral to another agency?
no
yes
8 Service concludes
9 Client Consents to release of specified PI to other agency?
yes
10 Agency A enables Agency B access to client PI in HMIS
11 HMIS allows Agency B to access client PI
no
12 Agency B cannot see client PI
(Agency B)
13 Client receives service from Agency B

Figure 1: HMIS Personal Information Process Flows

10. If the client consents, the first agency will set a flag in HMIS to make that client's personal

information in HMIS available to the second agency.

11. Once the HMIS flag has been set by the first agency, HMIS will make the client's personal information available to the second agency for a period of one year. After that period, the second agency will have to renew access with the first agency each year.

12. If the client does not consent, the referral to the second agency will still occur, but the second agency will need to repeat the client's registration at step 1. Doing so will not jeopardize the client's services from the second agency, but will prevent the second agency from seeing possibly relevant service records from the first agency and will require the creation of a second, separate client record in HMIS.

If HMIS access to client personal information is available, the second agency can deliver service to the client without repeating the registration process and with information about the client's universal data elements and service transactions with the first agency.

2.2 HMIS LEGISLATIVE ENVIRONMENT

2.2.1 ILLUSTRATIONS

Figures 1 through 4 illustrate the privacy legislation framework which governs the management of personal information in HMIS.

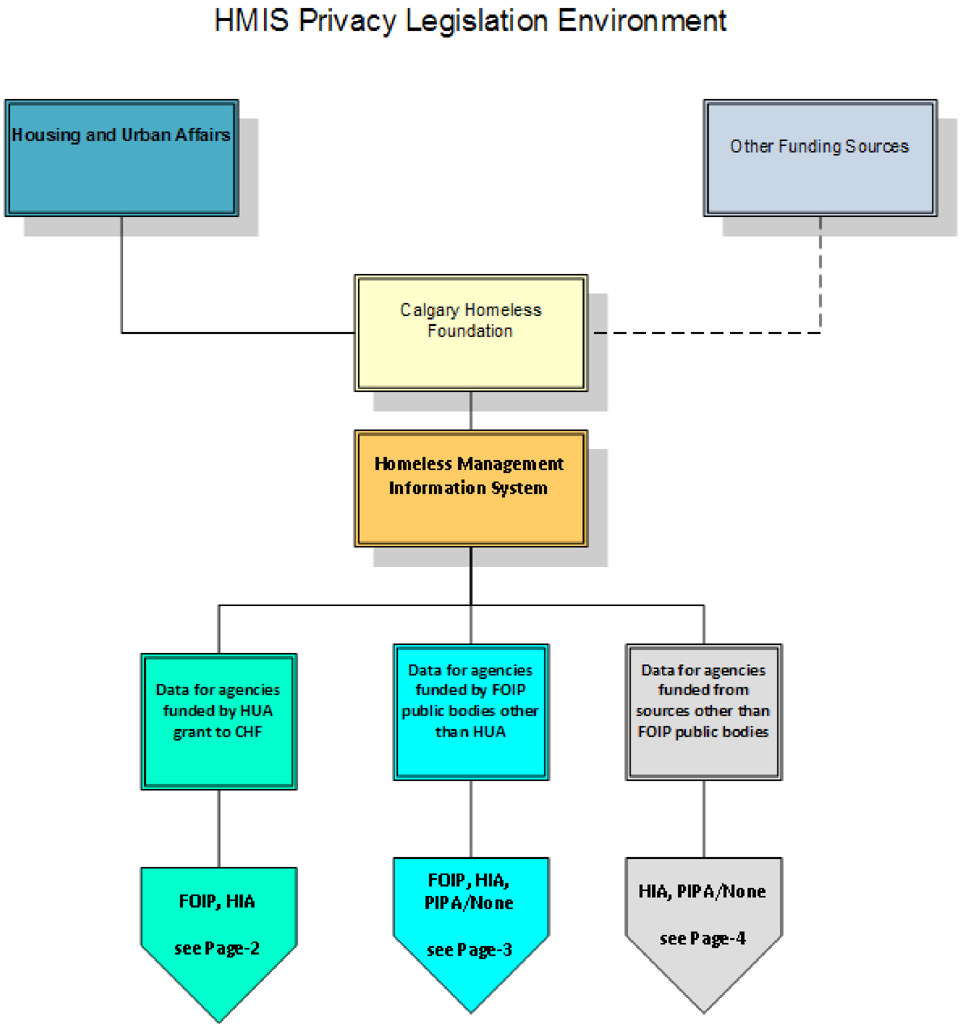

HMIS Privacy Legislation Environment
Housing and Urban Affairs
Other Funding Sources
Calgary Homeless Foundation
Homeless Management Information System
Data for agencies funded by HUA grant to CHF
Data for agencies funded by FOIP public bodies other than HUA
Data for agencies funded from sources other than FOIP public bodies
FOIP, HIA
see Page-2
FOIP, HIA, PIPA/None
see Page-3
HIA, PIPA/None
see Page-4

Figure 2: Overall Legislative Environment

As illustrated in Figure 2 above, the Calgary Homeless Foundation and the HMIS function in a complex legislative environment. The Calgary Homeless Foundation is not a public body under the Freedom of Information and Protection of Privacy Act, nor is it covered by the Personal Information Protection Act except insofar as it engages in commercial activities.

Neither the Calgary Homeless Foundation nor the agencies to which it offers the HMIS are custodians under the Health Information Act, although some such agencies may employ custodians. If they do, and if those custodians were to store health information in the HMIS, the Calgary Homeless Foundation would become an information manager under the HIA.

None of the agencies that will use HMIS are directly subject to the FOIP Act, but many are brought under FOIP jurisdiction by virtue of funding agreements with Alberta Housing and Urban Affairs or other public bodies, such as other government departments and the City of Calgary. However, the application of FOIP for these agencies could be limited by the terms of the relevant agreements with public bodies. It is also affected by the fact that such agencies provide services that are not subject to agreements with public bodies, as well as those that are.

Because of this complexity, it is necessary for the CHF to make some decisions regarding the application of legislation to the HMIS. Before we discuss those decisions, we will examine in somewhat more detail the legislative circumstances for three different scenarios:

1. The agency is subject to FOIP and the HIA.
2. The agency may be subject to FOIP, PIPA, the HIA, or no privacy legislation at all.
3. The agency may be subject to PIPA, the HIA, or no privacy legislation at all.

These scenarios are discussed in sections **Error! Reference source not found.** through **Error! Reference source not found.** below. We provide these discussions to illustrate the complexity of the privacy legislation environment in which HMIS functions. However, it is important to be clear that Calgary Homeless Foundation has made the decision that the HMIS system itself will be FOIP compliant, regardless of the legislation that applies to the agencies using HMIS.

In all cases, references to the HIA apply only if an HMIS agency employs an HIA custodian and that custodian stores health information on the HMIS. Agencies will be advised to avoid such circumstances if possible. If, however, HMIS stores health information subject to the HIA, the CHF will enter into information manager agreements with such agencies as necessary and will work with the affected custodians to complete the necessary HIA privacy impact assessments.

This PIA does not address HIA compliance, because at time of writing the HMIS did not store health information subject to the HIA and it was not the intention of the CHF to encourage situations in which it might do so.

FOIP compliance for the HMIS means that all the data elements it contains must be necessary and authorized for agencies subject to FOIP. The HMIS contains no data elements for which collection, use and disclosure is not authorized by FOIP for agencies subject to FOIP. If HMIS is used by agencies not subject to the FOIP Act, they will still be restricted to those data elements that can be authorized under FOIP for agencies subject to FOIP.

HMIS agencies not subject to FOIP must agree to voluntarily adopt PIPA as a minimum standard of privacy protection, whether or not they are subject to that Act otherwise. Such adoption of PIPA as a privacy standard is a condition of the HMIS Agency Participation Agreement.

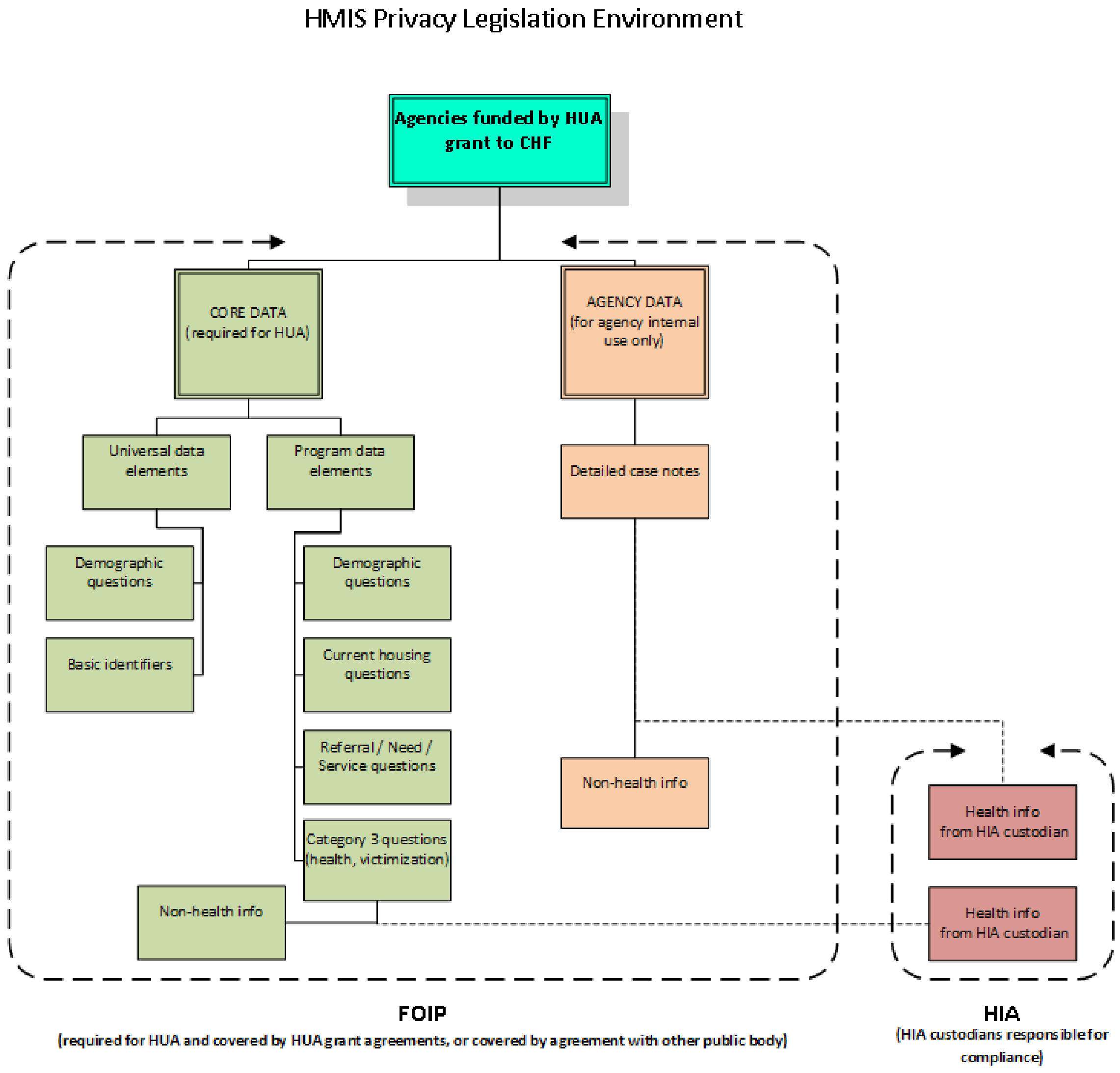

HMIS Privacy Legislation Environment
Agencies funded by HUA grant to CHF
CORE DATA (required for HUA)
AGENCY DATA (for agency internal use only)
Universal data elements
Program data elements
Detailed case notes
Demographic questions
Basic identifiers
Demographic questions
Current housing questions
Referral / Need / Service questions
Category 3 questions (health, victimization)
Non-health info
Non-health info
Health info from HIA custodian
Health info from HIA custodian
FOIP
(required for HUA and covered by HUA grant agreements, or covered by agreement with other public body)
HIA
(HIA custodians responsible for compliance)

Figure 3: Legislative Environment for HUA-Funded Agencies (Page-2)

Agencies that are funded by HUA are subject to the FOIP Act by virtue of the Act's definition of an "employee".

The diagram above reflects the stated HUA position that all data stored in HMIS by agencies funded by HUA is subject to FOIP, whether or not that data is required to be reported back to HUA. Core data are needed for reporting purposes. Agency data are not needed for reporting purposes, but are necessary to deliver the services that are funded by HUA grants, directly or indirectly. Therefore agency data are also subject to FOIP and their collection is authorized under s.33(c), since they are necessary to support the HUA programs and activities undertaken as part of the provincial homeless initiative.

The HIA applies only if health information as defined in the HIA is stored in HMIS. See section 2.2.5 for additional discussion of the application of the HIA. The application of the HIA is the same in all scenarios.

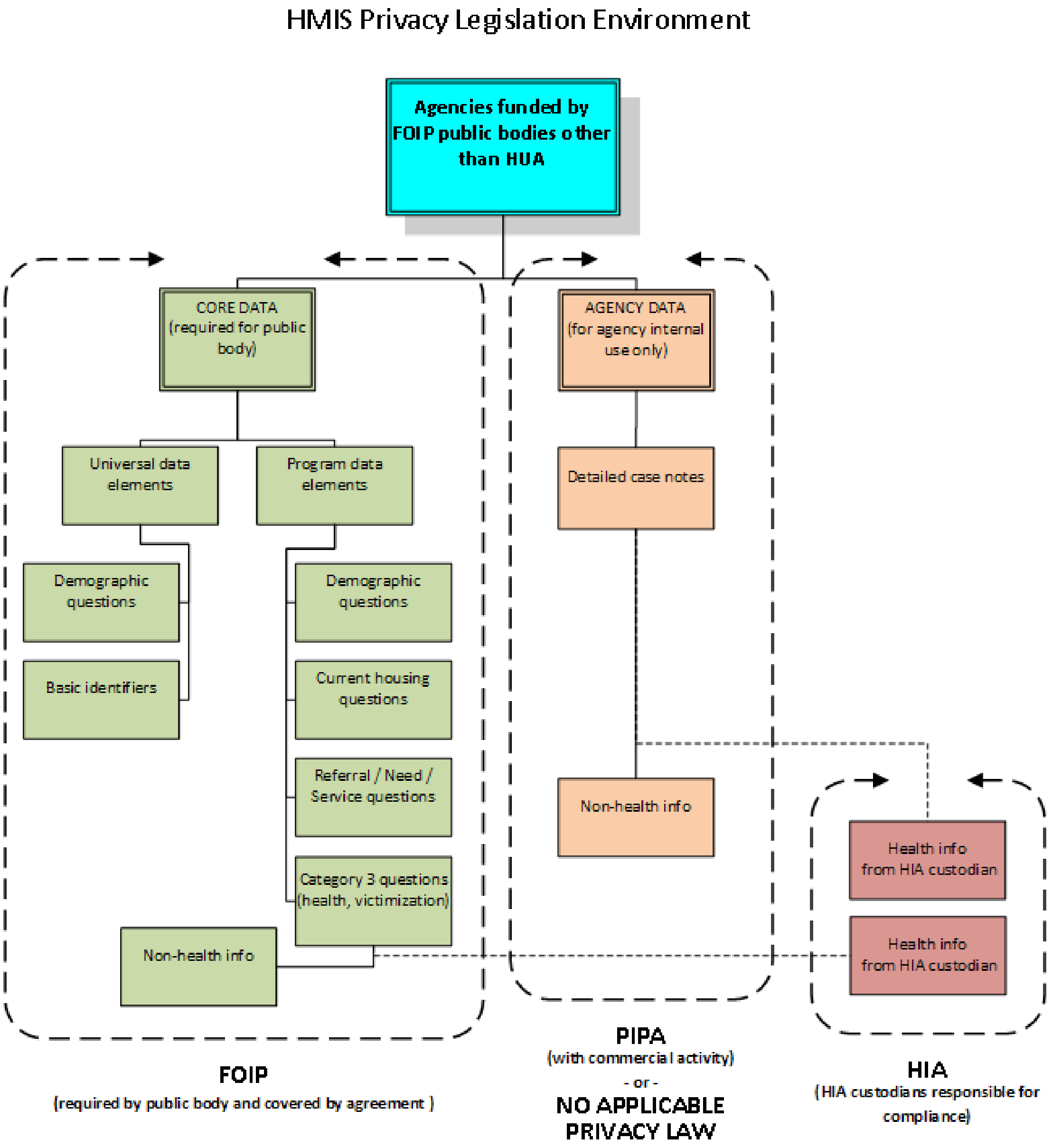

HMIS Privacy Legislation Environment
Agencies funded by FOIP public bodies other than HUA
CORE DATA (required for public body)
Universal data elements
Program data elements
Demographic questions
Basic identifiers
Demographic questions
Current housing questions
Referral / Need / Service questions
Category 3 questions (health, victimization)
Non-health info
AGENCY DATA (for agency internal use only)
Detailed case notes
Non-health info
Health info from HIA custodian
Health info from HIA custodian
FOIP
(required by public body and covered by agreement)
PIPA
(with commercial activity)
- or -
NO APPLICABLE PRIVACY LAW
HIA
(HIA custodians responsible for compliance)

Figure 4: Legislative Environment for Agencies Funded by FOIP Public Bodies other than HUA (Page-3)

As in the previous scenario, agencies that are funded by FOIP public bodies are assumed to be subject to the FOIP Act by virtue of the Act's definition of an "employee". The extent to which this is the case will depend to some degree on the terms of funding agreements between the agencies and public bodies. In the diagram above, we have assumed that such agreements would exert the control of the public body over data required by the public body, but that agency data not required by the public body would not be subject to FOIP. This would not be the case if the relevant agreements explicitly exerted the control of the public body over all agency data. In that case, the previous scenario would apply.

If there is a commercial activity related to the data, such as if the agency is paying for HMIS usage, or if the agency is not incorporated under the *Societies Act*, PIPA will apply. If the agency is incorporated under the *Societies Act* and there is no commercial activity related to the data or the services that generate them, no privacy legislation applies.

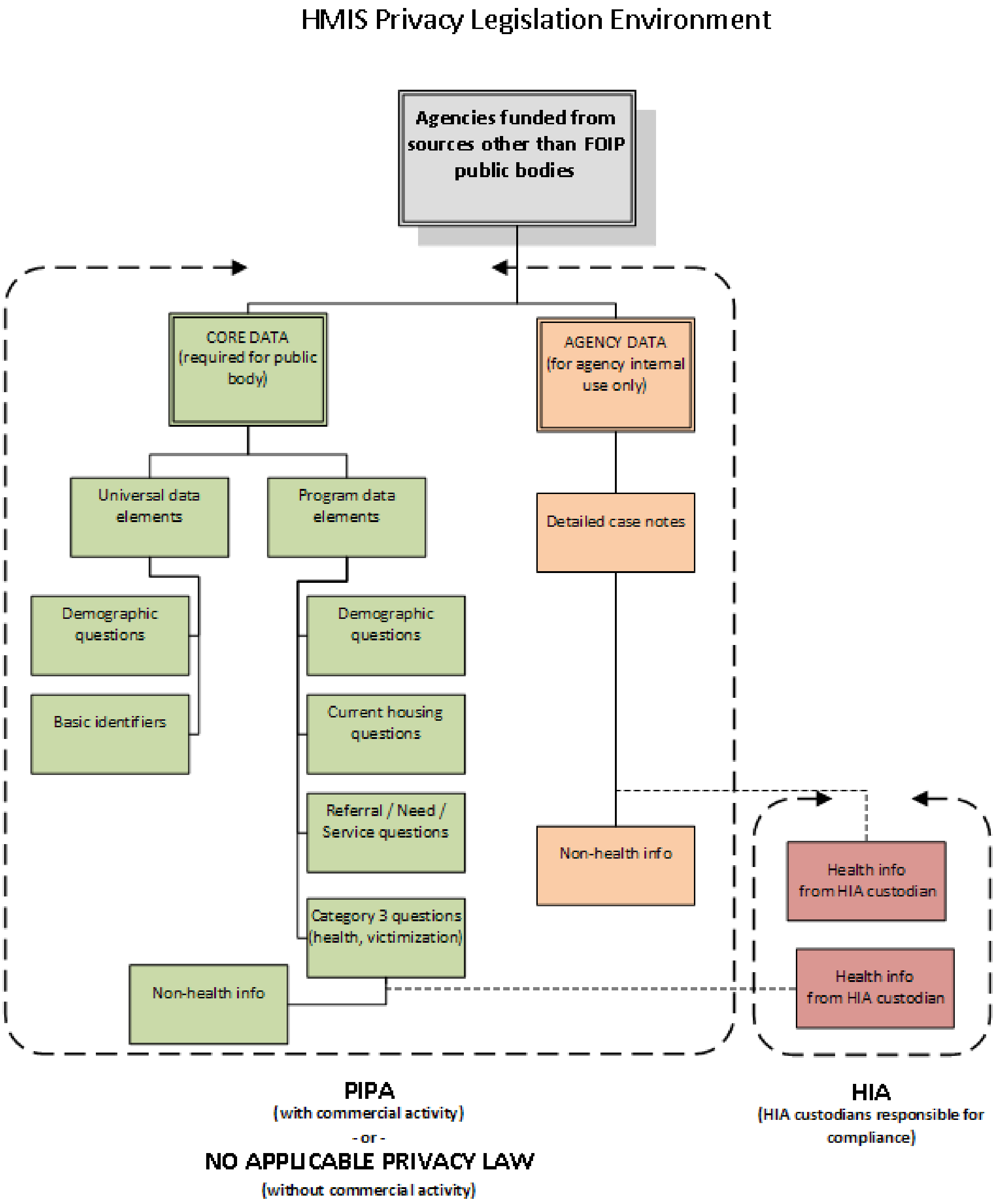

HMIS Privacy Legislation Environment
Agencies funded from sources other than FOIP public bodies
CORE DATA (required for public body)
AGENCY DATA (for agency internal use only)
Universal data elements
Program data elements
Detailed case notes
Demographic questions
Basic identifiers
Demographic questions
Current housing questions
Referral / Need / Service questions
Category 3 questions (health, victimization)
Non-health info
Non-health info
Health info from HIA custodian
Health info from HIA custodian
PIPA
(with commercial activity)
- or -
NO APPLICABLE PRIVACY LAW
(without commercial activity)
HIA
(HIA custodians responsible for compliance)

Figure 5: Legislative Environment for non-FOIP Agencies (Page-4)

In the event that the agency receives no funding from a FOIP public body and is subject to no other agreement establishing control by a public body over agency data, either PIPA or no privacy legislation applies. If there is a commercial activity related to the data, such as if the agency is paying for HMIS usage, or if the agency is not incorporated under the *Societies Act*, PIPA will apply. If the agency is incorporated under the *Societies Act* and there is no commercial activity related to the data or the services that generate them, no privacy legislation applies.

2.2.2 PERSONAL INFORMATION PROTECTION ACT

The CHF as an organization is subject to the *Personal Information Protection Act* (PIPA), but only insofar as it engages in commercial activities. Because PIPA exempts charitable organizations[1] not engaged in commercial activities, most of the activities of the CHF are not subject to any privacy legislation. PIPA applies to HMIS to the extent that CHF imposes any fees or charges for the use of HMIS[2], but only if neither FOIP nor the HIA apply as well. If they do, their application will supersede the application of PIPA.

Some agencies will be charged for HMIS seat licenses above the maximum of 10 that come with the HMIS by default. In these cases PIPA may come into effect, by virtue of the fact that the provision of HMIS has become a commercial activity. Although this interpretation of "commercial activity" is arguable in these circumstances[3], CHF chooses to assume that it is a commercial activity for PIPA purposes. However, as we note elsewhere in this report, CHF has chosen to comply with FOIP for all HMIS operations. For practical purposes, then, the application of PIPA is moot.

For the purposes of this PIA, we have assumed that HMIS agencies are charitable organizations for PIPA purposes. If not they are subject to PIPA, except to the extent that FOIP or the HIA applies.

For those HMIS agencies that are not subject to FOIP by virtue of agreements with FOIP public bodies, the HMIS agency participation agreement requires that agencies adopt PIPA requirements as the minimum standard for the protection of all personal information stored in the HMIS.

2.2.3 PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

The HMIS vendor, Bowman Systems LLC, is an American firm that is not subject to Canadian privacy legislation. However, it has contracted with an Ontario data centre to host the HMIS. That data centre is subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

CHF has a privacy schedule to its contract with Bowman (appended per section 5.5). That schedule requires that Bowman include similar provisions in its contract with the data centre operator. The data centre, therefore, is bound by PIPEDA directly and by FOIP-derived contractual requirements via the privacy schedule.

[1] Specifically, organizations incorporated under the *Societies Act*.

[2] PIPA does not define the term "commercial activity", nor does PIPEDA, from which the term originates. In general, though, any activity involving an exchange of value for value should be assumed to be a commercial activity, unless it has been shown by an OIPC or court decision not to be.

[3] It is arguable because the personal information in HMIS is not actually part of the commercial activity. The commercial activity could take place without any personal information ever being stored in HMIS. However, because the central purpose of the HMIS is the storage of personal information, it is best to assume that PIPA would apply.

2.2.4 FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

The CHF is not a public body under the *Freedom of Information and Protection of Privacy Act* (FOIP), but it receives grant funding from the Housing and Urban Affairs (HUA) department of the Government of Alberta. As such, it falls under the "employee" definition in the FOIP Act, which includes agents and contractors. If so, it is subject to the FOIP Act to the extent that the "employee" definition applies[4] via its agreement with HUA, or via any similar agreements with other FOIP public bodies.

Although CHF and its contracted service providers may be directly subject to other (or no) other privacy legislation, they are made subject to the FOIP Act by virtue of the grant funding agreement that CHF has signed with HUA. Clauses 27 through 31 and schedule D of the agreement (appended per section 5.2) outline the requirements placed on CHF and their subcontracted service providers to protect and manage personal information. They clearly bring CHF under the FOIP Act for the programs funded by HUA. Under the agreement, “custody” of the personal information is with CHF, while HUA maintains “control” of the personal information collected, used and disclosed in the programs it is funding. See clauses 27 to 31 and clause (g) in Schedule D of the HUA Agreement.

HUA officials have stated that they consider all HMIS data that come from HUA-funded organizations to be under the control of HUA for FOIP purposes. This includes detailed case notes and other personal information that would not be reported back to HUA. The HUA opinion is based in the intended effect of the agreement provisions cited above.

HUA officials have also stated that they consider any access to FOIP-governed HMIS personal information by any agency that is not subject to FOIP to be a violation of FOIP, unless there is specific case-by-case authority for the exchange of personal information. That authority would normally be derived by the written consent of the subject.

Accordingly, the FOIP Act governs all HMIS data that are provided by agencies that are funded in whole or in part by FOIP public bodies, whether that funding is direct or through the CHF. The FOIP Act applies by virtue of CHF's HMIS grant agreement with Alberta Housing and Urban Affairs and any other similar agreements with other public bodies, whether on the part of CHF or other HMIS agencies. The HUA-CHF grant agreement explicitly states that the FOIP Act applies to all information under the control of HUA because of the agreement. The grant agreement is sufficient to make CHF an employee of HUA for FOIP purposes. Any similar agreements between HMIS agencies and other public bodies have a similar effect, even if the agreements do not explicitly address it.

Furthermore, the CHF and the vendor contracted by CHF will have access to all personal information contained in HMIS for purposes of HMIS administration and technical support, regardless of whether the contributing agency is governed by FOIP. Therefore, the most reasonable course of action is for CHF to treat the entire HMIS database as being subject to FOIP. This is what CHF has decided to do.

The CHF has decided that the HMIS and all the data it contains will be managed according the requirements and procedures laid out in the FOIP Act. The responsible public body is considered to be Alberta Housing and Urban Affairs , by virtue of the grant agreement between it and the CHF.

[4] The FOIP definition of "employee" applies to individual employees of an organization, not to the organization as a whole, but for simplicity we refer to the organization.

The FOIP Act governs privacy protection by imposing specific conditions under which the collection, use and disclosure of personal information are authorized. If the HMIS is to comply with FOIP, it must have the necessary authority for collection, use and disclosure.

Because some HMIS data will be subject to FOIP and there is to be no physical separation of HMIS data that are and are not subject to FOIP, HMIS must be FOIP compliant throughout. By virtue of the CHF agreement with HUA, HUA-funded agencies rely on CHF to ensure that the vendor upholds FOIP standards for privacy and security.

Because the HMIS vendor is not directly subject to FOIP, the CHF contract includes provisions in its privacy schedule (appended per section XX) to bind the vendor to privacy and security standards equivalent to those required in FOIP. Such provisions are also extended to vendor subcontractors, especially the one that provides Canadian data centre services for HMIS.

2.2.5 HEALTH INFORMATION ACT

CHF is not a custodian under the *Health Information Act* (HIA) and is therefore not normally subject to that Act. However, it is likely that HMIS will contain "health information" as defined by the HIA. Whether the HIA applies will depend on whether the health information in question is provided by HIA custodians.

The agencies that will use HMIS are not custodians, but when recent HIA amendments go into effect they may employ custodians. Amendments to the HIA in 2010 expanded the definition of "custodian" to include members of designated health professions, including registered nurses among others. As amendments passed in 2010 go into effect, such professionals will become individual custodians under the Act, some as early as June 2011. Any such health professionals who work or volunteer for HMIS agencies will be subject to HIA requirements for their use of HMIS if they use HMIS to store health information.

If members of these professions submit health information to HMIS, then the HIA will apply to that information. Some HMIS data elements would be health information in the hands of HIA custodians. Under such circumstances, the CHF would be an "information manager" under the HIA.

Section 66(1) of the HIA defines an information manager as a person or body that:

a) *processes, stores, retrieves or disposes of health information,*
b) *in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or*
c) *provides information management or information technology services.*

RSA 2000 cH-5 s66;2009 c25 s21

As an information manager the CHF would be subject to the relevant provisions of the HIA insofar as the HMIS was concerned. Information managers are obligated to comply with the HIA generally, but the two main requirements are for:

a. an information manager agreement between the custodian and the information manager that meets the requirements set out in the regulations [s.66(2)], and

b. a PIA by each custodian addressing the role and responsibilities of the information manager [s.64].

The CHF will discourage HMIS agencies from using HMIS to store health information. HMIS is not intended to store health information subject to the HIA.

However, because some personal information on HMIS could be subject to the HIA if provided by HIA custodians[5], the possibility that such storage might occur has been recognized. This will be monitored; in the event that health information appears likely to be stored on HMIS, the CHF will work with the responsible custodian(s) to complete the necessary information manager agreement(s), privacy impact assessment(s) and related policies and procedures.

2.3 APPLICATION OF THE FOIP ACT TO THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

HUA is providing conditional grant funding to CHF to assist homeless individuals to obtain housing and provide the support services and referrals required to maintain long-term housing stability.

Although CHF and its contracted service providers may be subject to other (or no) privacy legislation in their routine activities, they are brought under the authority of the FOIP Act for this initiative by virtue of the Grant Funding Agreement that CHF has signed with HUA and the related Agency Agreements with CHF. All personal information collected, used and disclosed in support of the HUA-funded Outreach and Support Services Initiative is subject to the FOIP Act. The FOIP Act also applies to the management of the personal information stored and managed in HMIS. See section 3 of this report for a fuller analysis.

In order to determine what information would be required to deliver the HUA-funded programs, CHF established the HMIS Advisory Committee to review existing data sets, prioritization processes and common outcomes to end homelessness, and tailor these to Calgary's needs. The committee representation included funders, homeless serving agencies, researchers, clients and CHF to ensure that the data elements identified would meet both reporting and case management needs. The committee then reduced the data elements to the basic elements deemed directly related to and necessary for the operation of the funded programs.

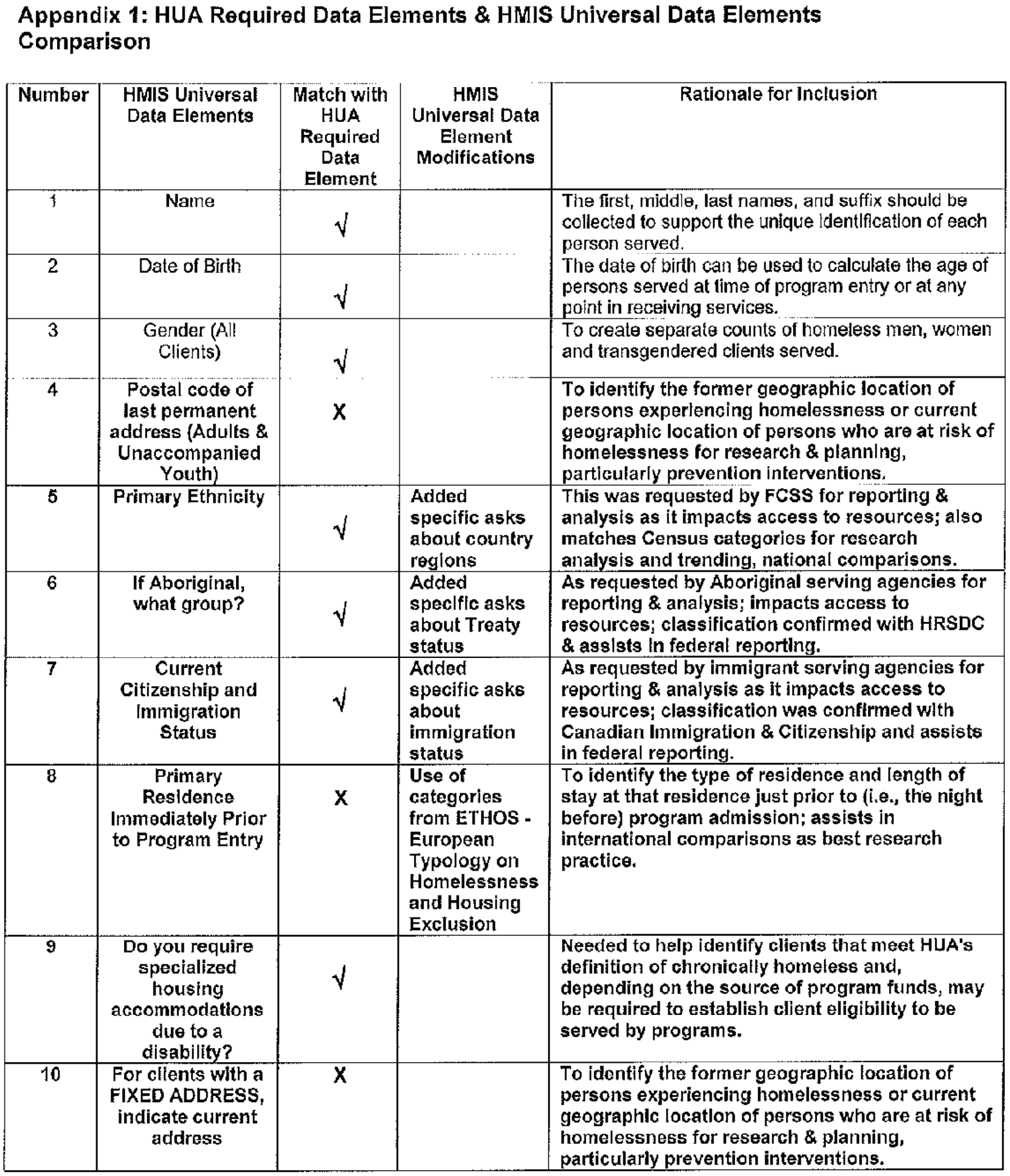
The HMIS Advisory Committee continues to meet regularly to review the data elements, discuss further information requirements and HMIS enhancements, and to consider privacy implications.

All data elements collected in support of the HUA-funded programs require approval by HUA. A complete list of HMIS data elements appears in section 5.8. (This list may exclude some data elements used by the application only for internal purposes, such as audit flags, but it includes all data elements seen by HMIS users.)

[5] HMIS may record the personal health number (PHN) or certain information about medical conditions. Case notes could also contain information about health conditions or treatments. Such information would be subject to the HIA if it was under the control of a custodian.

2.3.1 UNIVERSAL DATA ELEMENTS (UDE)

All Authorized Users on the HMIS will ask, collect, and enter the UDE into the HMIS. This information can be viewed by all authorized users.



Appendix 1: HUA Required Data Elements & HMIS Universal Data Elements Comparison

Number	HMIS Universal Data Elements	Match with HUA Required Data Element	HMIS Universal Data Element Modifications	Rationale for Inclusion
1	Name	√		The first, middle, last names, and suffix should be collected to support the unique identification of each person served.
2	Date of Birth	√		The date of birth can be used to calculate the age of persons served at time of program entry or at any point in receiving services.
3	Gender (All Clients)	√		To create separate counts of homeless men, women and transgendered clients served.
4	Postal code of last permanent address (Adults & Unaccompanied Youth)	X		To identify the former geographic location of persons experiencing homelessness or current geographic location of persons who are at risk of homelessness for research & planning, particularly prevention interventions.
5	Primary Ethnicity	√	Added specific asks about country regions	This was requested by FCSS for reporting & analysis as it impacts access to resources; also matches Census categories for research analysis and trending, national comparisons.
6	If Aboriginal, what group?	√	Added specific asks about Treaty status	As requested by Aboriginal serving agencies for reporting & analysis; impacts access to resources; classification confirmed with HRSDC & assists in federal reporting.
7	Current Citizenship and Immigration Status	√	Added specific asks about immigration status	As requested by immigrant serving agencies for reporting & analysis as it impacts access to resources; classification was confirmed with Canadian Immigration & Citizenship and assists in federal reporting.
8	Primary Residence Immediately Prior to Program Entry	X	Use of categories from ETHOS - European Typology on Homelessness and Housing Exclusion	To identify the type of residence and length of stay at that residence just prior to (i.e., the night before) program admission; assists in international comparisons as best research practice.
9	Do you require specialized housing accommodations due to a disability?	√		Needed to help identify clients that meet HUA's definition of chronically homeless and, depending on the source of program funds, may be required to establish client eligibility to be served by programs.
10	For clients with a FIXED ADDRESS, indicate current address	X		To identify the former geographic location of persons experiencing homelessness or current geographic location of persons who are at risk of homelessness for research & planning, particularly prevention interventions.

2.3.2 PROGRAM-SPECIFIC DATA ELEMENTS (PDE)

Agencies may collect some, none or all of these data elements depending on the requirements of the privacy legislation that applies to the personal information being collected. The intent is to standardize the responses for the following program-specific data elements. If the Agency has the authority under the applicable privacy legislation to collect any of the following data elements, they agree to pose questions and collect responses consistent with the PDE. For example, if agencies collect responses from the PDE, all agree to ask the questions in the same manner. This information can only be viewed by authorized users at the agency that collected the information and may only be disclosed and used under the authority of the applicable privacy legislation.

1. Provincial Health Number (PHN)
2. Household Structure/Relationship
3. Marital Status
4. Aboriginal Status Type
5. Primary Language
6. If client is NOT a Canadian citizen, what is country of citizenship?
7. If client is NOT a Canadian citizen, what was his/her arrival date?
8. Date of Calgary Residency
9. Able to produce identification?
10. Level of Education
11. Monthly Income (gross)
12. Current Sources of Income
13. Employment Status
14. If UNEMPLOYED and able to work, how many months has client been unemployed?
15. Currently attending employment-related training?
16. How many times has client lived in shelter or outside over the past year?
17. How many times has client lived in shelter or outside over the past three (3) years?
18. On average, for about how long was client in that situation each time?
19. Homeless Classification
20. Client Phone Number(s)
21. Emergency Contact Information
22. Program Entry Date
23. Program Exit Date
24. Referred for Intake by?
25. Needs Identified/Services Rendered
26. Do you have a mental health condition?
27. Do you have a physical health condition?
28. Do you have a substance abuse issue?
29. Do you have HIV/AIDS?
30. Have you ever been a victim of family violence?

2.3.3 AGENCY DATA ELEMENTS

HMIS also has case management functionality to enable service providers to enter information that would normally be recorded in the course of providing services to clients. HMIS enables service providers to collect information to support particular service delivery requirements. A caseworker, for example could input case notes, goals set with the client and other information required to manage their clients' files.

HUA will not have access to HMIS for this client-level information, but as noted in the previous section, will receive monthly downloads of anonymous individual information and as well, does have the authority to audit information collection to verify FOIP compliance.

Agency data elements are authorized under FOIP s.33(c), because they are necessary for the delivery of services by HUA funded agencies in support of the Government of Alberta's homelessness strategy, for which Alberta Housing and Urban Affairs has been given lead responsibility.

2.3.4 HUA REPORTING REQUIREMENTS

Anonymous individual information collected in support of the HUA-funded programs will be provided monthly to HUA in a download to HUA's Homeless Information Management Database (HIMD). In addition, aggregated information reports will be provided to HUA to fulfill its monitoring and evaluation responsibilities. HUA's requirements are described in clause 17 of the Grant Funding Agreement. Clause t in Schedule D of the agreement gives HUA the right to "inspect and evaluate the Recipient's compliance with the privacy, security and information management requirements under this Agreement". See section 5.3 for data elements collected on the data collection forms used by the agencies funded by HUA through CHF.

2.4 CUSTODY AND CONTROL OF PERSONAL INFORMATION

Alberta Housing and Urban Affairs (HUA) is a public body as defined in s.1(p) of the FOIP Act. All records in its custody or under its control are subject to the FOIP Act.

For the purposes of determining whether the FOIP Act applies to a record that is in the custody of a public body, custody means physical possession. For records under the control of a public body, control means the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

HUA maintains control of the personal information collected, used and disclosed in the programs it is funding under the Outreach and Support Services Initiative. Control is formalized in clauses 27 to 31 and clause g in Schedule D of the Agreement.

Under the Grant Funding Agreement, custody of the personal information during the life of the agreement is with CHF. When the agreement ends or is terminated, HUA will provide direction for the disposition of the personal information collected during the course of the program. See clause f in Schedule D of the Agreement. See section 5.2.

2.5 HMIS USERS

Only authorized users will have access to HMIS. The HMIS Agency Contact for each service provider, together with the HMIS Manager, will determine the physical access controls appropriate for the service provider's organizational settings and the service provider's HMIS users. Prior to accessing the HMIS all users must complete training and sign an HMIS User Agreement. See section 3.5.2 of this report and Standard Operating Procedures 2.8 and 5.1 to 5.3 in 5.1.

Table 1
User Matrix

Position & Job Title	User Role	Type of Access (Read, Write, Edit)	Description of Information this User Can Access
Vendor System Administrator	System Administrator	RWE	All information including client identifiable information and service provider-specific information
HMIS Manager	System Administrator	RWE	All information including client identifiable information and service provider-specific information
Executive Director	Administers service provider-specific information; able to audit service provider user access; able to enter and view client information	RWE (at the service provider-level and for any programs that fall under the service provider)	User can access all service provider profile information (necessary for service provider setup), user information, and client information that has been input by any user within the service provider or that has been specifically shared with the service provider. Can delete Agency Administrator account.
Agency Administrator	Administers service provider-specific information; able to audit service provider user access; able to enter and view client information	RWE (at the service provider-level and for any programs that fall under the service provider)	User can access all service provider profile information (necessary for service provider setup), user information, and client information that has been input by any user within the service provider or that has been specifically shared with the service provider.
Case Manager	Enters and updates client information necessary for the case management process	RWE (at the program-level)	User can access all client files that are created or updated by the programs to which the user has been given access; user will manage assessments, case notes, referrals, and service information.

Position & Job Title	User Role	Type of Access (Read, Write, Edit)	Description of Information this User Can Access
Agency Staff	Enters and updates client information necessary for the case management process	RWE (at the program-level)	User can access all client demographic information within the files that are created or updated by the programs to which the user has been given access; user will manage client demographic, services provided and service records.
Agency Volunteer[6]	Enters and updates client information necessary for the case management process	RWE (at the program-level)	User can access all client demographic information within the files that are created or updated by the programs to which the user has been given access; user will manage client demographic and referral records

[6] Although this user class refers to "volunteers", it is intended to apply to junior HMIS users generally. Such users are restricted to client data related to basic demographics and referrals. Agencies will be discouraged from giving HMIS user accounts to actual volunteers.

3 PROTECTION OF PERSONAL INFORMATION ANALYSIS

HUA, under the authority of the *Housing and Urban Affairs Grants Regulation AR 180/2009*, has a grant funding agreement with CHF to work with community partners to deliver services necessary to meet the unique needs of the homeless.

Although CHF and its contracted service providers may be subject to other (or no) privacy legislation, they are brought under compliance of the FOIP Act by virtue of the Grant Funding Agreement that CHF has signed with HUA and the individual agreements between CHF and each contracted service provider to provide services under this Agreement. HUA is bound by the requirements of the FOIP Act whether it conducts its own personal information collection activities or uses an outside agent, in this case CHF and CHF-contracted service providers, to carry out the collection on its behalf.

CHF's responsibilities are described in the Grant Funding Agreement. Clauses 27 through 31 and schedule D of the Agreement outline the requirements placed on CHF and its subcontracted service providers to protect and manage personal information collected in their activities carried out for the Outreach and Support Services Initiative. As a condition of the Grant Funding Agreement (see clause b in Schedule D) CHF in turn, uses individual agreements with each contracted service provider to ensure that protection of personal information responsibilities are explicitly made known to each service provider. As well, CHF has developed policies and standard operating procedures to provide guidelines, requirements, responsibilities, processes, and procedures governing the use of HMIS. See section 5.1.

Therefore the protection of personal information analysis below focuses on compliance with FOIP Act requirements. The analysis applies to CHF and the contracted service providers covered by the HUA Conditional Grant Funding Agreement with CHF. It also applies to CHF and CHF-contracted service providers funded by Human Resources and Skill Development Canada through the Homelessness Partnering Strategy Contribution Agreement – Community Entity Model .

In those situations in which a contracted service provider collects health information as defined under the *Health Information Act* (HIA), then that service provider must first conduct a separate PIA to address that collection before any health information is entered into HMIS.

For service providers participating in HMIS, but not funded by a public body, collection, use and disclosure of personal information will be governed by the *Personal Information Protection Act* (PIPA). See Privacy Legislation Environment figures in section 2.1 of this report.

In all cases, access by an agency to personal information in HMIS about a given individual will be limited to the information entered by that agency, unless the individual provides specific and explicit consent for disclosure by one agency to another specific agency.

3.1 PURPOSE FOR COLLECTION OF PERSONAL INFORMATION [S.33]

The personal information described in section 2.2 is being collected under the authority of the FOIP Act:

> 33(c) *No personal information may be collected by or for a public body unless that information relates directly to and is necessary for an operating program or activity of the public body.*

The authority to establish the 10 Year Plan to End Homelessness as a HUA operating program or activity and to collect information to support the 10 Year Plan comes from the *Government Organization Act*:

> 8(1) *A Minister may establish or operate any programs and services the Minister consider desirable in order to carry out matters under the Minister's administration.*
>
> 8(2) *A Minister may institute inquiries into and collect information and statistics relating to any matter under the Minister's administration.*

As noted in section 2 of this report, HUA requires CHF and the CHF-contracted service providers to provide progress reports that contain aggregate information and statistics. HUA does not require personal information collected as a result of the services provided to clients by the CHF-contracted service providers. However, the aggregate information required by HUA is derived from the collection of personal information by the contracted service providers participating in the Outreach and Support Services Initiative. These providers also need to collect additional personal information to carry out their case management activities related to the program.

3.1.1 POTENTIAL RISK(S) AND MITIGATION MEASURES ADOPTED AS A RESULT

Potential Risk: A HMIS service provider user might collect more personal information than is authorized by s.33(c) of the FOIP Act.

Mitigation Measure: Before a contracted service provider organization is granted access to HMIS, the organization must provide a list of data elements collected, the rationale for their collection, all information collection forms used to collect this information and identify legislation and agreements that may govern the service provider's collection, use and disclosure of personal information. See Standard Operating Procedures 4.1 and 4.3 in section 5.1.

Mitigation Measure: CHF and HUA approval is required before additional information described in sections 2.1 and 2.2 is entered into HMIS. See Standard Operating Procedures 4.1 and 4.3 in section 5.1.

3.2 MANNER OF COLLECTION OF PERSONAL INFORMATION [S.34]

This section of the FOIP Act establishes direct collection as the primary method for obtaining personal information. Direct information collection helps to ensure that an individual is aware of the type of personal information being used to make a decision concerning him or her. Authorized exceptions to direct collection are listed in s.34(1) of the FOIP Act.

Section 34(2) requires a FOIP notification statement when collecting information directly from a client. The purpose of the FOIP notification is to direct an individual to someone who can answer their questions about the collection and use of their personal information.

Any data entered into HMIS requires client consent, as does information sharing with another agency. For CHF-funded agencies, authorized users must obtain the client's written consent in the form of the FOIP Client Consent Form which will limit the collection and use of Client information. See Attachment J in section 5.1. For non-CHF-funded agencies, authorized users must obtain the client's written consent in the form of the Client Consent Form Basic Identifiers and the Client Consent Form for Additional Information, both of which limit the collection and use of client information. See Attachments H and I in section 5.1.

Clients may refuse to have their information entered into the HMIS. Service providers are forbidden from making service contingent on client consent to enter their information into HMIS. See Standard Operating Procedure 4.4 in section 5.1.

Throughout the information collection process, the client is reminded that his or her decision to decline will not affect eligibility for services. The Client Consent Form is scanned and attached the client's electronic file in HMIS, and the hardcopy is maintained in the organization's file. A client may withdraw his or her consent at any time by completing the Client Consent Cancellation Form. See Attachment K in section 5.1.

Each service provider will post the Privacy Notice in intake areas or in a comparable location to provide all Clients an opportunity to view the HMIS Privacy Policy. The Privacy Notice will be made available in languages and reading levels commonly understood by Clients. See Attachments E, F, and G in section 5.1.

CHF has designed materials that are intended to increase client awareness of privacy and confidentiality concerns:

1. A posted notification that all service providers will need to display in any area where client information is collected for HMIS. The HMIS Poster explains the intended uses for the information that is collected. See Attachment G in section 5.1.
2. A Client Privacy Brochure that explains how information is used, client rights and contact information for addressing questions that the client might have. See F in section 5.1.
3. The client consent forms where the risks and benefits of providing information for the HMIS are explained. The client must authorize the input of his or her information by signing the form prior to data entry. See Attachments H, I and J in section 5.1.

3.2.1 POTENTIAL RISK(S) AND MITIGATION MEASURES ADOPTED AS A RESULT

Potential Risk: A HMIS service provider user might use client consent to collect more personal information than is authorized by s.33(c) of the FOIP Act.

Mitigation Measure: Service providers are not permitted to use client consent to collect additional information. See Standard Operating Procedure 4.3 in section 5.1.

3.3 ACCURACY AND RETENTION [S.35]

This section of the FOIP Act provides that if a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete; and retain the personal information for at least one year after using it so that the individual has an opportunity to obtain access to it.

3.3.1 ACCURACY

Training is required for all HMIS users prior to accessing the HMIS and is regularly provided by the HMIS Manager. All HMIS users are expected to collect, enter, and maintain quality data in the HMIS that is timely, complete, accurate and consistent. Understanding data quality is one of the training topics covered. See Standard Operating Procedures 4.14, 4.15 and 5.1 in section 5.1.

3.3.2 RETENTION

Electronic files will be retained in accordance with s.35 of the FOIP Act. This means that records must be retained for a minimum of one year. Clause 16 of the Grant Funding Agreement and Schedule C establish the requirements for records management, retention and disposition. Records must be retained for seven years. Record disposition must be approved by HUA.

Client data contained in the HMIS are retained for seven (7) years from the last client contact. System logs of user access and records of client data releases and disclosures will be retained for ten (10) years. When data has met the retention period, the data will be archived as aggregate, de-identified information. See Standard Operating Procedure 4.13 in section 5.1.

3.4 RIGHT TO REQUEST CORRECTION OF PERSONAL INFORMATION [S.36]

The intent of this section of the FOIP Act is that if an individual believes that the information held about them is inaccurate (in error or something omitted) they have the right to ask for the information to be corrected.

Under the Standard Operating Procedure established by CHF, clients have the right to view and receive copies of their records at their request. Whenever possible, requests for changes must be supported by documented proof. Routine factual changes such as an address change or a demographic information correction may be made verbally. Where a discrepancy occurs between the client and their caseworker over information that is based on professional opinion, a written annotation must be added to the client's files indicating that the client disagrees with the information, and the client's point of view must also be documented. See Standard Operating Procedure 4.8 in section 5.1.

Potential Risk: Service providers might handle a client correction request in a manner not consistent with CHF's requirements.

Mitigation Measure: CHF has a request for correction process that all service providers must follow. See Standard Operating Procedure 4.10 in section 5.1.

Mitigation Measure: Clients have the right to submit a grievance directly to CHF if they are unable to have their concern addressed by the service provider. See Standard Operating Procedure 4.11 and Attachment L in section 5.1.

3.5 PROTECTION OF PERSONAL INFORMATION [S.38]

CHF has established policies and procedures to ensure that every organization and HMIS user understands their role in maintaining confidentiality, the impact of a breach of privacy, and how to utilize their best judgment.

3.5.1 SERVICE PROVIDER (AGENCY) LEVEL

Each service provider must make reasonable arrangements for the protection of personal information against such risks as unauthorized access, collection, use, disclosure, and destruction. Each service provider signs an HMIS Agency Agreement, confirming a commitment to adhere to all HMIS policies and standard operating procedures.

3.5.1.1 ADMINISTRATIVE SECURITY MEASURES

Administrative security measures required of service providers include the following:

- Designating a position that has overall responsibility for security within the service provider;
- Ensuring that service provider staff understand their responsibilities and the service provider's privacy measures by providing them with written procedures and instituting training programs;
- Arranging to resume operations in the case of loss of computer-based data or capabilities;
- Checking the references and background of an officer, employee or volunteer to ensure that he or she is a suitable person to have access to sensitive information, information systems and the facilities where they are located;
- Implementing the "need-to-know" principle where access to particular information or systems can be limited to certain officers, employees and volunteers who have a need for such access because it is necessary to perform their duties;
- Conducting process audits and periodically reviewing access logs, etc.; and
- Establishing sanctions for breaches of the security policy and the CHF process for reporting and investigating breaches.

3.5.1.2 TECHNICAL SECURITY MEASURES

Technical security measures required of service providers include the following:

- Using software, hardware or operating system access controls including passwords, termination on inactivity, clearance of display screens, transaction logs and error logs;
- Using secure communications and encryption, especially for mobile devices such as laptops;
- Anti-virus, anti-malware and firewall protection for new and existing computer equipment;
- Establishing security controls for remote access to information systems; and
- Conducting audit checks of data and system integrity, and establishing procedures for database recovery and back-up.

3.5.2 HMIS USER LEVEL

In addition to internal training and awareness surrounding privacy, CHF has striven to include appropriate privacy awareness and training measures. All persons who need access to HMIS as a part of their job duties will sign a User Agreement, which includes the User Policy, Roles and Responsibilities, and Code of Ethics. All users should also be familiar with the HMIS Policies and Procedures (see section 5.1). All of this information will be reinforced at software training and at User Group meetings. All User Agreements are kept on file by CHF and renewed annually; software training classes and User Group meetings are also documented and kept on file with their corresponding agendas and meeting notes.

3.5.2.1 ADMINISTRATIVE SECURITY MEASURES

Service providers are charged with ensuring authorized users who need access to the HMIS in relation to job duties have sufficient skills to use a web-based client management information system. Prior to accessing HMIS all users must complete training and sign an HMIS User Agreement. The responsibilities associated with the role of user are:

- Read, sign, and comply with the system-wide HMIS User's Agreement;
- Protect the privacy and confidentiality of client information collected and maintained in the HMIS;
- Notify the HMIS Agency Contact of all potential and actual breaches in privacy and/or security;
- Comply with HMIS Policies and Procedures;
- Collect and record all service provider required data elements;
- Create passwords that meet requirements contained in [see SOP 5.4 in section 5.1];
- Never share password and username to anyone (including other staff, supervisors, and Executive Directors); and
- Never store or display written information specifically pertaining to user access (e.g., username and password) in any publicly accessible location.
- Established organization and community-wide policies to make end-users and system managers aware of the requirements of using the HMIS;
- Required agencies to implement time-out features on local desk-tops and alter password creation standards; and
- Users receive formal training on maintaining the confidentiality of their password and not under any circumstances sharing a password.

3.5.2.2 TECHNICAL SECURITY MEASURES

User licenses will be assigned at a security level that allows no more information than needed to perform job responsibilities. As part of the User ID creation process the authorized service provider contact will determine the exact level of access an individual employee requires in order to complete their position's responsibilities. The HMIS supports a graduated layering of user privileges. While some large organizations may require multiple "Agency Administrator" access, by design each service provider will only have one user authorized to access all aspects of the service provider's authorizations. CHF has followed a similar policy internally and has only one authorized individual with system wide access. Below the "Agency Administrator" are several levels that provide access to specific sections of a case file based on job function. This segregation allows for the protection of a client's health information from access by individuals without sufficient credentials, education, or need-to-know. See User Matrix in section 2.4 of this report.

- Each individual user is provided a one-time password which is inactivated upon initial log-in, every user then chooses their own password known only to the user;
- Passwords must be altered on a 60 day cycle; every 60 days the end user is required to change their password in order to log-on;
- The HMIS automatically logs out a user that is inactive for a certain period of time; and
- The HMIS inactivates the account of any User ID that has an incorrect password entered 4 times in a row.
- The transfer of data from the server is encrypted to industry standard levels to support secure transactions between social service agencies and the HMIS server;
- Firewalls are required at service provider sites that are connecting to the HMIS;
- Data is stored in segregated network requiring multi-factor authentication for direct access;
- Personally identifying information is stored only in an encrypted format on the data server;
- All associated database and application servers are monitored and regularly audited to ensure integrity and confidentiality of HMIS; and
- Data is regularly replicated and stored off-site in the event of disaster.

3.5.3 HMIS VENDOR

The Calgary Homeless Foundation requires the HMIS vendor to uphold all of its contracted privacy and security obligations. The vendor will provide regular security status reports to CHF. The software vendor is located in Shreveport, Louisiana, United States; they will offer technical assistance to the Calgary HMIS Project Manager and will support the operations of the HMIS, as necessary. The vendor is to provide assistance only, but because of the nature of the HMIS, persons employed by the software vendor may have access to client information. The vendor is not to release or use any data from the Calgary HMIS.

The servers that house all HMIS data are located in Cambridge ON, Canada at Momentum Advanced Solutions, A Division of OnX Enterprise Solutions Ltd., 231 Shearson Crescent., Suite 104, Cambridge, Ontario, Canada L1T 1J5.

None of the data center personnel at Peer1 have access to the HMIS data, and only the IT Staff and Amy Chesney at Bowman have access to the raw data files. The servers themselves are password-protected and cannot be accessed there in Toronto without them. In addition, the servers are in a datacenter that is protected by biometric and card key access security measures.

3.5.3.1 PHYSICAL SECURITY MEASURES

- Hosting facility limits access to physical site to authorized employees and agents;
- Hosting facility verifies identities of all individuals onsite regardless of task;
- All servers and critical networking equipment is physically protected and requires key/codes;
- Server room has sufficient environmental controls to maintain humidity and temperature to optimal levels;
- Server room has requisite fire prevention and suppression system to decrease likelihood of complete systems loss; and

- Hosting facility maintains multiple connections to Internet to prevent single-point-of-failure from impacting HMIS operations.

3.5.4 BREACHES, SANCTIONS AND REVIEW

All breaches must be reported to the HMIS Manager who will report to the Audit Committee and HUA. If a breach is known or suspected, an investigation into the breach of security would be conducted. CHF has a process for reporting a privacy or security breach. See Standard Operating Procedure 4.12 in section 5.1.

If a breach is found, administrative or disciplinary sanctions will be applied. Sanctions may consist of the removal of access to sensitive information or information systems, verbal or written reprimand, suspension without pay, or dismissal. The sanction will depend on the policies of the service provider, the circumstances and the record of the officer or employee.

3.5.5 AUDIT COMMITTEE

The HMIS Audit Committee will provide oversight and recommendations to the Calgary Homeless Foundation and the HMIS Manager. The HMIS Audit Committee will review activities undertaken by the HMIS Manager with regard to operating and maintaining the HMIS and complying with the HMIS Policies and Procedures. This includes monitoring compliance with privacy protection measures via regular audits.

Once audit logs and reports have been determined and a baseline of appropriate outputs has been developed the HMIS Audit Committee will convene to review the materials on a regular basis. The audits will include the access and use of the HMIS by the HMIS Manager; access and use of the HMIS by the service provider users; and compliance with administrative and technological measures. The results of these regular audits will inform future improvements to improve privacy protection measures.

The HMIS Audit Committee will provide advice and recommendations to CHF concerning improvements and adjustments to audit policy and procedures as necessary. The committee's recommendations are not binding on CHF, but CHF will give all recommendations careful consideration.

3.6 USE OF PERSONAL INFORMATION [S.39]

Section 39 of the FOIP Act limits the use of personal information collected from individuals only for the purpose for which it was obtained or a consistent purpose; for another purpose with the consent of the individual; or, for purposes allowed under the disclosure sections of the *FOIP Act*.

The primary purposes that apply to CHF and the contracted service providers for the collection of personal information are described in clause a of Schedule D of the Grant Funding Agreement; that is:

- to provide outreach support services to clients, including case management;
- to coordinate the provision of services among service providers; and,
- to undertake research projects.

These purposes are in accordance with s. 39(1)(a) of the FOIP Act.

For all other purposes, client consent must be obtained on a consent form approved by HUA. It should be noted that client consent cannot be used to collect, use or disclose personal information in contravention of the FOIP Act. For this project, s. 39(1)(c) and s.40(1)(a) of the FOIP Act enables contracted service providers to use information considered necessary for the delivery of a common or integrated program or service.

The personal information collected in this initiative is not provided to HUA. The only information products provided to HUA are aggregated information reports which are used to fulfill HUA's monitoring and evaluation requirements as described in clause 17 of the Grant Funding Agreement.

3.7 DISCLOSURE OF PERSONAL INFORMATION [S.40]

Section 40 of the *FOIP Act* provides for specific and limited situations where public bodies may disclose personal information without specific individual consent.

The various services and activities funded by HUA through the Grant Funding Agreement are considered to be an integrated service approach [see clauses a(ii) and c in Schedule D]. This approach is in accordance with the FOIP Act:

> 40(1) *A public body may disclose personal information only*
>
> (i) *to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,*

Under the integrated service arrangement, CHF-contracted service providers under the HUA Grant Funded Agreement may disclose personal information among themselves and without client consent, with the proviso that s.39 requirements must be met (see section 3.6 of this report). It is HUA's and CHF's position that due to the nature of the information involved for participation in this program, service providers must obtain client consent prior to disclosures of personal information. This best practice has been adopted to ensure that clients are aware of how their personal information is being used, and to give them the opportunity to ask questions and deny their consent in appropriate circumstances. See Standard Operating Procedure 4.8 in section 5.1.

Disclosures of information outside of this outreach support program (i.e. to any third parties not under the grant funding agreement) are prohibited unless the disclosure is permitted with the prior express written consent of HUA under the authority of one of the provisions of s.40 or in accordance with s.42 of the FOIP Act. See Standard Operating Procedure 4.8 in section 5.1.

Individually identified client data will only be released with client permission and only then in compliance with FOIP, PIPA, and HIA, and any other applicable legislation. See Standard Operating Procedure 4.8 in section 5.1.

Aggregate reports released by CHF will not allow for the re-identification of individual clients through any means and will affirmatively ensure that data sets are sufficiently robust to avoid identification of unique individuals.

CHF is contractually obligated to provide data to funders on programs utilizing the HMIS for monitoring and evaluation purposes, CHF will include all such obligations in service provider participation agreements.

3.8 DISCLOSURE FOR RESEARCH OR STATISTICAL PURPOSES [S.42]

This section enables research to take place while at the same time ensuring that privacy is protected.

The HMIS Reporting Committee will provide guidance and recommendations to the Calgary Homeless Foundation regarding the analysis and release of HMIS data.

CHF will apply the process developed by HUA to review research requests, and use the HUA research proposal template and research agreement template to govern researchers.

The following conditions apply to the handling of research requests:

- CHF does not routinely disclose information for research or statistical purposes.
- CHF-contracted service providers must forward all research requests to CHF.
- HUA must approve a submitted research proposal and signed research agreement before any information, including personal and aggregate, can be disclosed.
- HUA must review any reports using the information collected under this initiative, prior to the release of these reports.

4 CONCLUSION

The Calgary Homeless Foundation has been working with stakeholders and HUA to ensure that all privacy requirements are met and that any potential for privacy concerns are addressed. This has included working with an advisory group of stakeholders, adjusting existing organizational policies and procedures, and establishing project policies and procedures that are ever-mindful of threats to security and privacy.

4.1 HMIS POLICIES AND PROCEDURES

CHF under the advisement of the HMIS Advisory Committee has developed the HMIS policies which include standards for HMIS Organization and Management; Participation Requirements, Data Collection; and Operation and Technical Requirements. All service providers accessing HMIS are contractually required to implement and comply with the HMIS Policies and Procedures through an executed agreement between CHF and the individual service providers. The HMIS policies are reviewed annually for continued relevance and responsiveness to statutory requirements and community needs. See section 5.1.

4.2 TRAINING AND AWARENESS

Each user who accesses the HMIS must attend training during which they are apprised of the HMIS Policies and Procedures.

The HMIS Manager will provide regular training to service provider staff on the use of HMIS. Upon completion of training, service provider staff should reasonably understand how to enter and extract data from the HMIS. Participating staff access to the HMIS is contingent on completing User Training, reading the Policies and Procedures, and submitting a signed copy of the HMIS User Agreement to the HMIS Manager.

Basic User Training Agenda:

- Introduction to HMIS;
- Review Privacy and Security Policy;
- Understand data quality;
- Discuss support request procedures;
- Logging into system;
- Record Client consent to release information;
- Enter agreed upon client and program data; and
- Produce reports.

4.3 CONTRACTS AND AGREEMENTS

CHF has developed several contracts with guidance from the HMIS Advisory Committee to regulate all parties that utilize the HMIS.

Agency Agreements

All service providers accessing the HMIS must enter into a formal agreement with CHF in the form of an Agency Agreement. The agreement ensures the service providers are aware of policies, procedures and responsibilities. Responsibilities of both CHF and the Agency service providers are stipulated in the agreement including: commitment of resources; adherence to the HMIS Policies and Procedures; and ethical data collection, use and disclosure practices.

User Agreements

All individuals with HMIS access privileges must enter into a formal agreement with CHF in the form of a User Agreement. The User Agreement ensures the user is aware of the aware of policies, procedures and responsibilities; ethical data collection, use and disclosure practices; expectations of use, and sanctions for misusing the HMIS.

Third Party Agreements

Third-party contractors, including HMIS software vendors and HMIS data hosting companies, have access to identifiable client health data in the course of implementing, maintaining, supporting and upgrading hardware and software for HMIS. As such, all third parties must enter into a formal agreement or contract indicating policies, procedures, and responsibilities and establishing expectations for compliance with the HMIS privacy requirements prior to accessing the HMIS.

4.4 DEDICATED AUDIT FUNCTION

The Information Manager for the Calgary HMIS Project is an employee of the Calgary Homeless Foundation bearing the title of HMIS Manager. The HMIS Manager manages daily HMIS operations, develops and manages HMIS resources and provides HMIS system support to HMIS Users. This person has access to all user and administrative functions and all client information. Privacy related functions of this position include:

- Manage contractual agreements between the Calgary Homeless Foundation and participating agencies;
- Provide guidance to service providers on implementing and maintaining the HMIS Policies and Procedures as needed;
- Audit access to and use of HMIS to document full participation and compliance by participating service providers;
- Monitor data quality with regard to accuracy, timeliness and completeness and notify service providers if problems arise;
- Conduct data quality assessments at a minimum each year; and if possible, more frequently;
- Conduct annual onsite data quality reviews at service providers;
- Audit compliance with the HMIS Policies and Procedures;

- Provide ongoing training on data entry, reporting, privacy practices and security requirements;
- Provide service providers with assistance to support their successful use of HMIS, including on-site support;
- Conduct end user meetings to discuss HMIS updates, data quality, reports and system use issues;
- Monitor issues related to contractual performance of the HMIS software vendor pertaining to software development, system upgrades, hosting and data protection services; and
- Monitor issues related to privacy, including conducting and reviewing Privacy Impact Assessments.

5 APPENDICES

To save paper and improve search capability, the appendices to this report have not been printed. Appendices are embedded in the Acrobat (.pdf) version of this report, which is the version we recommend because the contents of the report and most appendices are searchable (some appendices contain graphics, which are not searchable). The appendices are provided on a compact disk (CD) accompanying the paper version of this report.

The sections below provide summary descriptions and filenames for the given appendices.

5.1 HMIS POLICIES AND STANDARD OPERATING PROCEDURES

This document provides the policies and procedures governing the use of the HMIS by the CHF and all agency users. It remains in draft form at time of writing.

Filename: Draft for HMIS Policies and Procedures 4-13-2011.pdf

5.2 CHF CONDITIONAL GRANT FUNDING AGREEMENT WITH HUA

This agreement forms the basis of the funding arrangement between Housing and Urban Affairs and the Calgary Homeless Foundation that supports the HMIS. Dollar amounts are irrelevant for PIA purposes and have been severed.

Filename: HUA-CHF Funding Agreement.pdf

5.3 DATA COLLECTION FORMS

These forms are used for the collection of HMIS data by the agency from or about the client.

Filename: Data Collection Forms.pdf

5.4 HMIS AUDIT SPREADSHEET TEMPLATE

This spreadsheet lists the audit controls that Housing and Urban Affairs has required of HMIS.

Filename: CHF HMIS Audit.pdf

5.5 CONTRACT PRIVACY SCHEDULE

The Privacy Schedule lays out the privacy obligations of HMIS contractors and agencies. The schedule appearing here is the template for the agency schedule, but the same wording is contained in the privacy schedule that has been agreed to by the HMIS vendor.

Filename: Calgary HMIS Privacy Schedule D.pdf

5.6 IT SERVICE PROVIDER CONTRACTS

5.6.1 CALGARY HOMELESS FOUNDATION WITH HMIS VENDOR

This is the contract between the CHF and the HMIS vendor. Dollar amounts are irrelevant for PIA purposes and have been severed.

Filename: Bowman contract schedules.pdf

5.6.2 HMIS VENDOR WITH CONTRACTED HMIS DATA CENTRE

This is the contract between the HMIS vendor and the Canadian data centre operator that hosts the HMIS. Note that the CHF does not contract directly with the data centre operator; the HMIS vendor is responsible for to the CHF for HMIS hosting services.

Filename: Peer 1 Contract.pdf

5.7 SAMPLE HMIS SCREENS

This document contains a selection of screen images from the HMIS application.

Filename: HMIS Screen Shots.pdf

5.8 SERVICEPOINT DATA ELEMENT LISTING

Provides a listing of data elements for each database table in the HMIS. The HMIS database structure is the same as the ServicePoint application upon which it is based. This listing provides ServicePoint data elements. Accordingly, some data elements retain their original American labels, but they have been repurposed in the HMIS for Alberta purposes. For example, the data element that is used to store the Alberta Personal Health Number (PHN) is labelled as if it was storing the American Social Security Number (SSN). Also, HMIS may make little or no use of some data elements.

Filename: ServicePoint Data Element Listing.pdf