Information Sharing Guidelines

For Community Mobilization and Hubs

June 2016

Prepared by: Information Sharing Issues Working Group (ISIWG)
(Ministries of Justice, Health, Social Services, Education, Ministry of Justice, Corrections and Policing Division)

Table of Contents

I. Introduction

Government institutions, local authorities and health trustees who provide care and support to children, youth, adults and families, may need to be able to share personal information[1] and personal health information[2] within their custody and/or control with other service providers in order to mobilize resources to address individuals/families with acutely elevated levels of risk of probable harm occurring to them or their community.

Acutely elevated risk is a state where an individual (for example) is recognized to be in a position of risk to herself or himself and/or to others and that the risk is heightened to such a degree that a quick response is deemed necessary.

The appropriate sharing of personal information and personal health information assists organizations to enhance and more effectively deliver those services in a collaborative and integrated approach known as common or integrated services.

A common or integrated service delivery refers to a program designed to benefit an individual, which is delivered by one or more government institutions and may include other parties such as local authorities, trustees under HIPA, First Nations, police services and non-profits agencies.

In support of the Cabinet Committee on Children and Youth (CCCY), the Joint Policy Committee of Saskatchewan Justice and Attorney General established a working group to review and recommend improvements to inter-ministerial / inter-agency information sharing related to a cross-government response to child, youth and family issues. In particular, the working group examined examples of perceived barriers to information sharing which impede collaborative processes with the intent of improving information sharing in situations involving provision of services to children, youth and families. These particular Guidelines are focused on information sharing in a Community Mobilization Project, specifically on the Hub component of the project.

These Guidelines may be used by any organization preparing to enter into a common or integrated service delivery model but are particularly applicable to government institutions subject to *The Freedom of Information and Protection of Privacy Act* (FOIP), local authorities subject to *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP) and health trustees subject to *The Health Information Protection Act* (HIPA).

These Guidelines reflect the legislative environment as of June 1, 2016 and may be updated from time to time as needed to reflect changes in legislation, best practice or policy.

---

[1] As defined at section 24 of *The Freedom of Information and Protection of Privacy Act* and section 23 of *The Local Authority Freedom of Information and Protection of Privacy Act..*

[2] As defined at section 2(m) of *The Health Information Protection Act.*

II. Purpose

Ensuring appropriate, collaborative and holistic service delivery in a community-based environment is the primary reason for the development of these *Information Sharing Guidelines.* These Guidelines not only support the delivery of integrated services by assisting service providers to understand their privacy obligations when meeting the needs of children, youth, adults and families, they also comply with the principles and requirements of existing privacy legislation*.*

Specifically, the Guidelines are intended to:

- provide information about privacy rules and best practice to be followed before sharing information about children, youth, adults and families for common or integrated service delivery among public sector and service provider organizations;
- support a common or integrated approach to service delivery for individuals and families in situations where acutely elevated risk must be addressed by strengthening the ability to share information;
- enable effective mobilization of supports and services by public sector and service provider organizations, including the ability to collectively plan short-term and long-term interventions; and
- prevent the unnecessary sharing of identifiable information in situations where doing so would not be supported by legislation or policy.

III. Vision

Appropriate cross-sector information sharing in support of integrated assessment, planning and service will lead to more beneficial and achievable outcomes for children, youth, adults and their families.

The information sharing vision is based on the following principle:

- Saskatchewan residents' privacy rights as set out in legislation must be respected when their information is shared in a common or integrated service delivery context.
- Children, youth, adults and families benefit from a common or integrated approach to planning and service delivery.
- Legislation permits the sharing of information within certain guidelines and parameters.
- Children, youth, adults, families, and public sector and service provider organizations including government ministries, local authorities and trustees of personal health information have access to clear, easy-to-understand guidelines for cross-sectoral information sharing.

- Children, youth, adults and families are involved in, informed of and, whenever possible, consent to plans and services that involve them.

IV. Principles

The following principles provide direction for sharing information related to providing services and supports to children, youth, adults and families.

Respect for Privacy —The right to individual privacy of children, youth, adults and families must be respected. Only the minimum and necessary amount of personal information and personal health information may be shared and only with those service providers that must be engaged in order to effectively deal with the situation at hand. Information must only be shared within the boundaries of existing legislation.

Consent Based — Consent to share personal information and personal health information is a central component of access and privacy legislation. Obtaining consent should be the goal in every situation where information is shared. It is recognized that in situations dealt with by common or integrated services where acutely elevated risk necessitates the sharing of information, it may not always be reasonable to obtain consent at the outset.

Informed consent from the individual or their parent/guardian where appropriate, is the preferred method of enabling the sharing of information among professionals and service providers and should be sought wherever possible. "Deemed consent" may be relied up where it is legislatively authorized and circumstances will exist where information may be shared without consent in accordance with legislation[3].

Government institutions, local authorities and health trustees should be aware of the consent requirements of applicable statutes and in particular know whether written or verbal consent is required or whether an implied or deemed consent is applicable.

Coordinated Services and Supports — Children, youth, adults and families are better served when their needs and the resources required to meet those needs are considered and provided using a coordinated approach, rather than in isolation.

"Need to Know"—In a common or integrated services setting, agencies should only disclose and collect personal information or personal health information on a "need to know" basis. A basic operating principle should be to only disclose or share the minimal information needed to achieve a purpose and to only share that minimal information

[3] An example is in HIPA: 27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

(a) where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person

with those who need to know it in order to achieve the purpose. Discussions should involve only de-identified information initially. Agencies should record information only to the extent they are involved in addressing acutely elevated risk factors; if they do not have a role to play in addressing acutely elevated risk, agencies should not record any information.

Information sharing in a need-to-know context enables the mobilization of agencies that have a role to play in the situations discussed, so that the acutely elevated risk factors can be countered by immediate, coordinated and integrated responses.

Transparency — Children, youth, adults and families should understand what information about them will be shared, why it will be shared and how..

Right of Access and Correction – Individuals whose personal information or personal health information is collected by government institutions, local authorities or health trustees have a right of access to those records and can request that corrections be made.

V. Information Sharing

Government institutions, local authorities and health trustees provide care and support to children, youth, adults, and their families. These organizations often need to share personal information and personal health information within their custody and/or control with other service providers in order to enhance and more effectively deliver those services in a common or integrated service approach.

Various pieces of Saskatchewan legislation apply to information sharing situations, including:

- *The Freedom of Information and Protection of Privacy Act* (FOIP)
- *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP)
- *The Health Information Protection Act* (HIPA)
- *The Child and Family Services Act*
- *The Youth Drug Detoxification and Stabilization Act*
- *The Public Health Act, 1994*
- *The Correctional Services Act*
- *The Correctional Services Act, 2012*

Additionally, federal privacy legislation must also be considered in certain situations, including the:

- *Privacy Act*
- *Access to Information Act*
- *Personal Information Protection and Electronic Documents Act* (PIPEDA)

- *Youth Criminal Justice Act* (YCJA)

The relevant provisions are attached as Appendix 1 to these Guidelines.

VI. Guideline Directions

A: Sharing Information in an Integrated Service Context

Care must be taken to ensure that information sharing is required before any information is shared in a common or integrated service context. The originating agency must determine that the need(s) or risk level that must be addressed are beyond the scope of acting on its own or through normal, established processes. Once that determination is made, however, information sharing within the appropriate legislative and policy parameters may take place within an integrated service approach and the delivery of services to children, youth, adults and families will be facilitated. Information sharing, however, must still only take place where privacy legislation authorizes doing so.

Saskatchewan now has a set of regulations[4] to allow for the disclosure of personal information and personal health information for the purposes of carrying out common or integrated service, defined in the regulations as:

> "a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:
>
> i. another government institution;
> ii. a local authority;
> iii. a trustee as defined in The Health Information Protection Act;
> iv. a First Nation;
> v. a police service or regional police service as defined in The Police Act
> vi. the Royal Canadian Mounted Police;
> vii. a non-profit organization that provides a service of the type to be included in the common or integrated service;
> vii. any other agency or organization that the Minister determines is appropriate"

[4] *Freedom of Information and Protection of Privacy (Information Sharing Agreements) Amendment Regulations, 2016*
Local Authority Freedom of Information and Protection of Privacy (Information Sharing Agreements) Amendment Regulations, 2016
Health Information Protection (Information Sharing Agreements) Amendment Regulations, 2016
The Youth Drug Detoxification and Stabilization (Information Sharing Agreements) Regulations, 2016

The amendments are intended to facilitate the disclosure of essential personal information and personal health information between government institutions and third party agencies that are delivering common or integrated service programs with or for the provincial government.[5] The amended regulations authorize information sharing for the purposes of programs like Hubs and other multi agency programs.

To achieve this, the following regulations have been amended effective June 1, 2016:

- *The Freedom of Information and Protection of Privacy Regulations;*
- *The Local Authority Freedom of Information and Protection of Privacy Regulations;*
- *The Health Information Protection Regulations* and
- *The Youth Drug Detoxification and Stabilization Regulations*

As common and integrated programming generally involves the collection, use and disclosure of both personal information and personal health information, the regulations were passed as a package and work together to provide the structure and rules for information sharing to take place for common and integrated programming.

The collection, use and disclosure of personal information and personal health information is complex. In addition to the regulation amendments, various privacy legislation authorities allow participants in an integrated service to share personal information and personal health information. Government institutions, local authorities and health trustees must consider and observe applicable privacy laws before entering into new common or integrated service models. Agencies in this context should ensure that their representatives are fully aware of their privacy obligations and that their policies and procedures adhere to applicable legislation.

In particular:

- Government institutions must consider Part IV of *The Freedom of Information and Protection of Privacy Act* if personal information is to be shared, that appropriate authority exists to collect the information (sections 25 and 26), that they follow rules regarding accuracy (section 27), that they use and disclose the information according to the Act (sections 28 and 29), and that individuals are given access to records about themselves and are able to make corrections to their information (sections 31 and 32).
- Local authorities must consider Part IV of *The Local Authority Freedom of Information and Protection of Privacy Act* if personal information is to be shared, that appropriate authority exists to collect the information (sections 24 and 25), that they follow rules regarding accuracy (section 26), that they use and disclose the information according to the Act (sections 27 and 28), and that individuals are given access to records about themselves and are able to make corrections to their information (sections 30 and 31).

[5] These changes do not deal with information sharing issues associated with information governed by the section 74(1) of The Child and Family Services Act; this will require an amendment to the Act itself.

- Health trustees (including government institutions) must consider *The Health Information Protection Act.* Of particular interest should be Parts II, III, IV and V and especially sections on need-to-know (section 23), collection (section 24 and 25, use (section 26) and disclosure (sections 27, 28 and 29) of personal health information.

Agencies subject to *The Freedom of Information and Protection of Privacy Act* may be able to disclose personal information in their possession or control under the following provisions of FOIP:

- For the purpose the information was collected or a consistent purpose [FOIP: 29(2)(a)]
- To the police on their request for the purpose of enforcing a law or carrying out a lawful investigation [FOIP: 29(2)(g)]
- Where necessary to protect the mental or physical health or safety of a person [FOIP: 29(2)(m)]
- Where disclosure may reasonably be expected to assist in the provision of service for the benefit of the individual to whom the information relates [FOIP Regulations: 16(c)];
- To an officer as defined in *The Child and Family Services Act* for the purpose of managing case files, including carrying out an investigation pursuant to *The Child and Family Services Act* [FOIP Regulations: 16(r)];
- With consent.

Personal health information may be disclosed with consent. In addition, consent is deemed to have been provided in a number of situations as set out in *The Health Information Protection Act*:

- for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose [HIPA: 27(2)(a)];

for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject Individual [HIPA: 27(2)(b)]provided the requirements in s. 27(3) regarding policies and ethical practices are met.

In addition, a trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

- where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person[6] [HIPA: 27(4)(a)];
- with some restrictions[7], where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee,

[6] In the November 21, 2007 Report H: 2007-001, the Office of the Information and Privacy Commissioner determined that the following criteria apply in this context: a) must be a reasonable expectation of probable harm; b) harm must constitute damage or detriment and not mere inconvenience and c) must be a causal connection between disclosure and the anticipated harm. Please see page 24 for more detail.

disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent [HIPA: 27(4(j)]; or

- for other purposes provided for in sections 27, 28 and 29 of the Act.

Similar abilities to share information are contained in other laws. Ministries and agencies participating in common or integrated services should ensure that those laws applicable to them are understood and observed. Relevant portions of these laws are appended to these Guidelines in Appendix 1.

B: Integrated Service Delivery Forums

The term 'common or integrated service delivery' is widely used across all human services and it can connote a variety of approaches. In the context of these guidelines, this term refers specifically to specially convened forums wherein professionals from a variety of human service sectors come together for the purpose of identifying the need for, and developing immediate plans for, multi-agency interventions. These forums and their resulting interventions are intended to reduce acutely elevated risk situations that if left unattended, are deemed by the professionals involved to be highly likely to create imminent harm to individuals, families or the community. A prime example of this type of forum is the Hub, currently operating as part of Community Mobilization Prince Albert (CMPA). Their website can be accessed for additional information. It can be found at:

http://www.mobilizepa.ca/

A number of other Hubs have been established in other areas of the province, built off the established CMPA model.

A Hub is a discussion between multiple agencies that may include government institutions, local authorities, health trustees, police services, First Nations and community-based organizations in the human services delivery sector taking place on a regular basis. It is typically a discussion and does not have any actual case management role or authority. The case management and the actual service delivery fully remain with the agencies. The discussion focuses on providing immediate coordinated and integrated responses through mobilization of resources to address situations facing individuals, families or environments with acutely elevated risk factors, as recognized across a range of service providers.

[7] HIPA: 27(6) requires that the person receiving disclosure in this context must agree to use the information for only the purpose for which it was disclosed and not to make a further disclosure in the course of carrying out any activity.

The purpose of the integrated service delivery meeting is to discuss situations where there is an acutely elevated risk to an individual or the community and to mobilize existing resources with the expectation that early intervention can help the individuals / community in question with the intent of reducing the possibility of the situation worsening to the point where more significant problems emerge, including more formal interventions from police, social services, etc.

It is expected that an agency only brings those situations to the discussion that it has determined involve risk factors outside its own scope or usual practice, and thus represent situations that could be much more effectively addressed in a multi-agency manner. The agency must therefore examine each situation carefully and internally come to the conclusion that the risk(s) posed by situation are serious and urgent enough to take to the Hub for discussion there. These situations are relatively exceptional, with significantly more handled internally than that are taken to the Hub. Criteria that can be taken into account at this stage include:

- The nature of the presenting risk(s)
    - Is the presenting risk of such concern that the individual or family's privacy intrusion justified by bringing the situation to the Hub for discussion?
    - Are the risk factors higher than what can reasonably be considered the norm?
    - Is there a reasonable expectation of probable harm if nothing is done?
    - Would that harm constitute damage or detriment and not mere inconvenience to the individual?
    - Is it reasonable to assume that disclosure to the Hub will help minimize or prevent the anticipated harm?
    - Are these risks applicable across multiple agencies?
    - Is it beyond the agency's scope or mandate to mitigate the risk alone?
- The agency's experience with the subject individual or family
    - Did the agency bringing forward the situation do all it could to mitigate the risk?
    - Were the agency's traditional/standard/levels/options exhausted?
    - Can one agency appropriately mitigate the risk alone? A multi-agency approach is required to appropriately mitigate the risk.
    - Does the complexity of the situation warrant Hub discussion and multi-agency involvement?

Part of the Hub discussion is the identification of specific tasks to be undertaken by agencies in order to address the risk. The tasks are identified by the participating agencies based on the nature of the situation and the discussion. In follow-up discussions, if the initial intervention did not reduce the risk to an acceptable level, the

agencies review the tasks and their progress to determine if the risk has been appropriately met by the intervention or if more tasks need to be undertaken. The bulk of the meeting is focused on the discussion of the risk situations.

Typically, a situation will stay open for as short a time as possible. The intent is to deal with a situation as soon as possible after discussion with the hope that the matter can be closed at the next meeting or at a meeting soon after. As each situation is reviewed during a meeting, the outstanding actions are reviewed and if completed are closed. If the situation of acutely elevated risk remains and new actions are identified, they are bookmarked to be done within days and will be reviewed at a future meeting.

Once the existing situations are discussed, new situations are introduced. This is done in a roundtable format – the discussion moves around the room allowing any person at the table to propose a new situation. Situations are introduced and discussed in a staged approach designed to minimize disclosure of personal information to the participating agencies that need to be involved in resolving the situation. Introduction of a new situation begins using non-identifiable information only. Limited identifiable information is introduced into the discussion only as necessary to determine actions as outlined in the four filter process. This process is described more fully later in these Guidelines.

C: Acutely Elevated Risk

Key to sharing information in a Hub context is the need to strike a balance between an individual's right to privacy with the benefits of the reduction of acutely elevated risk. Acutely elevated risk describes a state where an individual (for example) is recognized to be in a position of risk to herself/himself and/or to others and that the risk is heightened to such a degree that a quick response is deemed necessary. Before bringing a situation to the Hub discussion, each agency should reach the conclusion that a state of acutely elevated risk exists. The agency will seek confirmation of this in initial Hub conversations.

The agencies involved in the Hub discussion help determine whether given the de-identified personal information there are services, programs, etc., their agency can provide to the individual and whether a multi-agency approach is appropriate (i.e. whether more than one agency should be involved). These services, programs, etc. may be aimed at current risks or aimed at preventing a risk or harm that seems probable given the information provided.

Given the amount of agencies involved in a Hub discussion and that every individual is unique, several criteria are used to determine if acutely elevated risk is present in the situations discussed:

- Significant interest at stake - Important interests that justify and or require

discussion of the situation such as when a child is in need of protection or when there is reason to believe there is an imminent risk of serious bodily harm or death to an identifiable person or group.

- Probability of harm - There is a reasonable expectation of harm to individuals if nothing is done.
- Significant intensity of harm - The harm would constitute damage or detriment and not mere inconvenience to the individual. It is reasonable to assume that disclosure to the Hub would help minimize or prevent the anticipated harm.
- Multidisciplinary nature of risk - The risk factors are beyond the Originating Agency's (i.e. the agency bringing the situation forward for discussion) scope or mandate to mitigate the elevated level of risk. Operating risk factors cut across multiple human service disciplines. Traditional inter-agency approaches have been considered or attempted.

D: The Four Filter Approach: Working towards Minimal Data and Need to Know

As important as the type of information that is shared at a common or integrated service, with whom that information is shared is just as important. It is recommended that common or integrated service providers adopt a four filter approach to the sharing of information in order to be able to meet privacy expectations. The filters:

- Guide discussion where acutely elevated risks exist;
- Minimize the identifiable personal information and personal health information that is disclosed to the discussion;
- Limit the agencies to which more detailed personal and personal health information is disclosed; and
- Limit the recording of identifiable information – i.e. only agencies with a role to play record identifiable information and no identifiable information is recorded in the central records of the integrated service.

This is the approach that has evolved at CMPA with considerable success. The *Privacy Impact Assessment* that was revised respecting that program in April 2016 and describes the process as follows:

Four Filter Process

The Hub has developed this four filter process to attempt to minimize the risk of inappropriate or unnecessary data sharing and to ensure participation in the discussions on a need to know basis. The four filters help minimize the need to share identifiable personal information and personal health information except where it is agreed that a situation meets the definition of an acutely elevated risk where harm to one or more individuals was a potential outcome if no action was taken and the situation was something that a Hub discussion may be able to help address. This process was created partly in response to risks identified through conducting a Privacy Impact Assessment and discussions with CMPA.

Information is introduced to the Hub discussion through the four filters in a staged manner in an effort to minimize data collection, use and disclosure and to limit disclosure to only those agencies that may have a need to know certain information when dealing with specific circumstances.

Filter One

Each individual agency is responsible for its own Filter One screening processes. Information is introduced to the Hub discussion by the participating agencies only once the agency has determined that the risk factors are beyond its scope/mandate to mitigate and all traditional approaches have been exhausted. Once an agency has identified a situation it considers to meet the requirements for discussion, the initial disclosure of information to the Hub discussion will occur in Filter Two.

Filter Two

The initial disclosure to the Hub discussion is limited to de-identified information. The agency will describe the risk factors in generic terms to enable the discussants to:

- help assess if the situation warrants a Hub discussion (respectively meets the threshold of acutely elevated risk also in filter two); or,
- determine if no Hub discussion is warranted because further effort should appropriately be made by the originating agency (perhaps with the help of one or more other agencies at the table).

Information disclosed at this time may include the following:

- Age group (e.g. Child 0 to 11, Youth 12 to 17, Adult 18+ and Senior 65+);
- Gender;
- Short description of the risk situation (i.e. risk factors such as drug use, gang association, truancy and how they come into play); and
- In so far as necessary to demonstrate that filter one was executed appropriately, the efforts made by the agency to resolve the situation.

A Glossary of Risk Factors has been developed by CMPA and the Building Partnerships to help define the risk factors more precisely. These risk factors are reflected in the Common Referral Form contained in Appendix 2.

If the circumstances do not meet the threshold, no personal information or personal health information is disclosed and the situation is not addressed at the Hub discussion (rejection in filter two). However, in some circumstances a situation meets filter two and gets rejected only in Filter Three once identifiable information is shared (Filter Three rejection).

Filter Three

If it is determined that a discussion at the Hub is warranted, limited personal information and personal health information may be included at this stage if necessary to help determine who should continue to be part of the discussion. Generally, the identifiable information introduced at this point is:

- Name;
- Actual Age; and
- Other limited information to allow other agencies to determine if they are already involved with this person.

If another agency knows the individual, they may at this time disclose aspects of their relationship in order to help determine if they or others may have a role to play in remedies or actions to be decided upon or if they have information that will show that the situation should be rejected. Information disclosed at this point may include:

- Known relevant facts about the individual being discussed such as:
    - If he or she is known to another agency;
    - General information on involvement with the individual if it is relevant to the decision if the situation needs to be accepted or rejected and/or if it is relevant with regards to identifying the agencies that need to be involved (e.g. information on additional risks).

Disclosure throughout this exercise is still limited as the group actively tries to satisfy the need to know principle.

By the end of this stage, it will be determined if the discussion will continue and which agencies need to be involved in the continuing discussion.

Filter Four

By this point most of the agencies have been eliminated from participating in further discussions. Typically three or four agencies (including the lead agency) will remain in the discussion – e.g. Social Services, a School Division and the Regional Health Authority; or Social Services, the Regional Health Authority, a School Division and the Prince Albert Police Service.

Additional personal information and personal health information may be disclosed at this point so that the participating agencies can better determine the actions that can or should be taken. Information eventually shared at the group can include:

- Name, age, address of the youth, adult, etc. e.g. 13 year old girl,
- Known facts, concerns – e.g. doesn't attend school regularly, frequent drug user, suspected hush pregnancy, etc.
- Relevant family circumstances, family connections – mother is user, husband in jail, etc.

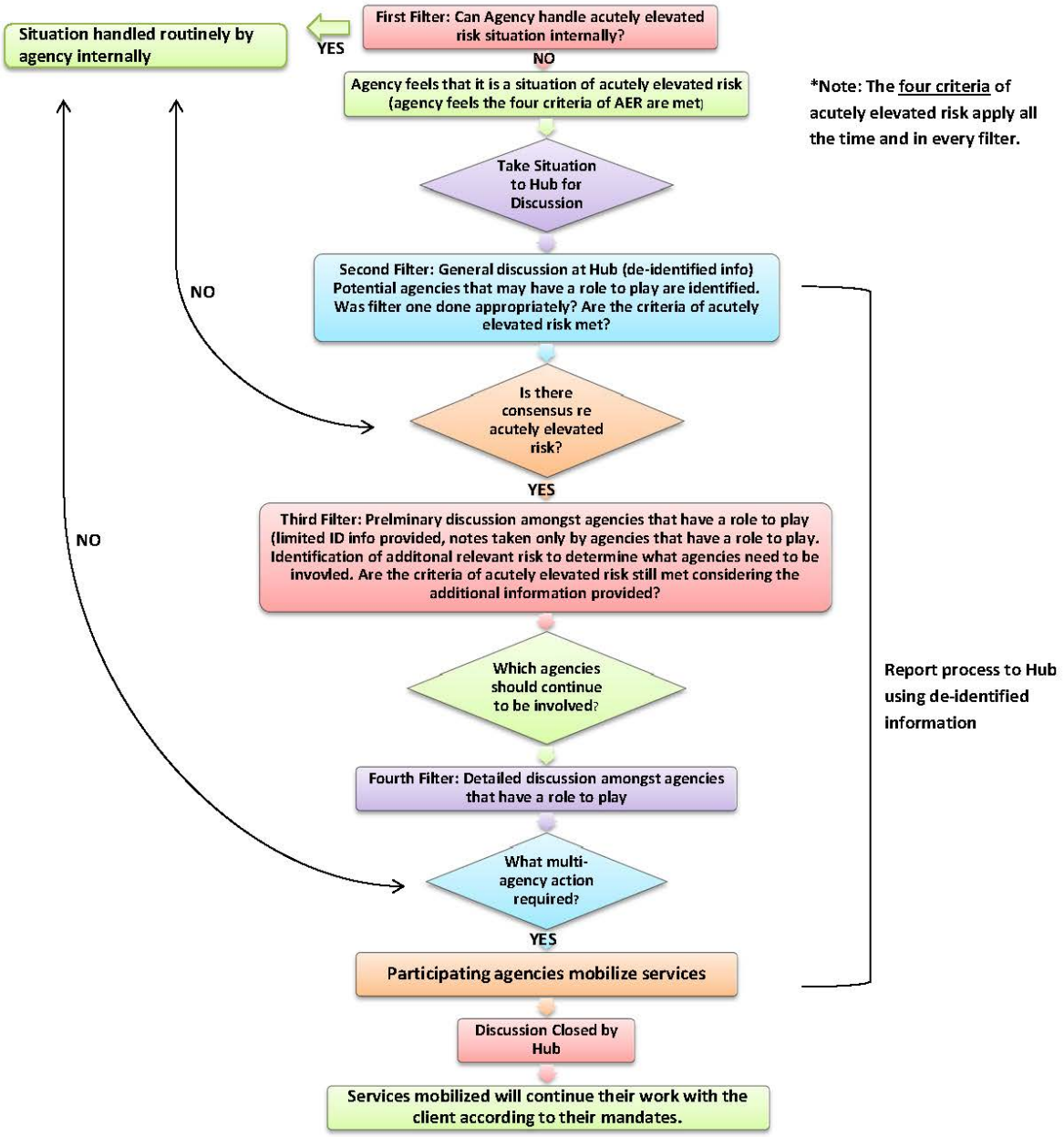
Actions taken can include a "door knock" or visit to an individual or family deemed to be in need of services. At that time an invitation for services is offered and, if accepted, the services are then provided by the individual agencies as part of their normal business, though usually with more inter-agency cooperation than what might otherwise be provided.

If at any point in the above, it becomes evident that resources are currently being provided within existing agencies and the Hub is confident elevated risk is being mitigated, the Hub discussion is closed.

A Common Referral Form and corresponding Instruction Guide outlining the components associated with each filter to guide the participant through the four filter process is attached in Appendix 2. This referral form should be the agency's internal record of each discussion and the form itself is not shared with the Hub or other Hub participants. The RCMP utilizes a similar referral form.

The flowchart on the following page shows how the filters are applied:

Hub Decision Making Flow Chart



E: Record Keeping, Data Entry, Retention and Storage

In accordance with their legislative authority and policy, records are kept by the individual agencies as part of their agency file only if it is determined they have a role to play in mitigating the situations of acutely elevated risk and only to the extent needed to address the risk factors. If an agency has no role to play in the situation, they should not record any information. The Chair of the Hub provides ongoing direction regarding note taking – i.e. that participants should only take notes if they are involved and that they only be on a need to know basis.

There is also a central provincial record of each Hub discussion; that record is limited to de-identified information. The data is entered online into a password protected Microsoft Customer Relationship Management (CRM) database hosted by the Saskatchewan Ministry of Justice. The data entry is done in real-time at the Hub meeting by a designated Hub representative. The representative is provided a secure login and password to access and input information. The data that is recorded in the database is as follows:

- Hub discussion number,
- date opened,
- reopening (yes, or no),
- old discussion number (if applicable),
- originator (which agency brought forward the situation),
- type of situation (person, dwelling, neighbourhood, environmental, family),
- gender, age group (0-11, 12-17, 18+, 65+),
- category (e.g.; child welfare, housing, maintenance, domestic related, mental health, addictions, miscellaneous, criminality, elder abuse, physical health),
- the actual risk factors (there are 105 risk factors available for selection, e.g.: Criminal Involvement - assault, Physical Violence - physical violence in the home, Self-Harm – person has engaged in self-harm, Physical Violence - perpetrator of physical violence, Crime Victimization - sexual assault, Criminal Involvement - homicide, Suicide – person current suicide risk, Drugs - drug abuse by person, Alcohol - alcohol abuse by person, Missing School – Chronic Absenteeism, Housing – person does not have access to appropriate housing),
- lead agency,
- assisting agencies,
- if the discussion is held as a YCJA case conference,
- date for next discussion,
- date concluded,
- Acceptance reason (accepted/rejected),

- reason for conclusion (connected to services/cooperative, connected to services in other jurisdiction, deceased, informed of services, refused services/uncooperative, relocated, unable to locate).

Agencies record the corresponding Hub Discussion Number alongside the individual's name in their internal notes and on the Common Referral Form.

Personal information and personal health information collected by the participating agencies at the integrated service will be subject to retention periods that apply to that agency. Provincial government ministries will be subject to *The Archives and Public Records Management Act* for retention and disposal of records. Secondary purposes may also be considered (such as program evaluation, research and analysis) when determining retention periods.

F: Managing Access Requests, Individual Access and the Record's Accuracy

A key principle in privacy practice is to provide individuals with a means to access their own information. Central to this principle is to provide individuals with the ability to know what information is collected about them and to provide an opportunity to challenge the accuracy of that information.

Saskatchewan access and privacy law provides individuals with a legal right to access personal information about themselves in the possession or control of government institutions, local authorities and health trustees subject to FOIP, LAFOIP and or HIPA. Identifiable records may be maintained by participating agencies. Those agencies will provide access to those records in accordance with applicable legislation.

The common or integrated service should not maintain an identifiable record to which access would be an issue. Nevertheless, the records maintained by the service may have a Discussion Number through which information could be re-identified if necessary. This re-identification should only be undertaken in exceptional circumstances and then only by a participating agency. The common or integrated service itself should not retain the key. Only agencies that had a role to play in solutions to a situation will know which Discussion Number relates to a particular individual. Individuals seeking to access their records must therefore contact their participating agency directly.

Access requests made to participating agencies are managed according to each agency's legislative and or policy requirements. FOIP, LAFOIP and HIPA each have requirements for access and accuracy of personal information in the possession or control of bodies subject to those laws. Federal laws have similar requirements.

Generally, accuracy is addressed through active management of the records in question, along with ensuring that individuals have access to their own records and have the ability to request corrections where errors or disagreements about accuracy are noted.

G: Information Sharing Agreements (ISA)

Organizations that propose to facilitate the sharing of information within a common or integrated service approach should utilize an information sharing agreement. The regulation amendments to the provincial legislation defines an information sharing agreement as an agreement that governs the collection, use and disclosure of personal information and personal health information by the parties involved in the provision of a common or integrated service. The regulations set out that:

- a government institution must be involved in the programming;
- an information sharing agreement governing the collection, use and disclosure of personal information and personal health information must be in place between the parties that are participating in the common or integrated service;
- the information sharing agreement must contain the following elements:
    - a description of the common or integrated service;
    - a description of the purpose of the service;
    - provisions setting out the obligations of the parties to secure and protect personal information received under the agreement;
    - prohibitions on subsequent use or disclosure of that information except where the individual consents to that use or disclosure or it is required or authorized by law;
    - provisions setting out the process for the withdrawal of a party from the agreement and prohibiting subsequent use or disclosure of that information except where the individual consents to that use or disclosure or it is required or authorized by law;
    - provisions setting out the ongoing obligations of an existing party to continue to secure and protect that personal information;
    - provisions setting out the process for the termination of the agreement and prohibiting subsequent use or disclosure of that information except where the individual consents to that use or disclosure or it is required or authorized by law; and
    - provisions setting out the ongoing obligations of the former parties to the agreement to continue to secure and protect that personal information.

Where these are in place, personal information and personal health information about a person may be disclosed to a party to the information sharing agreement for the purposes of:

- determining eligibility to participate in common or integrated services;
- assessing and planning the common or integrated service; and
- providing and delivering the common or integrated service.

See Appendix 3 for an information sharing agreement template.

H: Collection, Use and Disclosure

Privacy legislation in the public and private sectors imposes different legal obligations with respect to the collection and disclosure of personal information and personal health information. Public bodies subject to FOIP or LAFOIP must be authorized to collect personal information. Government agencies should not exceed their mandates, although they can use and disclose personal information for other purposes with consent.

Trustees subject to HIPA can collect and disclose personal health information within an arena of providing a health service, but generally require consent unless one of the HIPA exemptions applies.

Where contracts with other agencies are involved, the legislation governing the principle will apply to personal information or personal health information in the custody of the contracted service provider. To facilitate delivery of a common or integrated program or service, program or service partners need to consider their own legal obligations as well as the obligations of their partners.

Applying the relevant legislation within a common or integrated service need not be unduly onerous. An approach based on:

- a clear mandate to provide the program or service, or part of the integrated program or service;
- collection, use, disclosure and retention of personal information or personal health information only to the extent necessary for the program or service;
- notification of the purposes of the collection and of contact information for a person who can provide information about the collection; and
- obtaining informed consent of the client whenever possible is likely to meet the applicable legislative requirements.

Informed consent will allow the individual to understand and agree to:

- ***what*** personal or health information will be shared;
- with ***whom***;
- for ***what purpose***; and
- for ***how long*** (consent can be withdrawn at any time).

The FOIP and LAFOIP regulation amendments now allow consent to be obtained verbally for the purposes of a common or integrated service; this now aligns with HIPA. No similar provision exists in the HIPA regulations as HIPA already allows for verbal consent to be provided.

This verbal consent authority should help to obtain consent when having phone discussions or in person (i.e. at door knocks[8]). It is recommended that the person who obtains a verbal consent must document this in writing:

- that the person who provided the consent was informed of the expected uses and disclosures of their personal information;
- the date the consent was provided;
- whether the consent was provided personally, by telephone, or other method;
- the anticipated uses and disclosures of personal information the consenting person was advised of; and
- any restrictions on consent that were provided.

I: Privacy Management Framework

A privacy management framework should already exist in many participating agencies, especially those otherwise subject to FOIP, LAFOIP, HIPA or to one of several federal statutes. A privacy management framework is generally a description of how an agency has established its way of protecting privacy rights and may include practices and policies, training, organizational structure of responsibility (e.g. person or people for ensuring privacy is understood and maintained), various types of safeguards, etc. If a Hub record is collected and managed by one of those agencies, then the record will already be subject to their management. Where the record is held by an agency not subject to one of those Acts (e.g. a regional police service) then a privacy management framework for the Hub should be created, including naming an individual to be the privacy officer, ensuring an ISA is in place, managing access to information requests and generally ensuring best practice with respect to privacy

See Appendix 4 for more information.

VII. Checklist

In order to assist in the use of these guidelines, a checklist that integrated service delivery programs can follow as it addresses information sharing is attached as Appendix 5.

VIII. Outcomes

It is intended that directions identified within these Guidelines will achieve the following broad outcomes:

[8] Door knock refers to a situation where limited Hub participants attend to the place of residence of the individual discussed at Hub to offer support and an connection to services

- appropriate and effective sharing of information for integrated planning of services and supports for children, youth, adults and families;
- greater understanding by delivery staff of their ability to share information related to service provision for the same individual;
- improved coordination of services and supports by cross-sector professionals and service providers, and enhanced capacity to collectively plan short- and long-term interventions; and
- greater participation and benefits experienced by children, youth, adults and their families in the coordination of services and supports.

IX. Future Directions for the Guidelines

These Guidelines are developed in accordance with the legislative environment in existence at June 1, 2016 and may be revised as required to reflect any subsequent changes to privacy legislation. A regular review of common or integrated service delivery processes may also identify further areas for improvement and these will base further revision.

Appendix 1| Background, Privacy Legislation Summary, and Excerpts

1. BACKGROUND

Saskatchewan's Information Sharing Issues Working Group was given the mandate of developing recommendations that would remove barriers and enhance the sharing of information about children, youth, and their families between public sector and service provider organizations who provide services to this client group. The focus was on making recommendations that would lead to the creation of an information exchange process that would then support an enhanced level of collaborative and integrated service delivery while protecting the privacy of the people who receive services.

The balance of these Guidelines provides an overview of the legislation that must be considered to share personal and health information as well as a process to achieve an integrated and collaborative information sharing process.

2. LEGISLATION

The current legislative privacy regime in Saskatchewan consists of provincial and federal privacy legislation in both the public and private sectors, as outlined in the following chart:

LEGISLATION	SECTOR	SCOPE
The Freedom of Information and Protection of Privacy Act (FOIP)	Public	• Provincial government organizations, including Ministries, Crown corporations, agencies boards and commissions
The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP)	Public	• municipalities; • any prescribed board, commission or other body that is appointed pursuant to *The Cities Act*, *The Municipalities Act* or *The Northern Municipalities Act, 2010* • a board of education or conseil scolaire • a regional health authority or an affiliate, as defined in *The Regional Health Services Act*; • any prescribed board, commission or other body that receives more than 50% of its annual budget from the Government of Saskatchewan or a government institution
The Health Information Protection Act (HIPA)	Public, some private	• regional health authorities • government institutions subject to FOIP • health services providers (include pharmacists/pharmacies) • others
The Public Health Act, 1994	Public	• any person who exercises any power, duty or function pursuant to this Act or its regulations
The Youth Drug Detoxification and Stabilization Act	Public	• any person who exercises any power, duty or function pursuant to this Act or its regulations
The Child and Family Services	Public,	• members of the board as set out in the Act

Act	some private	• members of family review panels • mediators • officers and employees of the ministry • members of boards of directors of agencies • officers and employees of agencies • foster parents • all other persons who are employed in or assist with the administration of this Act
The Correctional Services Act, The Correctional Services Act, 2012	Public	• Any person carrying out their powers or duties pursuant to this Act
The *Youth Criminal Justice Act* (Federal)	Public	• Provincial and federal government organizations including the RCMP and other police services
Privacy Act (Federal)	Public	• Federal government organizations, including agencies, boards and commissions (includes the RCMP)
Access to Information Act (Federal)	Public	• Federal government organizations, including agencies boards and commissions (includes the RCMP)
Personal Information Protection and Electronic Documents Act (PIPEDA) (Federal)	Private	• Saskatchewan private sector organizations when collecting, using or disclosing personal information in the course of commercial activity (i.e. if money is involved). Only applies to employee information of federally regulated businesses.

A: The Freedom of Information and Protection of Privacy Act

The Freedom of Information and Protection of Privacy Act (FOIP) contains a set of requirements that a government institution must abide by in collecting, protecting, using, disclosing and providing access to personal information in its custody and/or under its control. While FOIP protects personal information by among other things limiting the collection, use and disclosure of personal information only for purposes specified in the Act, these purposes cover many of the circumstances when government institutions need to collect, use and disclose personal information in an integrated service setting.

The act also provides a right of access to general information and an individual's own personal information, and allows for a right of correction of personal information. FOIP continues to apply to personal information in the control of a government institution, even when in the custody of a service provider. For example, when a private sector agency provides counseling services under contract to a government department, the personal information remains protected under FOIP.

FOIP defines government institutions as "any department, secretariat or other similar agency of the executive government of Saskatchewan" and "prescribed boards, commissions, Crown corporation or other bodies duly appointed", which would include:

- Government agencies, boards and commissions listed in Schedule 1 of *The Freedom of Information and Protection of Privacy Regulation*
- Government ministries

FOIP will apply to the personal information collected, used and disclosed by government institutions. FOIP sets limits on the appropriate collection, use and disclosure of personal

information or personal health information. An organization that is subject to the Act can only collect, use or disclose personal information or personal health information, as the case may be, in accordance with the Act. The Act ensures that privacy is protected while also allowing sharing in certain circumstances. Agencies must ensure that their circumstance is provided for in the Act before collection, use or disclosure occurs.

Collection

In a Hub discussion, a government institution should only collect personal information if it believes it can assist the subject individual by offering a program or service to the individual or to see if it has had any history with the individual that would be useful in assisting him or her. Preferably, a government institution will collect personal information directly from the subject individual. However, the government institution can collect personal information indirectly:

- that may be disclosed to it pursuant to subsection 29(2) of FOIP (pursuant to s. 26(1)(b) of FOIP); or
- where another manner of collection is authorized pursuant to another Act or a regulation [FOIP: 26(1) (h)].

Therefore, if personal information may be disclosed to the government institution in integrated service discussions pursuant to subsection 29(2) of FOIP, then the government institution would be able to collect the personal information during that discussion.

Use and Disclosure

In most circumstances, consent should always be sought for use or disclosure. Once provided, information sharing is permitted as long as it is shared within the parameters set out by that consent. For example, if an individual is approached and offered services, he or she may be asked to consent to provide their personal information to other integrated service providers and for them to be able to use that information in order to do so. Consent should be in writing unless it is not practicable to do so.

However, the government institution may also use or disclose the information under its control in two situations:

- for the purpose it was collected or a consistent use [FOIP: 28(a) and 29(2)(a)]; and
- for a purpose for which the information may be disclosed to the government institution pursuant to subsection 29(2) of FOIP [s. 28(b) and 29(2)].

Therefore, the most straightforward way to allow government institutions to collect and use personal information during integrated service discussions is to use a provision that permits the information to be disclosed to the government institution pursuant to subsection 29(2) of FOIP. Basically, if the personal information can be disclosed to the government institution for the purposes of the integrated service discussion, then the government institution is also allowed to collect and use this information.

Subsection 29(2) governs how government institutions may disclose personal information under their control without the consent of the subject individual. For example, s. 29(2) (m) allows a government institutions to disclose personal information where it is necessary to protect the mental or physical health or safety of any individual. If personal information is disclosed to a Hub discussion for this purpose, then a government institution will be allowed to collect it for the same purpose.

Also, s. 29(2) (u) of FOIP allows disclosure in circumstances set out in Regulations. Section 16 of *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations) outlines when personal information may be disclosed for the purposes of s. 29(2)(u) of FOIP. Section 16(c) of the FOIP Regulations allows personal information to be disclosed to another government institution or local authority where disclosure may reasonably be expected to assist in the provision of services for the benefit of the individual to whom the information relates.

Consideration is currently being given to changing the law or regulations to enable a broader discussion in the integrated service context. Once changed, these Guidelines will be revised.

FOIP Excerpts

The Freedom of Information and Protection of Privacy Act

2(1) In this Act:

(d) "government institution" means, subject to subsection (2):

(i) the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or

(ii) any prescribed board, commission, Crown corporation or other body, or any prescribed portion of a board, commission, Crown corporation or other body, whose members or directors are appointed, in whole or in part:

(A) by the Lieutenant Governor in Council;

(B) by a member of the Executive Council; or

(C) in the case of:

(I) a board, commission or other body, by a Crown corporation; or

(II) a Crown corporation, by another Crown corporation;

(g) "personal information" means personal information within the meaning of section 24;

(i) "record" means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms that produce records;

(j) "third party" means a person, including an unincorporated entity, other than an applicant or a government institution

(2) "Government institution" does not include:

(a) a corporation the share capital of which is owned in whole or in part by a person other than the Government of Saskatchewan or an agency of it;

(b) the Legislative Assembly Service or offices of members of the Assembly or members of the Executive Council; or

(c) the Court of Appeal, Her Majesty's Court of Queen's Bench for Saskatchewan or the Provincial Court of Saskatchewan

Confidentiality provisions in other enactments

23 (1) Where a provision of:

(a) any other Act; or

(b) a regulation made pursuant to any other Act;

that restricts or prohibits access by any person to a record or information in the possession or under the control of a government institution conflicts with this Act or the regulations made pursuant to it, the provisions of this Act and the regulations made pursuant to it shall prevail.

(2) Subject to subsection (3), subsection (1) applies notwithstanding any provision in the other Act or regulation that states that the provision is to apply notwithstanding any other Act or law.

(3) Subsection (1) does not apply to:

(c) section 74 of The *Child and Family Services Act*

(e.1) *The Health Information Protection Act;*
(f) section 38 of *The Mental Health Services Act*

Interpretation
24(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:

(a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
(b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
(d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
(e) the home or business address, home or business telephone number or fingerprints of the individual;
(f) the personal opinions or views of the individual except where they are about another individual;
(g) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;
(h) the views or opinions of another individual with respect to the individual;
(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;
(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or
(k) the name of the individual where:
(i) it appears with other personal information that relates to the individual; or
(ii) the disclosure of the name itself would reveal personal information about the individual.

(1.1) "Personal information" does not include information that constitutes personal health information as defined in *The Health Information Protection Act.*
(2) "Personal information" does not include information that discloses:

(a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a government institution or a member of the staff of a member of the Executive Council;
(b) the salary or benefits of a legislative secretary or a member of the Executive Council;
(c) the personal opinions or views of an individual employed by a government institution given in the course of employment, other than personal opinions or views with respect to another individual;
(d) financial or other details of a contract for personal services;
(e) details of a licence, permit or other similar discretionary benefit granted to an individual by a government institution;
(f) details of a discretionary benefit of a financial nature granted to an individual by a government institution;
(g) expenses incurred by an individual travelling at the expense of a government institution.

(3) Notwithstanding clauses (2)(e) and (f), "personal information" includes information that:

(a) is supplied by an individual to support an application for a discretionary benefit; and

(b) is personal information within the meaning of subsection (1).

Purpose of information
25 No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

Manner of Collection
26 (1) A government institution shall, where reasonably practicable, collect personal information directly from the individual to whom it relates, except where:

(a) the individual authorizes collection by other methods;

(b) the information is information that may be disclosed to the government institution pursuant to subsection 29(2);

(c) the information:

(i) is collected in the course of, or pertains to, law enforcement activities, including the detection, investigation, prevention or prosecution of an offence and the enforcement of:

(A) an Act or a regulation; or

(B) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(ii) pertains to:

(A) the history, release or supervision of persons in custody, on parole or on probation; or

(B) the security of correctional institutions;

(d) the information is collected for the purpose of commencing or conducting a proceeding or possible proceeding before a court or tribunal;

(e) the information is collected, and is necessary, for the purpose of:

(i) determining the eligibility of an individual to:

(A) participate in a program of; or

(B) receive a product or service from the Government of Saskatchewan or a government institution, in the course of processing an application made by or on behalf of the individual to whom the information relates; or

(ii) verifying the eligibility of an individual who is participating in a program of or receiving a product or service from the Government of Saskatchewan or a government institution;

(f) the information is collected for the purpose of:

(i) management;

(ii) audit; or

(iii) administration of personnel;

of the Government of Saskatchewan or one or more government institutions;

(g) the commissioner has, pursuant to s. 33(c), authorized collection of the information in a manner other than directly from the individual to whom it relates; or

(h) another manner of collection is authorized pursuant to another Act or a regulation.

(2) A government institution that collects personal information that is required by subsection (1) to be collected directly from an individual shall inform the individual of the purpose for which the information is collected unless the information is exempted by the regulations from the application of this subsection.

(3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected.

Standard of accuracy
27 A government institution shall ensure that personal information being used by the government institution for an administrative purpose is as accurate and complete as is reasonably possible.

Use of personal information
28 No government institution shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:

(a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the government institution pursuant to subsection 29(2).

Disclosure of personal information
29 (1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30.

(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:

(a) for the purpose for which the information was obtained or compiled by the government institution or for a use that is consistent with that purpose;

(b) for the purpose of complying with:

(i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(c) to the Attorney General for Saskatchewan or to his or her agent or legal counsel for use in providing legal services;

(d) to legal counsel for a government institution for use in providing legal services to the government institution;

(e) for the purpose of enforcing any legal right that the Government of Saskatchewan or a government institution has against any individual;

(f) for the purpose of locating an individual in order to:

(i) collect a debt owing to Her Majesty in right of Saskatchewan or to a government institution by that individual; or

(ii) make a payment owing to that individual by Her Majesty in right of Saskatchewan or by a government institution;

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met;

(h) pursuant to an agreement or arrangement between the Government of Saskatchewan or a government institution and:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iii) the government of a foreign jurisdiction or its institutions;

(iv) an international organization of states or its institutions; or

(v) a local authority as defined in the regulations for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(h.1) for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*, to:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iii) the government of a foreign jurisdiction or its institutions;

(iv) an international organization of states or its institutions; or

(v) a local authority as defined in the regulations;

(i) for the purpose of complying with:

(i) an Act or a regulation;

(ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(iii) a treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada;

(j) where disclosure is by a law enforcement agency:

(i) to a law enforcement agency in Canada; or

(ii) to a law enforcement agency in a foreign country pursuant to an arrangement, a written agreement or treaty or to legislative authority;

(k) to any person or body for research or statistical purposes if the head:

(i) is satisfied that the purpose for which the information is to be disclosed is not contrary to the public interest and cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates; and

(ii) obtains from the person or body a written agreement not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(l) for the purpose of:

(i) management;

(ii) audit; or

(iii) administration of personnel;

of the Government of Saskatchewan or one or more government institutions;

(m) where necessary to protect the mental or physical health or safety of any individual;

(n) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

(o) for any purpose where, in the opinion of the head:

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

(ii) disclosure would clearly benefit the individual to whom the information relates;

(p) where the information is publicly available;

(q) to the office of the Provincial Auditor, or to any other prescribed person or body, for audit purposes;

(r) to the Ombudsman;

(s) to the commissioner;

(t) for any purpose in accordance with any Act or regulation that authorizes disclosure; or

(u) as prescribed in the regulations.

(3) A government institution that is a telephone utility may disclose names, addresses and telephone numbers in accordance with customary practices.

(4) Subject to any other Act or regulation, the Provincial Archivist may release personal information that is in the possession or under the control of The Saskatchewan Archives Board where, in the opinion of the Provincial Archivist, the release would not constitute an unreasonable invasion of privacy.

Personal information of deceased individual
30 (1) Subject to subsection (2) and to any other Act, the personal information of a deceased individual shall not be disclosed until 25 years after the death of the individual.
(2) Where, in the opinion of the head, disclosure of the personal information of a deceased individual to the individual's next of kin would not constitute an unreasonable invasion of privacy, the head may disclose that personal information before 25 years have elapsed after the individual's death.

Individual's access to personal information
31 (1) Subject to Part III and subsection (2), an individual whose personal information is contained in a record in the possession or under the control of a government institution has a right to, and:

(a) on an application made in accordance with Part II; and
(b) on giving sufficient proof of his or her identity;

shall be given access to the record.
(2) A head may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of determining the individual's suitability, eligibility or qualifications for employment or for the awarding of government contracts and other benefits, where the information is provided explicitly or implicitly in confidence.

Right of Correction
32 (1) An individual who is given access to a record that contains personal information with respect to himself or herself is entitled:

(a) to request correction of the personal information contained in the record if the person believes that there is an error or omission in it; or
(b) to require that a notation be made that a correction was requested but not made.

(2) Within 30 days after a request pursuant to s. (1)(a) is received, the head shall advise the individual in writing that:

(a) the correction has been made; or
(b) a notation pursuant to s. (1)(b) has been made.

(3) Section 12 applies, with any necessary modification, to the extension of the period set out in subsection (2).

The Freedom of Information and Protection of Privacy Regulations

Other disclosure of personal information
16 For the purposes of s. 29(2)(u) of the Act, personal information may be disclosed

(c) where disclosure may reasonably be expected to assist in the provision of services for the benefit of the individual to whom the information relates;
(r) to an officer as defined in *The Child and Family Services Act* for the purpose of managing case files, including:

(i) carrying out an investigation pursuant to *The Child and Family Services Act*;
(ii) carrying out an investigation pursuant to any other Act or regulations governing that officer; and
(iii) carrying out an investigation pursuant to any Act or regulation of the Parliament of Canada governing that officer;

Disclosure of personal information to a party to an information sharing agreement

17.1(1) In this section:

(a) 'common or integrated service' means a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:

(i) another government institution;

(ii) a local authority;

(iii) a trustee as defined in *The Health Information Protection Act*;

(iv) a First Nation;

(v) a police service or regional police service as defined in *The Police Act, 1990*;

(vi) the Royal Canadian Mounted Police;

(vii) a non-profit organization that provides a service of the type to be included in the common or integrated service;

(viii) any other agency or organization that the minister determines is appropriate;

(b) 'information sharing agreement' means an agreement that governs the collection, use and disclosure of personal information by the parties involved in the provision of a common or integrated service and that meets the requirements of subsection (2).

(2) An information sharing agreement must contain the following:

(a) a description of the common or integrated service to be provided;

(b) a description of the purposes or expected outcomes of the common or integrated service;

(c) provisions setting out the obligations of a party respecting the security and safeguarding of personal information received by that party;

(d) provisions that prohibit the subsequent use and disclosure of the personal information for purposes not related to the common or integrated service except:

(i) with the consent of the person to whom the information relates; or

(ii) if required or authorized by law;

(e) provisions for the withdrawal of a party and, in the case of a withdrawal, provisions that:

(i) prohibit any further use or disclosure of the personal information received by that party except:

(A) with the consent of the person to whom the information relates; or

(B) if required or authorized by law; and

(ii) specify the ongoing obligations of that party to secure and safeguard the personal information;

(f) provisions for the termination of the information sharing agreement and, in the case of a termination, provisions that:

(i) prohibit any further use or disclosure of the personal information received by the parties except:

(A) with the consent of the person to whom the information relates; or

(B) if required or authorized by law; and

(ii) specify the ongoing obligations of the parties to secure and safeguard the personal information;

(g) any other provisions that the minister considers necessary.

(3) For the purposes of clause 29(2)(u) of the Act, personal information may be disclosed to a party to an information sharing agreement entered into for the purposes of providing a common or integrated service:

(a) if that information is disclosed in accordance with the agreement for any or all of the following purposes:

(i) determining the eligibility of an individual to receive the common or integrated service;

(ii) assessing and planning the common or integrated service and delivering that service to an individual or that individual's family; or

(b) if consent to the disclosure was obtained pursuant to any other Act or regulation that does not require the consent to be in writing.

(4) If the Royal Canadian Mounted Police participates in providing a common or integrated service, the requirements of subsection (3) are met if the Royal Canadian Mounted Police enters into a single arrangement in writing with a government institution that is involved in the provision of the common or integrated service, under which the Royal Canadian Mounted Police signifies that it will comply with the terms governing the collection, use and disclosure of personal information contained in the information sharing agreement applicable to the common or integrated service in which the Royal Canadian Mounted Police participates.

(5) Notwithstanding section 18, consent to the use and disclosure of personal information for the purposes of receiving a common or integrated service is not required to be in writing if:

(a) the individual providing consent is informed of the anticipated uses and disclosures of the individual's personal information; and

(b) the person who obtained the consent records the following information and signs the record:

(i) the date on which consent was obtained;

(ii) the manner by which consent was obtained, whether the consent was obtained in person, by way of telephone or otherwise;

(iii) the anticipated uses and disclosures of personal information the individual consented to;

(iv) any restrictions on the consent that was provided**.**

Consent

18 Where the Act requires the consent of an individual to be given, the consent is to be in writing unless, in the opinion of the head, it is not reasonably practicable to obtain the written consent of the individual.

B: Health Information Protection Act

The *Health Information Protection Act* (HIPA) applies to personal health information held by individuals and organizations who are health information trustees as defined in the Act (see below). HIPA provides the rules for the collection, use, disclosure and protection of personal health information. HIPA is based on principles similar to FOIP, but differs from FOIP in several key areas. At the heart of HIPA is a firm understanding that health service providers require personal health care information in order to fulfill their service mandates. The concept of controlled sharing means that trustees are permitted to obtain and use the amount and type of health information that is necessary for them to perform their mandate.

HIPA Trustees

These include:

- Regional Health Authorities,
- members of regulated health professions such as doctors, dentists, etc.
- pharmacies
- government institutions
- health care organizations as defined in *The Regional Health Services Act*

- licensees or operators of health care facilities, personal care homes, mental health facilities, ambulances, community clinics
- people or organizations that are contracted, by a trustee, to provide a health service

Personal health information discussed at a Hub meeting may be governed by HIPA. Regional Health Authorities participating in a Hub should have policy related to the collection, use and disclosure of personal health information at these types of meetings. See Appendix 2 for sample policy.

HIPA allows personal health information to be collected:

- directly from the subject individual;
- using other methods if the individual consents [HIPA: 25(1)(a)];
- if direct collection would prejudice the mental health or physical safety of the individual or another individual [HIPA: 25(1)(c)];
- the personal health information is collected from another trustee and the disclosure is permitted by section 27, 28 or 29 of HIPA [s. 25(1)(f)]; or
- if the regulations prescribe the circumstances [HIPA: 25(1) (g)].

A trustee will collect personal health information during Hub discussions to determine if it has any history with the individual or because the trustee believes it can offer a program or service to the individual. It is permissible that in some situations, the trustee will believe that direct collection from the individual could result in harm to either the individual or another individual and thus s. 25(1)(a) of HIPA would allow collection from another source, such as at a Hub meeting.

Personal health information will only be introduced to the Hub in cases where there is a situation of acutely elevated risk. The health trustee may collect personal health information as a result of the discussion when doing so could reasonably be expected that the individual would benefit being offered a service, activity or program [HIPA: 24(1)].

Section 63(1) (l) of HIPA allows regulations to be drafted that would prescribe the circumstances in which personal health information may be collected by a trustee other than directly from the individual. New regulations are being considered in order to allow such collection to take place.

The trustee may use personal health information under its possession or control:

- for the purpose the information was collected or a consistent purpose;
- for a purpose for which it may be disclosed to the trustee pursuant to section 27, 28 or 29 [HIPA: 26(2)(a)];
- if the purpose is primarily to benefit the individual HIPA: 26(2)(c)]; or
- for a prescribed purpose [HIPA: 26(2) (d)].

Before any personal health information is disclosed at Hub discussions, the trustee should assess whether consent is practical or not (i.e. the individual is not accessible or an immediate response is required). If consent is determined not to be practical, a trustee may disclose personal health information without consent where the trustee believes that such disclosure will avoid or minimize a danger to any individual's health or safety [HIPA: 27(4)(a)]. To determine if this circumstance exists, the trustee should determine if the following factors exist:

1. There must be a reasonable expectation of probable harm

2. That harm must constitute damage or detriment and not mere inconvenience
3. There must be a causal connection between the disclosure and the potential reduction of the anticipated harm.

However, this test will not cover all discussions among integrated service providers. Section 27(4) (j) of HIPA allows disclosure for the provision of health or social services to the individual if such disclosure will benefit the health and well-being of the individual. This provision would allow disclosure to some agencies at the discussion table but not potentially to all agencies.

Finally, s. 27(4) (p) of HIPA allows disclosure to happen in prescribed circumstances. Section 63(1) (o) of HIPA allows regulations to be drafted to prescribe these circumstances. It is recommended that regulations be drafted pursuant to this clause to allow for all types of disclosure at an integrated service meeting, especially as it relates to the reduction of acute elevated risk. If the drafted regulations allowed the trustee to disclose to other agencies for the purposes of an integrated service, then such regulations would also allow trustees to use personal health information gathered during those discussions.

HIPA sets limits on the appropriate collection, use and disclosure of personal information or personal health information. An organization that is subject to the Act can only collect, use or disclose personal information or personal health information, as the case may be, in accordance with the Act. The Act ensures that privacy is protected while also allowing sharing in certain circumstances. Agencies must ensure that their circumstance is provided for in the Act before collection, use or disclosure occurs.

HIPA Excerpts

Health Information Protection Act

2 In this Act:

(b) “collect” means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means;

(d) “de-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed;

(h.1) “health care organization” means a health care organization as defined in *The Regional Health Services Act*

(m) “personal health information” means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

(o) “primary purpose” means the purpose for which personal health information was originally collected, and includes any purpose that is consistent with that purpose;

(p) “record” means a record of information in any form and includes information that is written, photographed, recorded, digitized or stored in any manner, but does not include computer programs or other mechanisms that produce records;

(s) “subject individual” means the individual to whom personal health information relates;

(t) “trustee” means any of the following that have custody or control of personal health information:

(i) a government institution;

(ii) a regional health authority or a health care organization;

(iv) a licensee as defined in *The Personal Care Homes Act*;

(v) a person who operates a facility as defined in *The Mental Health Services Act*;

(vi) a licensee as defined in *The Health Facilities Licensing Act*;

(vii) an operator as defined in *The Ambulance Act*;

(viii) a licensee as defined in *The Medical Laboratory Licensing Act*, *1994*;

(ix) a proprietor as defined in *The Pharmacy Act, 1996*;

(x) a community clinic:

(A) as defined in section 263 of *The Co-operatives Act, 1996*;

(B) within the meaning of section 9 of *The Mutual Medical and Hospital Benefit Associations Act*; or

(C) incorporated or continued pursuant to *The Non-profit Corporations Act, 1995*;

(xi) the Saskatchewan Cancer Foundation;

(xii) a person, other than an employee of a trustee, who is:

(A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or

(B) a member of a class of persons designated as health professionals in the regulations;

(xiii) a health professional body that regulates members of a health profession pursuant to an Act;

(xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;

(xv) any other prescribed person, body or class of persons or bodies;

(u) “use” includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

Collection, use and disclosure on need-to-know basis

23 (1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.

((2) A trustee must establish policies and procedures to restrict access by the trustee’s employees to an individual’s personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

(4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

Restrictions on collection

24 (1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.

(2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
(3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
(4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

Manner of collection
25 (1) Subject to subsection (2), a trustee shall collect personal health information directly from the subject individual, except where:

(a) the individual consents to collection of the information by other methods;
(b) the individual is unable to provide the information;
(c) the trustee believes, on reasonable grounds, that collection directly from the subject individual would prejudice the mental or physical health or the safety of the subject individual or another individual;
(d) the information is collected, and is necessary, for the purpose of:
(i) determining the eligibility of the individual to participate in a program of the trustee or receive a product or service from the trustee, in the course of processing an application made by or on behalf of the individual; or
(ii) verifying the eligibility of the individual who is participating in a program of the trustee or receiving a product or service from the trustee;
(e) the information is available to the public;
(f) the trustee collects the information by disclosure from another trustee pursuant to section 27, 28 or 29; or
(g) prescribed circumstances exist.

(2) Where the collection is for the purpose of assembling the family health history of an individual, a trustee may collect personal health information from the individual about other members of the individual's family.
(3) Where a trustee collects personal health information from anyone other than the subject individual, the trustee must take reasonable steps to verify the accuracy of the information.
(3.1) Subsection (3) does not apply to personal health information collected by the Saskatchewan Archives Board for the purposes of *The Archives Act, 2004*.

Restrictions on use
26 (1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
(2) A trustee may use personal health information:

(a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
(b) for the purposes of de-identifying the personal health information;
(c) for a purpose that will primarily benefit the subject individual; or
(d) for a prescribed purpose.

(3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent.

Disclosure
27 (1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.

(2) A subject individual is deemed to consent to the disclosure of personal health information:

(a) for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;

(b) for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual; or

(c) to the subject individual's next of kin or someone with whom the subject individual has a close personal relationship if:

(i) the disclosure relates to health services currently being provided to the subject individual; and

(ii) the subject individual has not expressed a contrary intention to a disclosure of that type.

(3) A trustee shall not disclose personal health information on the basis of a consent pursuant to subsection (2) unless:

(a) in the case of a trustee other than a health professional, the trustee has established policies and procedures to restrict the disclosure of personal health information to those persons who require the information to carry out a purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act; or

(b) in the case of a trustee who is a health professional, the trustee makes the disclosure in accordance with the ethical practices of the trustee's profession.

(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

(a) where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person;

(b) where, in the opinion of the trustee, disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services;

(c) where the disclosure is being made to a trustee that is the successor of the trustee that has custody or control of the information, if the trustee makes a reasonable attempt to inform the subject individuals of the disclosure;

(d) to a person who, pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*, is entitled to make a health care decision, as defined in that Act, on behalf of the subject individual, where the personal health information is required to make a health care decision with respect to that individual;

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual's estate; or

(ii) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual's immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;

(f) where the disclosure is being made in accordance with section 22 to another trustee or an information management service provider that is a designated archive;

(g) where the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a

health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:

(i) uses the information only for the purpose for which it was disclosed;

(ii) does not make a further disclosure of the information; and

(iii) takes reasonable steps to preserve the confidentiality of the information;

(h) subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession;

(i) where the disclosure is being made for the purpose of commencing or conducting a proceeding before a court or tribunal or for the purpose of complying with:

(i) an order or demand made or subpoena or warrant issued by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(j) subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent;

(k) where the disclosure is being made for the purpose of:

(i) obtaining payment for the provision of services to the subject individual; or

(ii) planning, delivering, evaluating or monitoring a program of the trustee;

(l) where the disclosure is permitted pursuant to any Act or regulation;

(m) where the disclosure is being made to the trustee's legal counsel for the purpose of providing legal services to the trustee;

(n) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Medical Profession Act, 1981* and approved by the minister;

(o) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996,* where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Pharmacy Act, 1996* and approved by the minister;

(p) in prescribed circumstances.

(5) For the purposes of s. (4)(h), where the personal health information in question is about a member of the profession regulated by the health professional body or prescribed professional body, disclosure may be made only:

(a) in accordance with s. (4)(i);

(b) with the express consent of the subject individual; or

(c) if the trustee has reasonable grounds to believe that the personal health information is relevant to the ability of the subject individual to practise his or her profession, on the request of the health professional body or prescribed professional body.

(6) Disclosure of personal health information pursuant to s. (4) (j) may be made only where the person to whom the information is to be disclosed agrees:

(a) to use the information only for the purpose for which it is being disclosed; and

(b) not to make a further disclosure of the information in the course of carrying out any of the activities mentioned in that section .

Disclosure of registration information

28 (1) The minister may disclose registration information without the consent of the subject individual:

(a) to a trustee in connection with the provision of health services by the trustee;

(b) to another government institution, a regional health authority or anaffiliate, for the purpose of verifying the eligibility of an individual to participate in a program of, or receive a service from, the government institution, regional health authority or affiliate:

(i) in the course of processing an application made by or on behalf of the individual; or

(ii) if the individual is already participating in the program or receiving the service;

(c) to another government institution, a regional health authority or an affiliate, for the purpose of verifying the accuracy of registration information held by the government institution, regional health authority or affiliate; or

(d) with the approval of the Lieutenant Governor in Council, to another government institution on any terms or conditions that the Lieutenant Governor in Council may determine.

(2) For the purposes set out in subsection (3), registration information may be disclosed without the consent of the subject individual:

(a) by the minister to a regional health authority or affiliate;

(b) by a regional health authority or affiliate to the minister; or

(c) by one regional health authority or affiliate to another regional health authority or affiliate.

(3) Registration information may be disclosed pursuant to subsection (2) for the purpose of planning, delivering, evaluating or monitoring a program of the minister, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

(4) The minister or a regional health authority may, without the consent of the subject individuals, disclose the names, dates of birth, telephone numbers and addresses of individuals under the age of seven years to a board of education or the Conseil scolaire fransaskois within the meaning of *The Education Act, 1995* for the purpose of planning or administration by the board of education or the Conseil scolaire fransaskois.

(5) With the approval of the Lieutenant Governor in Council, the minister may enter into agreements for the sharing of registration information with:

(a) the Government of Canada or the government of a province or territory of Canada; or

(b) a prescribed person or body.

(6) An agreement pursuant to subsection (5) must specify that the party to whom the registration information is disclosed shall use the information only for the purposes specified in the agreement.

(7) The minister may disclose registration information without the consent of the subject individual in accordance with an agreement entered into pursuant to subsection (5).

(8) Registration information may be disclosed without the consent of the subject individual in accordance with the regulations.

Use and disclosure for research

29 (1) A trustee or a designated archive may use or disclose personal health information for research purposes with the express consent of the subject individual if:

(a) in the opinion of the trustee or designated archive, the research project is not contrary to the public interest;

(b) the research project has been approved by a research ethics committee approved by the minister; and

(c) the person who is to receive the personal health information enters into an agreement with the trustee or designated archive that contains provisions:

(i) providing that the person who is to receive the information must not disclose the information;

(ii) providing that the person who is to receive the information will ensure that the information will be used only for the purpose set out in the agreement;
(iii) providing that the person who is to receive the information will take reasonable steps to ensure the security and confidentiality of the information; and
(iv) specifying when the person who is to receive the information must do all or any of the following:
(A) return to the trustee or designated archive any original records or copies of records containing personal health information;
(B) destroy any copies of records containing personal health information received from the trustee or designated archive or any copies made by the researcher of records containing personal health information received from the trustee or designated archive.

(2) Where it is not reasonably practicable for the consent of the subject individual to be obtained, a trustee or designated archive may use or disclose personal health information for research purposes if:
(a) the research purposes cannot reasonably be accomplished usingde-identified personal health information or other information;
(b) reasonable steps are taken to protect the privacy of the subject individual by removing all personal health information that is not required for the purposes of the research;
(c) in the opinion of the research ethics committee, the potential benefits of the research project clearly outweigh the potential risk to the privacy of the subject individual; and
(d) all of the requirements set out in clauses (1)(a) to (c) are met.

Use or disclosure prohibited
30 (1) No person who is aware, or should reasonably be aware, that he or she has received personal health information in contravention of this Act shall use or disclose the information without the consent of the subject individual or, where the subject individual is deceased, without the consent of a prescribed person.
(2) Subsection (1) does not apply to personal health information disclosed by a trustee to a member of the subject individual's immediate family or to anyone else with whom the subject individual has a close personal relationship.

Health Information Protection Act Regulations

Disclosure to police officers
5.1(1) For the purposes of clause 27(4)(p) of the Act, personal health information may be disclosed, without the consent of the subject individual, to a member of the Royal Canadian Mounted Police, or to a member of a police service within the meaning of The Police Act, 1990, in the following circumstances:
(a) by the minister if:
(i) the personal health information is required to locate the subject individual for any of the following purposes:
(A) enforcing an outstanding warrant for arrest that has been issued by a court, person or body that has the lawful authority to issue that warrant;
(B) serving a subpoena with respect to the prosecution of an indictable offence;
(C) locating a person reported missing; and
(ii) the personal health information to be disclosed is limited to:
(A) registration information respecting the subject individual; or

(B) information respecting the location that the subject individual last received or was offered a health service;

(b) by a trustee if:

(i) the personal health information is requested for any of the following purposes:

(A) enforcing the Criminal Code or the Controlled Drugs and Substances Act (Canada);

(B) carrying out a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act (Canada); and

(ii) the personal health information to be disclosed is limited to:

(A) registration information respecting the subject individual; or

(B) the nature and severity of an injury that:

(I) was suffered by the subject individual or another individual; and

(II) is connected with the enforcement or lawful investigation mentioned in subclause (i);

(c) by a trustee if:

(i) an individual received or was offered health services directly as a result of an incident that has been made the subject of a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act (Canada);

(ii) the personal health information to be disclosed is limited to:

(A) the factual circumstances surrounding the incident mentioned in subclause (i); and

(B) the factual circumstances surrounding the provision of, or offer to provide, health services; and

(iii) in the opinion of the trustee, the factual circumstances mentioned in subclause (ii) do not include the health history of the subject individual prior to the incident mentioned in subclause (i).

(2) For the purposes of clause 27(4)(p) of the Act, the minister or a trustee may disclose personal health information, without the consent of the subject individual, to the chief coroner or a coroner appointed pursuant to The Coroners Act, 1999 with respect to the conduct of an investigation or inquest by the chief coroner or other coroner pursuant to that Act.

Disclosure of personal health information to a party to an information sharing agreement

5.2(1) In this section:

(a) 'common or integrated service' means a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:

(i) another government institution;

(ii) a local authority;

(iii) a trustee as defined in *The Health Information Protection Act*;

(iv) a First Nation;

(v) a police service or regional police service as defined in *The Police Act, 1990*;

(vi) the Royal Canadian Mounted Police;

(vii) a non-profit organization that provides a service of the type to be included in the common or integrated service;

(viii) any other agency or organization that the minister determines is appropriate;

(b) 'information sharing agreement' means an agreement that governs the collection, use and disclosure of personal health information by the parties involved in the provision of a common or integrated service and that meets the requirements of subsection (2).

(2) An information sharing agreement must contain the following:

(a) a description of the common or integrated service to be provided;
(b) a description of the purposes or expected outcomes of the common or integrated service;
(c) provisions setting out the obligations of a party respecting the security and safeguarding of personal health information received by that party;
(d) provisions that prohibit the subsequent use and disclosure of the personal health information for purposes not related to the common or integrated service except:
(i) with the consent of the person to whom the information relates; or
(ii) if required or authorized by law;
(e) provisions for the withdrawal of a party and, in the case of a withdrawal, provisions that:
(i) prohibit any further use or disclosure of the personal health information received by that party except:
(A) with the consent of the person to whom the information relates; or
(B) if required or authorized by law; and
(ii) specify the ongoing obligations of that party to secure and safeguard the personal health information;
(f) provisions for the termination of the information sharing agreement and, in the case of a termination, provisions that:
(i) prohibit any further use or disclosure of the personal health information received by the parties except:
(A) with the consent of the person to whom the information relates; or
(B) if required or authorized by law; and
(ii) specify the ongoing obligations of the parties to secure and safeguard the personal health information;
(g) any other provisions that the minister considers necessary.

(3) For the purposes of clause 27(4)(p) of the Act, personal health information may be disclosed to a party to an information sharing agreement entered into for the purposes of providing a common or integrated service:
(a) if that information is disclosed in accordance with the agreement for any or all of the following purposes:
(i) determining the eligibility of an individual to receive the common or integrated service;
(ii) assessing and planning the common or integrated service and delivering that service to an individual or that individual's family; or
(b) if consent to the disclosure was obtained pursuant to any other Act or regulation that does not require the consent to be in writing.

(4) If the Royal Canadian Mounted Police participates in providing a common or integrated service, the requirements of subsection (3) are met if the Royal Canadian Mounted Police enters into a single arrangement in writing with a government institution that is involved in the provision of the common or integrated service, under which the Royal Canadian Mounted Police signifies that it will comply with the terms governing the collection, use and disclosure of personal health information contained in the information sharing agreement applicable to the common or integrated service in which the Royal Canadian Mounted Police participates.

C: The Local Authority Freedom of Information and Protection of Privacy Act

Local Authorities include:

- a municipality, such as a city, town, village, rural municipality;
- any board, commission or other body that is appointed pursuant to *The Cities Act*, *The Municipalities Act* or *The Northern Municipalities Act, 2010* and is prescribed

- any board of education or conseil scolaire within the meaning of *The Education Act*;
- a regional health authority or an affiliate, as defined in *The Regional Health Services Act*;
- any board, commission or other body that receives more than 50% of its annual budget from the Government of Saskatchewan or a government institution; and is prescribed.

Privacy obligations similar to those that apply to government institutions under FOIP are applicable to local authorities pursuant to LAFOIP.

LAFOIP will apply to local authorities involved in the discussion respecting integrated services. At those discussions, a local authority only collects personal information when it believes it can provide assistance to the subject individual or situation through one of its existing programs or activities or to determine if the subject individual has had any history with the local authority. As stated earlier, before an agency brings a subject individual up for discussion at the table, that agency would have made a decision about getting consent from the individual.

Collection

Personal information is not to be collected by a local authority unless it is for a purpose that relates to an existing or proposed program or activity of the local authority [LAFOIP: 24]. Further, where reasonably practicable, personal information is to be collected directly from the individual to whom it relates [LAFOIP: 25(1)]. However, if to collect the information directly from the individual would lead to inaccurate information or defeat the purpose for collection, then collecting the information directly from the individual is not required [LAFOIP: 25(3)].

Therefore, a local authority could collect information at an integrated service meeting if it was in relation to a program or activity it provided and it had made a determination that collecting this information from the individual was not practicable or would lead to inaccurate information. Local authorities could also take the individual's name back with them after the discussion and make a determination as to whether consent is practicable (i.e. uses the same system it uses to determine whether to bring a subject individual up for discussion at the integrated service table). The local authority could then collect personal information from integrated service discussions as long as the screening test was passed. It is likely not reasonably practical to collect the information directly from the individual given the acutely elevated risk test applied by the agencies. Local authorities should review their own internal screening process to ensure it aligns with the collection provisions of LAFOIP.

Use and Disclosure

Personal information can be used, without the individual's consent, for a purpose for which the information was obtained or compiled or for a purpose for which the information may be disclosed to a local authority (section 27). If the personal information was collected to determine which programs or activities to offer the individual, then the local authority could use this information to make such a determination. Further, if there is a purpose that allows personal information to be disclosed at the integrated service discussion then the local authority can also use the information for this purpose [LAFOIP: 27(b)].

Section 28 outlines the circumstances in which personal information may be disclosed by a local authority. For example, s. 28(2) (l) allows a local authority to disclose personal information where necessary to protect the mental or physical health or safety of any individual[9].

[9] Please see footnote 6 for more information.

Also, s. 28(2) (r) of LAFOIP allows a local authority to disclose personal information under its control for a purpose in accordance with any Act or regulation that authorizes disclosure. Should the FOIP regulation be redrafted, s. 28(2) (r) of LAFOIP may then allow local authorities to disclose and use personal information collected during the integrated service discussion. However, this would depend on how the provision is drafted under FOIP and this provision would not apply until that time. Collection would still be limited to an existing program or service of the local authority.

LAFOIP sets limits on the appropriate collection, use and disclosure of personal information or personal health information. An organization that is subject to the Act can only collect, use or disclose personal information or personal health information, as the case may be, in accordance with the Act. The Act ensures that privacy is protected while also allowing sharing in certain circumstances. Agencies must ensure that their circumstance is provided for in the Act before collection, use or disclosure occurs.

LAFOIP is similar to FOIP in that s. 28(2) (s) of LAFOIP allows local authorities to disclose personal information in a manner prescribed in the regulations. Section 10 of *The Local Authority Freedom of Information and Protection of Privacy Regulations* (LAFOIP Regulations) prescribes situations where personal information may be disclosed. Section 10(c) of LAFOIP Regulations allows disclosure where it may reasonably be expected to assist in the provision of the services for the individual's benefit. Section 10(c) of LAFOIP Regulations would allow local authorities to disclose personal information to some of the agencies at the table but it is hard to argue that it is necessary to disclose to all the participants that may attend an integrated service discussion. This concern is the same as expressed earlier respecting FOIP and HIPA and the use of the previously described four filter process is encouraged to alleviate it.
New regulations pursuant to s. 57(i) of LAFOIP are being considered to prescribe the purpose, circumstances and persons to whom personal information may be disclosed. If the purpose, circumstance and persons were prescribed it would also allow the local authority to use the personal information for a similar purpose. Should these changes occur, these Guidelines will be revised accordingly.

LAFOIP Excerpts

Local Authority Freedom of Information and Protection of Privacy Act

2 In this Act:

(f) "local authority" means:

(i) a municipality;

(iv) a committee of a council of a municipality;

(v) any board, commission or other body that:

(A) is appointed pursuant to *The Cities Act, The Municipalities Act* or *The Northern Municipalities Act, 2010*; and

(B) is prescribed;

(vi) the board of a public library within the meaning of *The Public Libraries Act, 1984*;

(vii) the Northern Library Office established pursuant to *The Public Libraries Act, 1984*;

(viii) any board of education or conseil scolaire within the meaning of *The Education Act*;

(ix) a regional college within the meaning of *The Regional Colleges Act*, other than the Saskatchewan Indian Community College;
(x) the Saskatchewan Institute of Applied Science and Technology;
(xi) the University of Saskatchewan, including Saint Thomas More College;
(xii) the University of Regina, including:
(A) Campion College; and
(B) Luther College with respect to its post-secondary level activities;
(xiii) a regional health authority or an affiliate, as defined in *The Regional Health Services Act*;
(xvii) any board, commission or other body that:
(A) receives more than 50% of its annual budget from the Government of Saskatchewan or a government institution; and
(B) is prescribed;

(g) "minister" means the member of the Executive Council to whom for the time being the administration of this Act is assigned;
(h) "personal information" means personal information within the meaning of section 23
(j) "record" means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms that produce records;
(k) "third party" means a person, including an unincorporated entity, other than an applicant or a local authority.

Purpose of information
24 No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.

Manner of collection
25 (1) A local authority shall, where reasonably practicable, collect personal information directly from the individual to whom it relates.
(2) A local authority that collects personal information that is required by subsection (1) to be collected directly from an individual shall, where reasonably practicable, inform the individual of the purpose for which the information is collected.
(3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected.
Standard of accuracy
26 A local authority shall ensure that personal information being used by the local authority for an administrative purpose is as accurate and complete as is reasonably possible.

Use of personal information
27 No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:
(a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or
(b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2).

Disclosure of personal information
28 (1) No local authority shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 29.

(2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:

(a) for the purpose for which the information was obtained or compiled by the local authority or for a use that is consistent with that purpose;

(b) for the purpose of complying with:

(i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(c) to the Attorney General for Saskatchewan or to his or her legal counsel for use in providing legal services to the Government of Saskatchewan or a government institution;

(d) to legal counsel for a local authority for use in providing legal services to the local authority;

(e) for the purpose of enforcing any legal right that the local authority has against any individual;

(f) for the purpose of locating an individual in order to collect a debt owing to the local authority by that individual or make a payment owing to that individual by the local authority;

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met;

(h) pursuant to an agreement or arrangement between the local authority and:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the Government of Saskatchewan or a government institution;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority; for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(h.1) for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*, to:

(i) a government institution;

(ii) the Government of Canada or its agencies, Crown corporations or other institutions;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

(i) for the purpose of complying with:

(i) an Act or a regulation;

(ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(iii) a treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada;

(j) where disclosure is by a law enforcement agency:

(i) to a law enforcement agency in Canada; or

(ii) to a law enforcement agency in a foreign country; pursuant to an arrangement, a written agreement or treaty or to legislative authority;

(k) to any person or body for research or statistical purposes if the head:

(i) is satisfied that the purpose for which the information is to be disclosed is not contrary to the public interest and cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates; and

(ii) obtains from the person or body a written agreement not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(l) where necessary to protect the mental or physical health or safety of any individual;

(m) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

(n) for any purpose where, in the opinion of the head:

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

(ii) disclosure would clearly benefit the individual to whom the information relates;

(o) to the Government of Canada or the Government of Saskatchewan to facilitate the auditing of shared cost programs;

(p) where the information is publicly available;

(q) to the commissioner;

(r) for any purpose in accordance with any Act or regulation that authorizes disclosure; or

(s) as prescribed in the regulations.

Personal information of deceased individual

29 (1) Subject to subsection (2) and to any other Act, the personal information of a deceased individual shall not be disclosed until 25 years after the death of the individual.

(2) Where, in the opinion of the head, disclosure of the personal information of a deceased individual to the individual's next of kin would not constitute an unreasonable invasion of privacy, the head may disclose that personal information before 25 years have elapsed after the individual's death.

Individual's access to personal information

30 (1) Subject to Part III and subsections (2) and (3), an individual whose personal information is contained in a record in the possession or under the control of a local authority has a right to, and:

(a) on an application made in accordance with Part II; and

(b) on giving sufficient proof of his or her identity; shall be given access to the record.

(2) A head may refuse to disclose to an individual personal information that is evaluative or opinion material compiled solely for the purpose of determining the individual's suitability, eligibility or qualifications for employment or for the awarding of contracts and other benefits by the local authority, where the information is provided explicitly or implicitly in confidence.

(3) The head of the University of Saskatchewan or the University of Regina may refuse to disclose to an individual personal information that is evaluative or opinion material complied solely for the purpose of:

(a) determining the individual's suitability for:

(i) appointment, promotion or tenure as a member of the faculty of the University of Saskatchewan or the University of Regina;

(ii) admission to an academic program; or

(iii) receipt of an honour or award; or

(b) evaluating the individual's research projects or materials for publication; where the information is provided explicitly or implicitly in confidence.

Right of correction
31 (1) An individual who is given access to a record that contains personal information with respect to himself or herself is entitled:

(a) to request correction of the personal information contained in the record if the person believes that there is an error or omission in it; or

(b) to require that a notation be made that a correction was requested but not made.

(2) Within 30 days after a request pursuant to s. (1)(a) is received, the head shall advise the individual in writing that:

(a) the correction has been made; or

(b) a notation pursuant to s. (1)(b) has been made.

(3) Section 12 applies, with any necessary modification, to the extension of the period set out in subsection (2)

Local Authority Freedom of Information and Protection of Privacy Regulations

Other disclosure of personal information
10 For the purposes of s. 28(2)(s) of the Act, personal information may be disclosed:

(a) to another local authority or a government institution for the purposes of:

(i) determining the eligibility of an individual to participate in a program of, or receive a product of service from, a local authority, the Government of Saskatchewan or a government institution, in the course of processing an application made by or on behalf of the individual to whom the information relates;

(ii) verifying the eligibility of an individual who is or was participating in a program of, or receiving a product or service from, a local authority, the Government of Saskatchewan or a government institution;

(iii) verifying the accuracy of personal information held by the other local authority or government institution;

(iv) collecting a debt or assisting in the collection of a debt owing to a local authority, Her Majesty in right of Saskatchewan or a government institution;

(b) to an individual or body providing consulting or other services to a local authority if the individual or body agrees not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(c) where disclosure may reasonably be expected to assist in the provision of services for the benefit of the individual to whom the information relates;

(d) to a professional association or professional regulatory body for the purpose of carrying out the lawful activities of the association or body;

(e) for the purpose of providing an employment reference with respect to a person who is or was employed by a local authority;

(f) for the purpose of commencing or conducting a proceeding or possible proceeding before a court or tribunal;

(g) to any person where the information pertains to:

(i) the performance of any function or duty or the carrying out of any responsibility by an officer or employee of a local authority; or

(ii) the terms or circumstances under which a person ceased to be an employee of a local authority, including the terms of any settlement or award resulting from the termination of employment;

(h) with respect to health care information, in compassionate circumstances, unless the person to whom the information relates requests that the information not be disclosed;
(i) to another local authority or a third party in order to obtain information from that local authority or third party to respond to an inquiry from the individual to whom the information relates, to the extent necessary to respond to that inquiry;
(j) to another local authority or a government institution to enable that local authority or government institution to respond to an inquiry from the individual to whom the information relates, to the extent necessary to respond to that inquiry; or
(k) by forwarding to another local authority or government institution a correspondence received from an individual to enable that government institution or local authority to reply directly to the individual where a direct reply is considered more appropriate; or
(l) in the case of names, dates of birth, telephone numbers and addresses of individuals under the age of seven years, by a regional health authority to a board of education or the conseil scolaire, as defined in *The Education Act, 1995*, for the planning or administrative purposes of that board of education or the conseil scolaire;
(m) in the case of the academic ranks or departmental designations of members of the faculty of the Saskatchewan Institute of Applied Science and Technology, by the Saskatchewan Institute of Applied Science and Technology to any person.

Disclosure re common or integrated service
10.1(1) For the purposes of clause 28(2)(s) of the Act, personal information may be disclosed in accordance with an information sharing agreement entered into pursuant to *The Freedom of Information and Protection of Privacy Regulations* or *The Health Information Protection Regulations* to a party involved in delivering a common or integrated service as defined in those regulations for the purposes of assessing, planning or delivering the common or integrated service.
(2) Notwithstanding section 11, consent to the use and disclosure of personal information for the purposes of receiving a common or integrated service mentioned in subsection (1) is not required to be in writing if:
(a) the individual providing consent is informed of the anticipated uses and disclosures of the individual's personal information; and
(b) either:
(i) the person who obtains the consent records the following information and signs the record:
(A) the date that consent was obtained;
(B) the manner by which consent was obtained, whether the consent was obtained in person, by way of telephone or otherwise;
(C) the anticipated uses and disclosures of personal information with respect to which the individual provided consent;
(D) any restrictions on the consent that the individual provided; or
(ii) consent to the disclosure was obtained pursuant to any other Act or regulation that does not require the consent to be in writing**.**

Consent
11 Where the Act requires the consent of an individual to be given, the consent is to be in writing unless, in the opinion of the head, it is not reasonably practicable to obtain the written consent of the individual.

D: The Public Health Act, 1994

Personal health information collected for the purposes of *The Public Health Act, 1994* has been accepted from the application of HIPA in relation to collection, use and disclosure of this specific information. Therefore the rules under *The Public Health Act* will apply to such information. This Act deals solely with confidentiality and not with collection or use. Disclosure of any information that comes to the person's knowledge in the course of carrying out responsibilities pursuant to this Act, the regulations or bylaws made pursuant to this Act concerning a subject being involved with a communicable disease is prohibited [s. 65(1)]. Disclosure, however, may be permitted where it is required to administer the Act, regulations or bylaws, to carry out a responsibility or to exercise a power conferred by the Act or by law. The subject of the information may approve disclosure, as well.

Although the Act does not provide an authority for disclosure, it authorizes disclosure of information in the circumstances that could be set out under regulations, enabling integrated service providers to share relevant information. These regulatory changes are being considered and if enacted will be included in revised Guidelines.

PHA Excerpts

Confidentiality
65 (1) Subject to subsection (2), no person shall disclose any information that comes to the person's knowledge in the course of carrying out responsibilities pursuant to this Act, the regulations or bylaws made pursuant to this Act concerning a person who:

(a) is infected with or is suspected to be infected with a communicable disease;
(b) is a carrier of or is suspected to be a carrier of a communicable disease;
(c) is a contact of a person mentioned in clause (a) or (b); or
(d) has or has had a non-communicable disease or an injury.

(2) A person may disclose information described in subsection (1) where the disclosure:

(a) is required:
(i) to administer this Act, the regulations or bylaws made pursuant to this Act;
(ii) to carry out a responsibility imposed or to exercise a power conferred by this Act, the regulations or bylaws made pursuant to this Act; or
(iii) by law;
(b) is requested or approved by the person who is the subject of the information;
(c) is ordered by the minister for the purpose of protecting the public health;
(d) is made:
(i) to a physician or nurse or in the course of consultation;
(ii) to a person who is conducting bona fide research or medical review if the disclosure is made in a manner that ensures the anonymity of the information;
(iii) between solicitor and client;
(iv) in the case of information pertaining to a child under 14 years of age, to a parent of the child or to a person who stands in loco parentis to the child; or
(v) in circumstances prescribed in the regulations.

E: The Youth Drug Detoxification and Stabilization Act

This Act permits disclosure of personal health information in circumstances specified in the regulations [18(1) (k] of the Act), but at present there are no regulations in place that do so.

Regulations permit disclosure of information in specified circumstances in the integrated service context.

YDDS Excerpts

The Youth Drug Detoxification and Stabilization Act

Confidentiality

18 (1) Subject to subsection (2), no person who exercises any power, duty or function pursuant to this Act or the regulations shall disclose information collected for the purposes of that power, duty or function except as otherwise authorized by this Act or the regulations.

(2) Subsection (1) does not apply to:
- (a) a parent of a youth with respect to information concerning that youth;
- (b) a police officer; or
- (c) a prescribed person or prescribed class of persons.

(3) Subject to the regulations and subsection (4), a person to whom this section applies may disclose information:
- (a) for the purposes of administering this Act or the regulations;
- (b) to another person exercising a power, duty or function pursuant to this Act or the regulations;
- (c) for the purposes of performing any duty or exercising any power conferred or imposed on that person pursuant to this Act;
- (d) for the purposes of arranging, assessing the need for, providing, continuing, or supporting the provision of an assessment, a detoxification or stabilization service or any other medically necessary service or treatment;
- (e) for the purposes of monitoring compliance with a community order or detoxification order;
- (f) if the person believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of the assessed youth;
- (g) if the disclosure is permitted pursuant to any Act or regulation;
- (h) to comply with a subpoena, warrant or court order issued by a court, person or body that has authority to compel the production of information;
- (i) with the consent of the assessed youth to whom the information relates;
- (j) to the official representative of the assessed youth or the assessed youth's legal counsel; or
- (k) in the prescribed circumstances.

(4) A person to whom this section applies shall disclose only the information that is reasonably necessary for the purposes for which it is being disclosed.
(5) *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act* do not apply to information or records prepared, maintained or disclosed for the purposes of this Act

The Youth Drug Detoxification and Stabilization Regulations

Disclosure re common or integrated agreement
5.1 For the purposes of clause 18(3)(k) of the Act, personal information may be disclosed in accordance with an information sharing agreement entered into pursuant to *The Health Information Protection Regulations* to a party involved in delivering a common or integrated

service as defined in those regulations for the purposes of assessing, planning or delivering the common or integrated service**.**

F: The Child and Family Services Act (CFS Act)

Subsection 74(1) of CFS Act states that information (name and any information that may identify the individual, including any files or documents that come into existence) that comes to the knowledge of an employee shall be kept confidential and shall only be disclosed in accordance with the Act. Information may be disclosed if consent is provided (subsection 74(5) of CFS Act) or if, in the opinion of the Minister, the release of the information outweighs any invasion of privacy (subsection 74(5.1) of CFS Act). The Minister's decision to release information must be done on a case by case basis. The Minister can delegate this authority to a person in writing (subsection 23(2) of *The Interpretation Act, 1995*). There is no current authority to allow regulations to be drafted that would enable information to be shared more broadly. Therefore, either changes to the Act would be necessary or the Minister could delegate the authority to release information on a case-by-case basis.

CFS Excerpts

Confidentiality
74 (1) Notwithstanding section 18 of *The Department of Social Services Act*, members of the board, members of family review panels, mediators, officers and employees of the department, members of boards of directors of agencies, officers and employees of agencies, foster parents and all other persons who are employed in or assist with the administration of this Act:

(a) shall preserve confidentiality with respect to:

(i) the name and any other information that may identify a person that comes to their attention pursuant to:

(A) this Act;

(B) *The Family Services Act*, not including Part III; or

(C) *The Child Welfare Act* , not including Part II; and

(ii) any files, documents, papers or other records dealing with the personal history or record of a person that have come into existence through anything done pursuant to:

(A) this Act;

(B) *The Family Services Act*, not including Part III; or

(C) *The Child Welfare Act*, not including Part II; and

(b) shall not disclose or communicate the information mentioned in s. (a) to any other person except as required to carry out the intent of this Act or as otherwise provided in this section.

(2) The minister, a director or an officer may disclose or communicate information mentioned in subsection (1) relating to a child to:

(a) the guardian, parent or foster parent of that child; or

(b) the child to whom the information relates.

(3) On the request of a person, the minister or a director may:

(a) disclose; or

(b) authorize an officer to disclose; information mentioned in subsection (1) relating to that person in any form that the minister or director considers appropriate.

(4) Notwithstanding subsection (2) or (3), no person shall, except while giving evidence in a protection hearing, disclose to anyone who is not an officer or a peace officer the name of a person who:

(a) makes a report pursuant to section 12; and

(b) requests that his or her name not be disclosed.
(5) Any information that may be disclosed to the person to whom it relates may, with the written consent of the person to whom it relates, be disclosed to any other person.
(5.1) Information mentioned in subsection (1) may be released where, in the opinion of the minister, the benefit of the release of information clearly outweighs any invasion of privacy that could result from the release.
(5.2) The information mentioned in subsection (5.1) may be released in any form that the minister considers appropriate.
(6) Any disclosure of information pursuant to this section does not constitute a waiver of Crown privilege, solicitor-client privilege or any other privilege recognized in law.

G: The Correctional Services Act and The Correctional Services Act, 2012

Under *The Correctional Services Act,* information can be disclosed as may be required by any regulation made under the Act. There is no clear authority to make regulations governing disclosure of records, just very general authorities relating to the operation of the facilities. However, information can be disclosed where approved by the executive director of corrections (13(c) of the Act). Therefore the Executive Director could approve the disclosure to an integrated service for the time being until the new legislation, *The Correctional Services Act,* 2012, comes into force.

Section 110 of *The Correctional Services Act, 2012* precludes the disclosure of information that comes to a person's knowledge in the course of carrying out duties under the Act, except where permitted by the Act or regulations. Section 110(2) (c) of the Bill permits the disclosure of information where permitted pursuant to an Act or regulation. Accordingly, if a FOIP regulation change is made, the new regulation would clarify the authority to disclose this type information in an integrated service setting, without the need for separate regulations under the 2012 legislation. Should this occur, these Guidelines will be revised.

CSA, 2012 Excerpts

109 (1) In this section and in section 110, "information" means information of any kind and in any form, including personal information, personal health information, photographs and other identification materials.

(2) The head of corrections may collect information about or relating to offenders that is required:
(a) for the administration of this Act or the regulations;
(b) to comply with or carry out any orders of a court; or
(c) to carry out programs established pursuant to this Act.

Confidentiality
110 (1) Subject to subsection (2), no person shall disclose any information that comes to that person's knowledge in the course of carrying out that person's powers or duties pursuant to this Act, except in accordance with this Act and the regulations.
(2) Subsection (1) does not apply to a disclosure of information that:
(a) is required for the administration of this Act or the regulations;
(b) is required to carry out a duty imposed or to exercise a power conferred by this Act or the regulations;

(c) is permitted or required by law, including by an Act or regulation, Act of the Parliament of Canada, any regulation made pursuant to those enactments, or any order or demand issued by a person with authority to compel production of information;
(d) is determined by the head of corrections to be appropriate for the purposes of:
(i) protecting the security of the correctional facility or the safety of inmates, staff members or the public;
(ii) the investigation of or prevention of the commission of an offence;
(iii) any investigation being conducted pursuant to the Act; or
(iv) assisting with law enforcement; or
(e) is made in prescribed circumstances

H: Youth Criminal Justice Act (Canada)

The YCJA severely restricts access to information respecting the identity of young persons that are dealt with under that Act, either as offenders or witnesses under the age of 18 years to offences committed by young persons. It does so by prohibiting identification unless doing so is authorized by a YCJA provision.

While the Ministry of Justice and Attorney General and its Corrections and Policing Division are subject to FOIP, federal legislation including the *Youth Criminal Justice Act* is paramount to that provincial law. The YCJA permits the disclosure of young offender records to other professionals (including school representatives) or persons involved in the care and supervision of the young person, in order "to facilitate the rehabilitation of the young person." At the same time there are specific requirements identified on the management of the records that identify the "young person". Note that any decision to share information must consider the obligations of the parties. For example, the RCMP is subject to the federal *Privacy Act*, whereas the municipal police services are not.

The YCJA permits information sharing during a conference convened to assist police, Crown Attorneys, courts or youth workers in making a decision under the Act. Should a young person's situation warrant discussion in an integrated service setting, the decision maker is encouraged to convene a conference then and there in order to facilitate the discussion.

Moreover, Saskatchewan's YCJA Information Sharing Order in Council (148/2013) has been revised clarifying that integrated service delivery discussions can take place respecting young persons subject to that law. The applicable provision states:

> (13) A party to an information sharing ageement, in a form approved by the Minister responsible for the administration of *The Freedom of Informationo and Protection of Privacy Act* (Saskatchewan), for the purposes of the identifiactiona nd delivery of an integrated service for the young person or his or her family.

An information sharing agreement between integrated service providers is therefore required in order for this provision to be utilized. Please see above for further discussion respecting such an agreement.

<u>YCJA Excerpts</u>

Identity of offender not to be published

110. (1) Subject to this section, no person shall publish the name of a young person, or any other information related to a young person, if it would identify the young person as a young person dealt with under this Act.

Limitation

(2) Subsection (1) does not apply

(*a*) in a case where the information relates to a young person who has received an adult sentence;

(*b*) in a case where the information relates to a young person who has received a youth sentence for a violent offence and the youth justice court has ordered a lifting of the publication ban under subsection 75(2); and

(*c*) in a case where the publication of information is made in the course of the administration of justice, if it is not the purpose of the publication to make the information known in the community.

Exception

(3) A young person referred to in subsection (1) may, after he or she attains the age of eighteen years, publish or cause to be published information that would identify him or her as having been dealt with under this Act or the *Young Offenders Act*, provided that he or she is not in custody pursuant to either Act at the time of the publication.

Application for leave to publish

(6) The youth justice court may, on the application of a young person referred to in subsection (1), make an order permitting the young person to publish information that would identify him or her as having been dealt with under this Act or the *Young Offenders Act*, if the court is satisfied that the publication would not be contrary to the young person's best interest or the public interest.

117. Sections 118 to 129 do not apply to records kept in respect of an offence for which an adult sentence has been imposed once the time allowed for the taking of an appeal has expired or, if an appeal is taken, all proceedings in respect of the appeal have been completed and the appeal court has upheld an adult sentence. The record shall be dealt with as a record of an adult and, for the purposes of the *Criminal Records Act*, the finding of guilt in respect of the offence for which the record is kept is deemed to be a conviction.

No access unless authorized

118. (1) Except as authorized or required by this Act, no person shall be given access to a record kept under sections 114 to 116 *[114-Court, 115-police or 116-government records]*, and no information contained in it may be given to any person, where to do so would identify the young person to whom it relates as a young person dealt with under this Act.

119. (1) Subject to subsections (4) to (6), from the date that a record is created until the end of the applicable [access] period set out in subsection (2), the following persons, on request, shall be given access to a record kept under section 114, and may be given access to a record kept under sections 115 and 116:

(*a*) the young person to whom the record relates;

(*b*) the young person's counsel, or any representative of that counsel;

(*c*) the Attorney General;

(*d*) the victim of the offence or alleged offence to which the record relates;

(*e*) the parents of the young person, during the course of any proceedings relating to the offence or alleged offence to which the record relates or during the term of any youth sentence made in respect of the offence;
(*f*) any adult assisting the young person under subsection 25(7), during the course of any proceedings relating to the offence or alleged offence to which the record relates or during the term of any youth sentence made in respect of the offence;
(*g*) any peace officer for
(i) law enforcement purposes, or
(ii) any purpose related to the administration of the case to which the record relates, during the course of proceedings against the young person or the term of the youth sentence;
(*h*) a judge, court or review board, for any purpose relating to proceedings against the young person, or proceedings against the person after he or she becomes an adult, in respect of offences committed or alleged to have been committed by that person;
(*i*) the provincial director, or the director of the provincial correctional facility for adults or the penitentiary at which the young person is serving a sentence;
(*j*) a person participating in a conference or in the administration of extrajudicial measures, if required for the administration of the case to which the record relates;
(*k*) a person acting as ombudsman, privacy commissioner or information commissioner, whatever his or her official designation might be, who in the course of his or her duties under an Act of Parliament or the legislature of a province is investigating a complaint to which the record relates;
(*l*) a coroner or a person acting as a child advocate, whatever his or her official designation might be, who is acting in the course of his or her duties under an Act of Parliament or the legislature of a province;
(*m*) a person acting under the *Firearms Act*;
(*n*) a member of a department or agency of a government in Canada, or of an organization that is an agent of, or under contract with, the department or agency, who is
(i) acting in the exercise of his or her duties under this Act,
(ii) engaged in the supervision or care of the young person, whether as a young person or an adult, or in an investigation related to the young person under an Act of the legislature of a province respecting child welfare,
(iii) considering an application for conditional release, or for a record suspension under the *Criminal Records Act*, made by the young person, whether as a young person or an adult,
(iv) administering a prohibition order made under an Act of Parliament or the legislature of a province, or
(v) administering a youth sentence, if the young person has been committed to custody and is serving the custody in a provincial correctional facility for adults or a penitentiary;
(*o*) a person, for the purpose of carrying out a criminal record check required by the Government of Canada or the government of a province or a municipality for purposes of employment or the performance of services, with or without remuneration;
(*p*) an employee or agent of the Government of Canada, for statistical purposes under the *Statistics Act*;
(*q*) an accused or his or her counsel who swears an affidavit to the effect that access to the record is necessary to make a full answer and defence;
(*r*) a person or a member of a class of persons designated by order of the Governor in Council, or the lieutenant governor in council of the appropriate province, for a purpose and to the extent specified in the order; and

(*s*) any person or member of a class of persons that a youth justice court judge considers has a valid interest in the record, to the extent directed by the judge, if the judge is satisfied that access to the record is

(i) desirable in the public interest for research or statistical purposes, or

(ii) desirable in the interest of the proper administration of justice.

Period of access

(2) The period of access referred to in subsection (1) is

(*a*) if an extrajudicial sanction is used to deal with the young person, the period ending two years after the young person consents to be subject to the sanction in accordance with paragraph 10(2)(*c*);

(*b*) if the young person is acquitted of the offence otherwise than by reason of a verdict of not criminally responsible on account of mental disorder, the period ending two months after the expiry of the time allowed for the taking of an appeal or, if an appeal is taken, the period ending three months after all proceedings in respect of the appeal have been completed;

(*c*) if the charge against the young person is dismissed for any reason other than acquittal, the charge is withdrawn, or the young person is found guilty of the offence and a reprimand is given, the period ending two months after the dismissal, withdrawal, or finding of guilt;

(*d*) if the charge against the young person is stayed, with no proceedings being taken against the young person for a period of one year, at the end of that period;

(*e*) if the young person is found guilty of the offence and the youth sentence is an absolute discharge, the period ending one year after the young person is found guilty;

(*f*) if the young person is found guilty of the offence and the youth sentence is a conditional discharge, the period ending three years after the young person is found guilty;

(*g*) subject to paragraphs (*i*) and (*j*) and subsection (9), if the young person is found guilty of the offence and it is a summary conviction offence, the period ending three years after the youth sentence imposed in respect of the offence has been completed;

(*h*) subject to paragraphs (*i*) and (*j*) and subsection (9), if the young person is found guilty of the offence and it is an indictable offence, the period ending five years after the youth sentence imposed in respect of the offence has been completed;

(*i*) subject to subsection (9), if, during the period calculated in accordance with paragraph (*g*) or (*h*), the young person is found guilty of an offence punishable on summary conviction committed when he or she was a young person, the latest of

(i) the period calculated in accordance with paragraph (*g*) or (*h*), as the case may be, and

(ii) the period ending three years after the youth sentence imposed for that offence has been completed; and

(*j*) subject to subsection (9), if, during the period calculated in accordance with paragraph (*g*) or (*h*), the young person is found guilty of an indictable offence committed when he or she was a young person, the period ending five years after the sentence imposed for that indictable offence has been completed.

Exception

(5) When a youth justice court has withheld all or part of a report from any person under subsection 34(9) or (10) (nondisclosure of medical or psychological report) or 40(7) (nondisclosure of pre-sentence report), that person shall not be given access under subsection (1) to that report or part.

Records of assessments or forensic DNA analysis
(6) Access to a report made under section 34 (medical and psychological reports) or a record of the results of forensic DNA analysis of a bodily substance taken from a young person in execution of a warrant issued under section 487.05 of the *Criminal Code* may be given only under paragraphs (1)(*a*) [young person], (b) [young person's counsel] (*c*) [AG], (*e*) [parents during proceedings or duration of sentence], (f) [adult assisting], (g) [peace officer] ,(*h*) [judge, court or review board] and (*q*) [accused or counsel for full answer and defence] and subparagraph (1)(*s*)(ii) [court ordered access with interests of proper administration of justice].

Introduction into evidence
(7) Nothing in paragraph (1)(*h*) or (*q*) authorizes the introduction into evidence of any part of a record that would not otherwise be admissible in evidence.

Application of usual rules
(9) If, during the period of access to a record under any of paragraphs (2)(*g*) to (*j*) [summary convictions, indictable offences and reinvolvements], the young person is convicted of an offence committed when he or she is an adult,

(*b*) this Part no longer applies to the record and the record shall be dealt with as a record of an adult;

Disclosure of information and copies of record
122. A person who is required or authorized to be given access to a record under section 119, 120, 123 or 124 may be given any information contained in the record and may be given a copy of any part of the record.

Where records may be made available
123. (1) A youth justice court judge may, on application by a person after the end of the applicable period set out in subsection 119(2), order that the person be given access to all or part of a record kept under sections 114 to 116 or that a copy of the record or part be given to that person,

(*a*) if the youth justice court judge is satisfied that

(i) the person has a valid and substantial interest in the record or part,

(ii) it is necessary for access to be given to the record or part in the interest of the proper administration of justice, and

(iii) disclosure of the record or part or the information in it is not prohibited under any other Act of Parliament or the legislature of a province;

Restriction for paragraph (1) (*a*)
(2) Paragraph (1)(*a*) applies in respect of a record relating to a particular young person or to a record relating to a class of young persons only if the identity of young persons in the class at the time of the making of the application referred to in that paragraph cannot reasonably be ascertained and the disclosure of the record is necessary for the purpose of investigating any offence that a person is suspected on reasonable grounds of having committed against a young person while the young person is, or was, serving a sentence.

Notice
(3) Subject to subsection (4), an application for an order under paragraph (1)(*a*) in respect of a record shall not be heard unless the person who makes the application has given the young person to whom the record relates and the person or body that has possession of the record at

least five days notice in writing of the application, and the young person and the person or body that has possession have had a reasonable opportunity to be heard.

Where notice not required
(4) A youth justice court judge may waive the requirement in subsection (3) to give notice to a young person when the judge is of the opinion that
(*a*) to insist on the giving of the notice would frustrate the application; or
(*b*) reasonable efforts have not been successful in finding the young person.

Use of record
(5) In any order under subsection (1), the youth justice court judge shall set out the purposes for which the record may be used.

Access to record by young person
124. A young person to whom a record relates and his or her counsel may have access to the record at any time.

Records in the custody, etc., of archivists
126. When records originally kept under sections 114 to 116 are under the custody or control of the Librarian and Archivist of Canada or the archivist for any province, that person may disclose any information contained in the records to any other person if
(*a*) a youth justice court judge is satisfied that the disclosure is desirable in the public interest for research or statistical purposes; and
(*b*) the person to whom the information is disclosed undertakes not to disclose the information in any form that could reasonably be expected to identify the young person to whom it relates.

Disclosure with court order
127. (1) The youth justice court may, on the application of the provincial director, the Attorney General or a peace officer, make an order permitting the applicant to disclose to the person or persons specified by the court any information about a young person that is specified, if the court is satisfied that the disclosure is necessary, having regard to the following circumstances:
(*a*) the young person has been found guilty of an offence involving serious personal injury;
(*b*) the young person poses a risk of serious harm to persons; and
(*c*) the disclosure of the information is relevant to the avoidance of that risk.

Opportunity to be heard
(2) Subject to subsection (3), before making an order under subsection (1), the youth justice court shall give the young person, a parent of the young person and the Attorney General an opportunity to be heard.

Ex parte application
(3) An application under subsection (1) may be made ex parte by the Attorney General where the youth justice court is satisfied that reasonable efforts have been made to locate the young person and that those efforts have not been successful.

Time limit
(4) No information may be disclosed under subsection (1) after the end of the applicable period set out in subsection 119(2) (period of access to records).

Effect of end of access periods
128. (1) Subject to sections 123, 124 and 126, after the end of the applicable period set out in section 119 or 120 no record kept under sections 114 to 116 may be used for any purpose that would identify the young person to whom the record relates as a young person dealt with under this Act or the *Young Offenders Act*.

Disposal of records
(2) Subject to paragraph 125(7)(*c*), any record kept under sections 114 to 116, other than a record kept under subsection 115(3), may, in the discretion of the person or body keeping the record, be destroyed or transmitted to the Librarian and Archivist of Canada or the archivist for any province, at any time before or after the end of the applicable period set out in section 119.

No subsequent disclosure
129. No person who is given access to a record or to whom information is disclosed under this Act shall disclose that information to any other person unless the disclosure is authorized under this Act.

I: Privacy Act (Federal)

The federal *Privacy Act* defines federal "government institutions". It sets out the controls for the protection of personal information by these federal public sector organizations such as the RCMP and other federal government institutions. It sets out the requirements that government institutions must abide by in the management (including collection, protection, use, access to and its disclosure) of information and protection of the privacy of a third party's personal information that is in its custody and/or under its control.

J: Access to Information Act (Federal)

The federal *Access to Information Act* applies to personal information held by federal government institutions such as the RCMP and other federal government organizations. The intent of the legislation is to allow individuals access to information under the control and custody of the federal government.

K: Personal Information Protection and Electronic Documents Act

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to personal information that a private-sector organization collects, uses and discloses in provinces and territories without similar legislation. The act applies within Saskatchewan to an organization involved in commercial activity that in the course of doing that activity, collects, uses or discloses personal information.

The act normally requires consent for the collection, use or disclosure of personal information with some exceptions. PIPEDA provides a right of access to personal information and a right to request a correction of incorrect information.

L: Other Excerpts

Regional Health Services Act

Interpretation

2 (1) In this Act:

(a) “affiliate” means a person who, immediately before the coming into force of this section, is the operator of a hospital approved pursuant to *The Hospital Standards Act* or a not-for-profit special-care home licensed pursuant to *The Housing and Special-care Homes Act,* and includes any successor to that operator but does not include a regional health authority or a prescribed person

(h) “health care organization” means:

(i) an affiliate; or

(ii) a prescribed person that receives funding from a regional health authority to provide health services

Appendix 2 | Common Referral Form and Instruction Guide

DRAFT HUB REFERRAL *(not for distribution)*					
Date: **(d/m/y)**	**Referring Name:**			**Telephone:**	
CLIENT/STUDENT INFORMATION: Not for disclosure until Filters 3 and 4 ***(Complete Information Relevant for Referring Agency)***					
Client/Student Name				**Agency Identifier**	**Hub No.**
Date of Birth (d/m/y)	**Age**	**Sex: □ F □ M** **□ Unknown**	**Email**	**Telephone**	**Cell Phone**
Address			**City/Province**		**Postal Code**

Parent/Guardian 1	Address	Telephone	Cell Phone
Parent/Guardian 2	Address		

School	Grade	School Contact

Are procedures under YCJA Pending?	☐ Yes ☐ No ☐ N/A	Type of Court Order/Warrant	
Applicable Order or Warrant Conditions			
Other:			

FILTER 1: Pre-Hub Screening	
A	**Situation Proposed for Referral and Previous Attempts at Engagement** (*Briefly describe the situation.*)

B	**Acutely-Elevated Risk: Risk Assessment and Need for Involvement of Other Agencies.** Check risk factors that apply: (*See the Hub Database Glossary for risk factors under each category and definitions*)				
☐	Alcohol	☐	Drugs	☐	Gambling
☐	Mental Health	☐	Cognitive Impairment	☐	Physical Health
☐	Suicide	☐	Self-Harm	☐	Criminal Involvement
☐	Crime Victimization	☐	Physical Violence	☐	Emotional Violence
☐	Sexual Violence	☐	Elderly Abuse	☐	Supervision
☐	Basic Needs	☐	Missing School	☐	Parenting
☐	Housing	☐	Poverty	☐	Negative Peers
☐	Antisocial/Negative Behavior	☐	Unemployment	☐	Missing/Runaway
☐	Threat to Public Health and Safety	☐	Gangs	☐	Social Environment
Agency Specific Assessments Relevant/Consulted:					
Four Elements: (Check all that apply)					
☐	**1) Significant interest at stake?** (What you are trying to achieve, prevent or protect is significant.)				
☐	**2) Probability of Harm Occurring?** (There is a reasonable expectation of harm to individuals if nothing is done.)				
☐	**3) Significant Intensity of Harm?** (The harm would constitute damage or detriment and not mere inconvenience to the individual. It is reasonable to assume that disclosure to the Hub would help minimize or prevent the anticipated harm.)				
☐	**4) Multidisciplinary nature of risk?** (The risk factors are beyond the Originating Agency's scope/mandate to mitigate the elevated level of risk. Operating risk factors cut across multiple human service disciplines. Traditional inter-agency approaches have been considered/attempted.)				
C. Authority for Use and Disclosure of Personal Information or Personal Health Information at the Hub					
☐	Written consent obtained (*attach written consent form – Appendix A*)				
☐	Verbal consent obtained (*attach verbal consent form – Appendix B*)				
	Not practicable to obtain consent. Reason why:				
	Proceeding without consent under authority of: (*provide applicable authority below*)				
☐	[Potential Regulations for common or integrated services.]				

☐	Other:

D. Agency Approval for Referral to Hub

☐	Supervisor/School Principal consulted	Name:

Signature of Supervisor/School Principal: (*If required by Referring Agency*)	Date:

C. Information to be Disclosed at Hub Discussion □ **New Discussion** □ **Previous Discussion**

FILTER 2 – De-identified Information Only

Use no identifiers like names, names of relatives, birth dates, addresses, telephone numbers, email addresses, health services numbers, social insurance numbers. Use age range, not actual age. Avoid quasi-identifiers that could allow identity to be guessed, unless they are necessary to determine acutely elevated risk. Quasi-identifiers include: gender, location information, name of school, marital status, significant dates, ethnic origin, diagnosis information, employment, income.

Purpose: Determine whether threshold of "Acutely Elevated Risk" has been met.

Discussion Type: ☐ Dwelling ☐ Environmental ☐ Family ☐ Neighbourhood ☐ Individual

Information to be disclosed: risk factors, expectation of harm, authority (**information listed in Section B**) and age range:

☐	0 – 4 (Pre-school Child)	☐	5 – 11 (School-age Child)	☐	12 – 17 (Youth)	☐	18 + (Adult)

☐	**Accepted**	☐	**Rejected**	**Reason for Rejection:**

FILTER 3 -- Minimal Identifiable Information

Purpose: Determine whether individuals are sufficiently connected to services, if elevated risk remains and, if so, identify agencies to participate in Filter 4 discussion

YO case Conference called by: ☐ Police ☐ Corrections

Information to be disclosed at Filter 3:

☐	Name	☐	Birth date	☐	Gender	☐	Other if required to meet the Filter 3 purpose. Specify below:

FILTER 4 – Identifiable Information Necessary to Address the Immediate Risk *(For Filter 4 Participants only)*

Lead Agency:

Assisting Agencies:

Issue Flags: ☐ Domestic violence ☐ Systemic issue ☐ # of people informed of/connected to/engaged in services through the intervention:

Study Flags:

Date of Discussion Pending:

Purpose: Determine action/intervention to be taken to reduce the acutely-elevated risk.	
Information to be disclosed at Filter 4: *(disclose only information necessary to enable assessment of the situation and determination of appropriate actions to address immediate risk)*	
E. Verification by Hub Participant of Information Disclosed	**Hub Meeting Date:**
☐	No information was disclosed at each filter other than the information specified under Section C above
OR	
☐	The following information was disclosed in addition to the information specified under Section C. above (*Indicate both the additional information disclosed and the filter at which it was disclosed*).
FORM TO BE PLACED ON CLIENT FILE/ AGENCY RECORD SYSTEM UPON COMPLETION	**File No./Name:**
IF A NEW SITUATION ARISES WITH THIS CLIENT, A NEW FORM SHOULD BE COMPLETED AND FILED	

DRAFT Instruction Guide – Hub Referral Form

Purpose: the Hub Referral Form was created to provide participating agencies with a common form to be used when bringing forward a situation to a Hub table. The form ensures that each agency is bringing similar information to the table. It also provides a record to be placed on the client's file that will indicate what information was disclosed at the Hub. This form is not to be shared with the other agencies.

Procedure:

1. Client is identified as being in an "acutely elevated level of risk" based upon home agency criteria.

2. Client/Student Information – this information should not be shared until filter 3 (name and age range only) and filter 4 (more identifying information, in order for other involved agencies at filter 4 to ensure they have the correct client). Only fill out the agency specific information.

3. Filter 1: Pre-Hub Screening – Section A
    - For the referring agency to briefly describe the current situation and what traditional/internal supports have been attempted.
    - Only the information that is necessary to make a decision on whether the client should be referred to the Hub.

4. Filter 1: Pre-Hub Screening – Section B
    - The first part of this section is for the referring agency to check off all risk factors that are present in the ***current*** situation. Past risk factors should not be included unless they would contribute to the current situation.
    - The second part is for agency specific assessments that were consulted to determine risk factors. Some agencies have behavioral or other assessments that may be of use in determining risks.
    - The final part is meant for the referring agency to determine why this situation needs to proceed to Hub and why it cannot be handled through traditional supports or methods.

5. Filter 1: Pre-Hub Screening – Section C
    - Authority for Use and Disclosure of Personal Information and Personal Health Information at Hub – specifically deals with consent and authority
    - Written consent – was it obtained and if so, attach a copy of the consent form to the referral form.
    - Verbal consent – verbal consent is valid under *The Health Information Protection Act* – attach confirmation of verbal consent to the referral form.

- Not practicable to obtain consent – detail the reason why it is was not practical to obtain consent of the subject individual
- Proceeding without consent – you must include your legislated authority to proceed without consent (i.e. 29(2)(m) of *The Freedom of Information and Protection of Privacy Act* - where necessary to protect the mental or physical health or safety of any individual)

6. Filter 1: Pre-Hub Screening – Section D
    - Agency Approval for Referral to Hub – where required by home agency policy, list the name of the Supervisor/School Principal consulted and have that individual sign and date the form.

7. Filter 1: Pre-Hub Screening – Section E (is listed at C, should be updated)
    - Check off whether this is a new discussion or a previous discussion.

8. Filter 2: De-identified information only – to determine if the threshold for Acutely Elevated Risk has been met.
    - Check off the discussion type.
    - Based on the information in filter 1, list the risk factors, expectation of harm, the legislated authority (or consent) and age range. This is the information that can be disclosed at the Hub table to all participants.
    - A brief description of the presenting situation, excluding identifying details.
    - After the discussion has concluded, a decision will be made on whether or not the discussion has been accepted or rejected. If rejected, list reason for rejection. If accepted, move to Filter 3.

9. Filter 3: Minimal Identifiable Information
    - The purpose of Filter 3 is to determine whether the individuals are sufficiently connected to services, if elevated risk remains regardless of services currently provided, and if so, which agencies need to participate in the Filter 4 discussion.
    - If this is a Young Offender Case Conference, this must be called by the police or by the Young Offender Probation Officer. No other individual may call a YO Case Conference.
    - The name of the individual, gender and possibly the birthdate (only if required) can be shared with the Hub table. Other information may be required if positive identification of the individual is unclear.
    - By the end of the Filter 3 discussion, the agencies that need to be involved in the Filter 4 discussion should be identified. Please note, there may be agencies that have involvement with the subject individual that should not be involved in the Filter 4 discussion because the presenting issues do not involve their agency. The “need to know” only extends to those agencies that should participate in the intervention.

10. Filter 4: Identifiable Information Necessary to Address the Immediate Risk
    - List the lead agency (does not have to be the home agency that brought the discussion forward) and any agencies that will assist in the Hub intervention.
    - Check of any issue flags that may be present in the current situation.
    - Study flags are those issues that appear to be recurring in your location (i.e. high instance of child prostitution) and you believe warrant an issue flag.
    - Date of Discussion Pending is the date that the referral will be brought forward so that the other participating agencies have time to look into their files for information pertinent to the current situation.
    - Purpose – to determine the action or intervention to be taken to address the acutely elevated risk. The information contained in this section will be identifiable and will detail the current situation. However, ensure that the information provided at this time is necessary (i.e. if the individual was homeless 5 years ago and now is presenting with self-harm concerns, the homelessness wouldn't be necessary. If the individual was homeless 5 years ago and is about to be evicted, it might be necessary information).

11. Section F (is listed at E, should be F) – Verification by Hub Participant of Information Disclosed.
    - Hub Meeting Date – this should be the date the Hub referral was first made.
    - Check off "no information was disclosed at each filter other than the information specified under Section C (should be E) above" if only the information on the form under each filter was released at each filter.
    - If additional information was provided at any one of the filters, check off the second box – "the following information was disclosed in addition to the information specified under Section C (should be E) above.
    - Indicate what additional information was provided and at what filter.

12. File No./Name – this is the agency file number and the name on the file.

Appendix 3 | Template Information Sharing Agreement

Information Sharing Agreement for Common or Integrated Service Providers for Community Mobilization Prince Albert

This Agreement is between:

The Government of Saskatchewan represented by the

Minister of Corrections and Policing and the Minister of Social Services

and

The Parkland Regional Health Authority

and

Saskatchewan Rivers Public School Division

and

The Prince Albert Catholic School Division

and

Prince Albert Mobile Crisis Unit Co-operative Limited

and

The Prince Albert Grand Council

and

The Prince Albert Board of Police Commissioners

And

The City of Prince Albert

Preamble

Whereas each party is involved in the community of Prince Albert and surrounding areas delivering or assisting in service delivery to individuals and families;

And Whereas the parties recognize the services they provide can be better co-ordinated and delivered through co-operation and integration of their activities, to achieve more complete services and result in better welfare for individuals, families and the community;

And Whereas in order to deliver co-ordinated services information about individuals will need to be collected, used and disclosed amongst the parties;

And Whereas the parties wish to put into place this Agreement governing the processes for such information sharing, including the collection, use, disclosure and protection of such information;

Therefore the parties agree as follows:

1.0 Definitions

In this Agreement:

1.1 "**Agreement**" means this Agreement, including any Schedules;

1.2 "**COR**" means the Centre of Responsibility, which performs research, data management, data analysis and reporting to assist in achieving longer term community service strategies and goals and as at the date of this agreement is made up of employees from the following parties:

1.2.1 [list party];

1.2.2 [list party] and

1.2.3 [list party].

1.3 **"Hub meeting"** means a meeting of employees and service providers of the parties to discuss situations which may involve states of elevated risk requiring the co-ordination and integration of services provided by two or more of the parties;

1.4 "Hub Record" means the non-nominal information recorded in accordance with this Agreement about a situation which is raised in a Hub meeting;

1.5 "**Information**" means:

(i) any personal information or personal health information collected by a party under this Agreement; and

(ii) any non-nominal information contained in Hub Records which is in a party's possession or control;

1.6 **"personal health information"** means personal health information as defined by *The Health Information Protection Act*:

"personal information" means personal information as defined by *The Freedom of Information and Protection of Privacy Act*, *The Local Authority Freedom of Information and Protection of Privacy Act.*

1.7 **"subject individua**l" means:

(i) in the case of personal information, the individual to whom the personal information relates; and

(ii) in the case of a Hub record, the person(s) to whom that Hub record relates;

1.8 **"third party"** means a person who is not a party to this Agreement.

2.0 Purpose

2.1 The parties agree to co-operate in the delivery of common or integrated services to individuals and families in Prince Albert and surrounding areas designed to benefit the health, safety, welfare and well-being of individuals and families. These services will include:

(a) identifying risks to individuals and families and arranging for timely mobilization of appropriate social, education, health, reintegration or other services and resources provided by the parties to assist individuals and families address their particular needs; and

(b) specific and limited research and analysis of non-nominal data to identify community issues and recommend changes to address those issues through longer term initiatives, strategies or systemic changes;

This Agreement sets conditions on the collection, use or disclosure of Information by the parties for the purpose of assessing, planning and delivering their common or integrated services.

3.0 Collection, Use and Disclosure of Information

3.1 Each party is responsible for the personal information and personal health information that it collects in the course of performing the services, duties or functions of that party.

3.2 Each party (Disclosing Party) agrees to disclose specific and limited personal information and personal health information with another party (Receiving Party) to assist that Receiving Party to carry out the purpose of this Agreement and to assist in the provision of services to a subject individual or that individual's family. All Parties agree that the following will apply to all personal information disclosed under this Agreement:

(a) personal information and personal health information disclosed will be limited to that which is reasonably necessary for the Receiving Party to know;

(b) no party will collect or record personal information or personal health information from a Disclosing Party unless it is required by the Receiving Party to provide services or determine if a service should be provided;

(c) personal information and personal health information which is collected by a Receiving Party will be used solely for the purposes for which it was collected under this Agreement and for no other purpose unless:

(i) such use is specifically authorized under law which is applicable to the Receiving Party; or

(ii) the subject individual has consented to the use;

(d) personal information and personal health information disclosed to and collected by a Receiving Party will become part of the records of that Receiving Party.

(e) a Receiving Party agrees to keep the personal information and personal health information disclosed to it confidential and will not further

disclose it except as required to fulfill the purpose of this Agreement and for no other purpose unless:

(i) such is required by law or specifically authorized under law applicable to the Receiving Party; or

(ii) the subject individual has consented to the disclosure;

3.3 The Parties agree that, where the RCMP is participating in a Hub meeting, that any information disclosed by the RCMP to any Party which constitutes personal information in the hands of the RCMP that the provisions of clauses 3.2 (b), (c), (d) and (e) will apply to that information.

4.0 Hub Meetings and Hub Record

4.1 The Parties will assign specific personnel to attend Hub Meetings. All personnel being assigned by a Party will be employees or service providers:

(a) involved in delivery of program services provided by that Party applicable to the common or integrated services to be provided under this Agreement; and

(b) have completed access and privacy training or if not, will do so within three months of the date they are assigned

4.2 No Party which has assigned employees to be members of the COR will assign that employee as a personnel to attend a Hub Meeting.

4.3 The Parties agree that no member of the COR will be permitted to attend Hub Meetings except for the following purpose:

(a) one COR member may attend to preside over the meeting;

(b) one COR member may attend to create a Hub Record for each case which is discussed at the Hub Meeting; and

(c) in exceptional circumstances when a Party's regular employee or service provider is unable to attend a HUB meeting, a back-up for that person from that Party Is not available and it is in the best interests of that Party that its representative on the COR attend that meeting on its behalf.

4.4 The Hub Record referred to in 4.3(b) shall be created in a non-nominal fashion and contain the following information:

(a) gender of the subject individual/family members;

(b) age range of the subject individual;

(c) risk factors associated with the subject individual/family members

(d) whether the risk factors are considered to place the subject individual/family members in a situation of elevated risk necessitating service involvement of parties other than the referring party;

(e) the party that referred the situation to the Hub Meeting

(f) the party that will be responsible for leading service delivery and the parties involved in service delivery;

(g) whether consent of the subject individual has been obtained for collection, use and disclosure of personal information; and,

(h) other non-nominal information which is approved by the Minister of Justice (Corrections and Policing) that is beneficial for statistical analysis and research.

4.5 The Hub Record will be created by COR members and will be stored and maintained by the Government of Saskatchewan, Ministry of Justice (Corrections and Policing). Only members of the COR and the Ministry of Justice (Corrections and Policing), may use the non-nominal information in the Hub Records for the purposes of data management, data linkage and analysis, including but not limited to supporting, reviewing, evaluating and improving the quality of the common or integrated services approach.

4.6 No Party will attempt to re-identify information in any HUB Record except where such is necessary to carry out the purposes of this Agreement or where such may be required by law, including where access to the HUB record may be requested by the subject individual. Once the purpose for re-identification has been satisfied, the identifiable information will be destroyed in accordance with any laws applicable to that Party.

4.7 The non-nominal information in the HUB Records shall not be provided to a third party unless such is provided for in this Agreement or authorized by law.

4.8 Any party to this Agreement which is not subject to legislation which governs the rights of subject individuals to access their information and which requires such information to be maintained in confidence agrees to comply with the confidentiality and access to personal information requirements of The Freedom of Information and Protection of Privacy Act as if those provisions applied to that party.

5.0 Responsibilities, Dispute Resolution and Costs

5.1 Responsibilities

Each party shall be responsible for the actions of its employees and service providers with respect to the collection, use and disclosure of the personal information and personal health information that is governed by this Agreement and the non-nominal information in the Hub Records.

5.2 Dispute Resolution

(1) In the event of a dispute between the parties with respect to the meaning and intent or any conflict, uncertainty or ambiguity in this Agreement, the senior management for each of the parties shall consult as to an appropriate resolution of the dispute.

(2) During the resolution of the dispute mentioned in subsection (1), the parties shall make reasonable efforts to minimize and mitigate any costs or delays associated with the resolution of the dispute.

5.3 Costs

Costs incurred by a party pursuant to this Agreement shall be the responsibility of that party.

6.0 Security of Information and De-identified Information

6.1 Administrative, Technical and Physical Safeguards

(1) Each party shall protect the Information which is in its possession or control pursuant to this Agreement according to its policies, procedures or guidelines regarding how it will maintain administrative, technical and physical safeguards for such information.

(2) If a party does not have policies, procedures or guidelines mentioned in subsection (1) that party shall create policies, procedures or guidelines within 3 months of entering into this Agreement.

(3) The administrative, technical and physical safeguards mentioned in subsection (1) must:

(a) Protect the integrity, accuracy and confidentiality of the Information;

(b) Protect against any reasonably anticipated:

(i) Threat or hazard to the security or integrity of the Information;

(ii) Loss of the Information; and

(iii) Unauthorized access to or use, disclosure, modification or deletion of the Information.

6.2 Incident Management

(1) Each party shall respond to an event of inappropriate collection, accidental or unauthorized access, use, disclosure, modification or deletion of personal information or personal health information according to its policies, procedures or guidelines for incident management. Such policies will include the notification of the individual of such incident unless the party involved is of the view that such could result in harm to any person.

(2) If a party does not have policies, procedures or guidelines mentioned in subsection (1), that party shall create policies, procedures or guidelines within 3 months of entering into this Agreement.

(3) In the event of accidental or unauthorized access, use, disclosure, modification or deletion of non-nominal information from the Hub Records, the party responsible shall promptly:

(a) notify all of the other parties of the event;

(b) take all reasonable steps to contain the disclosure ; and

(c) take all reasonable steps to prevent a recurrence of the event.

7.0 Retention and Disposition

7.1 Retention

(1) Each party shall retain the Information according to its policies, procedures or guidelines regarding retention periods.

(2) If a party does not have policies, procedures or guidelines mentioned in subsection (1), that party shall exercise due diligence in creating policies, procedures or guidelines.

(3) The policies, procedures or guidelines mentioned in subsection (1) must ensure the Information stored in any format is retrievable, readable and useable for the full retention period.

7.2 Disposition

(1) Each party shall dispose of the Information in a secure manner and according to its policies, procedures or guidelines.

(2) If a party does not have policies, procedures or guidelines mentioned in subsection (1) will be disposed, that party shall exercise due diligence in creating policies, procedures or guidelines.

(3) The policies, procedures or guidelines mentioned in subsection (1) must state how the Information will be disposed of in a manner that protects the privacy of the subject individual.

8.0 Access Requests

8.1 Each party shall follow its own process to be used in responding to an access request made by a subject individual for her or his information or his or her Hub Record.

8.2 If a party does not have a process mentioned in section 8.1, that party shall create a process within 3 months of entering into this Agreement which is consistent with LAFOIP, FOIP or access to information legislation applicable to that party.

9.0 Accuracy

9.1 Each party shall use reasonable efforts to ensure the completeness and accuracy of personal information and personal health information collected, used or disclosed pursuant to this Agreement.

9.2 It is understood and agreed that the parties cannot guarantee the accuracy and shall therefore not be held responsible for any damage to the other party resulting from the collection, use or disclosure of any personal information or personal health information that is inaccurate, incomplete or out-of-date.

9.3 Each party shall correct any inaccuracies of personal information or personal health information collected, used or disclosed pursuant to this Agreement.

9.4 Should a subject individual indicate to a Party that personal information or personal health information collected by that party is incorrect, that Party shall:

(a) correct the information and advise any other Parties of the need to correct their information should they have the same information, if the Party agrees that the information is incorrect; or

(b) make a notation on the record that the subject individual requested a correction, where the Party is not satisfied that the information is incorrect;

10.0 Indemnification

10.1 Subject to section 10.2, each party agrees to indemnify and save harmless all of the other parties and all of its employees, agents, volunteers and contractors from and against any damages, costs, losses or expenses or any claim, action, suit or other proceeding which they or any of them may at any time incur or suffer as a result of or arising out of any injury or loss which may be or be alleged to be caused by or suffered as a result of the acts or omissions of the other parties and its employees, agents, volunteers and contractors relating to, attributable to or in connection with the performance of this Agreement.

10.2 Each party agrees to give notice to the other parties of any claim, action, suit or proceeding relating to or in connection with the management of the information that is the subject of this Agreement. Each party must, at its own expense and to the extent reasonably requested by the other parties, participate in or conduct the defense of any such claim, action, suit or proceeding and any negotiations for the settlement of the same, but one party will not be liable to indemnify the other party or any other indemnified persons for payment of settlement of claim, action, suit or proceeding unless the other party has given prior written consent to the settlement.

11.0 Review of Agreement

The parties shall, on a periodic basis, review the Agreement, and the policies, procedures and guidelines mentioned in it, to ensure it is up-to-date and being followed.

12.0 Amendments

12.1 At any time during the term of this Agreement a party may, by written notice to all of the other parties, request changes to the Agreement.

12.2 Amendments requested pursuant to section 12.1 which are acceptable to all of the parties must be set out in a document executed by all parties and attached as an additional Schedule to this Agreement, whereupon this Agreement must be deemed to be amended in accordance with the provisions of such Schedule.

13.0 Assignability

This Agreement or any part hereunder, or any actual or any beneficial interest herein, shall not be assignable by the record holder without the written consent of all of the parties.

14.0 Withdrawal

14.1 Subject to section 14.3, a party may withdraw from this Agreement by providing ___ (days) (months) written notice to all other parties of its intent to do so.

(2) The obligations created by Articles 3.0, 4.0 6.0, 8.0, 10.0 and section 7.2 in relation to the Information will continue to apply to any party that withdraws from this Agreement under section 14.1.

(3) Where the Government of Saskatchewan is the withdrawing party, this agreement will terminate and the provisions of Article 15.0 will apply.

15.0 Termination

15.1 The parties may agree to terminate this Agreement.

15.2 In the event that this Agreement is terminated, the obligations created by Articles 3.0, 4.0 6.0, 8.0, 10.0 and section 7.2 in relation to the Information will continue to apply to the parties.

16.0 Coming into force

This Agreement comes into force on the date that the last of the Parties have executed this Agreement and remains in force until it is terminated in accordance with Article 15.

17.0 General

17.1 Any notice, amendment, request or communication pursuant to this Agreement must be in writing and must be delivered or mailed to all of the other parties:

in the case of the [name party]:

Name, Position

Branch/Area

Division [if applicable]

Ministry [if applicable]

Address

17.2 This Agreement and its Schedules shall constitute the entire Agreement of the parties and supersedes all previous agreements between the parties, which relate to the collection, use and disclosure of information and de-identified information covered by this Agreement.

17.3 The headings used in this Agreement are for convenience only and are not to be used in the interpretation of the Agreement.

17.4 This Agreement shall be governed by and interpreted in accordance with the laws in force in the Province of Saskatchewan.

18.0 Signatures, Signing Dates and Appendices

Agreed to behalf of the [name party] this____day of _____, 20__

_____ _____

(Witness Signature) **(Signature)**

_____ _____

(print name) **(print title)**

Agreed to behalf of the [name party] this _____day of _____, 20__

_____ _____

(Witness Signature) **(Signature)**

_____ _____

(print name) **(print title)**

Appendix 4 | Sample: Privacy Management Framework

CMPA Privacy Safeguards

Confidentiality and protection of personal information is an important aspect of CMPA's work. The agencies participating in Hub may need to be able to share personal and health information within their custody with other service providers in order to perform risk driven collaborative intervention. Such intervention is taking place through the mobilization of resources to address individuals/families with acutely elevated levels of risk.

Any disclosure, collection and use of personal information must be done carefully, disciplined and in an appropriate manner, while remaining considerate of the necessity of protecting the privacy of all persons as much as possible. CMPA Hub discussants are expected to be diligent in protecting all information in the Hub context in accordance with their home agency's privacy and information safeguard procedures.

The Information Sharing Guidelines for Hubs by the Information Sharing Issues Working Group (ISIWG) apply to any Hub work. The following aspects are particularly emphasized:

Information storage

- At the Hub discussion de-identified information is entered online in a secure provincial Hub database hosted by the SK Ministry of Justice.
- Hub discussants are following the legislation, regulations and protocols applicable to their home agency. Applicable principles include the need to know and data minimization.

Disclosure of information

- Information shared within Hub proceedings is subject to the **CMPA Participant Nondisclosure Agreement.** All Hub discussants will only share and record information necessary for the purpose of mitigating the acutely elevated risk situation.
- Any agency staff other than Hub discussants shall not make any notes or recordings of any personal or personal health information, and will keep anything heard in any Hub discussion in confidence, and not disclose anything to any person or agency. Any individual authorized to attend a Hub discussion is required to sign a **CMPA Nondisclosure Agreement** before they may experience Hub proceedings.

- Hub discussants shall propose any attendance of agency staff in advance and during regularly scheduled Hub meetings for unanimous discussant approval.

Note taking

Discussants involved in an acutely elevated risk situation will likely make reference notes on that situation in order to effectively co-ordinate and execute an intervention. The need to know and the data minimization principles also apply to the note taking. ***Only those Hub discussants identified as having a direct role in the intervention process of a specific discussion shall make notes.*** All notes made by Hub discussants remain the property of the discussant's home agency, and remain subject to that agency's privacy procedures.

Data retention and destruction

All notes taken by Hub participants remain the property of their home agency. They are subject to the data retention and destruction policy of the relevant home agency.

Right of access and correction

Individuals whose personal information or personal health information is collected by government institutions, local authorities or health trustees have a right of access to those records and can request that corrections be made.

In the event of a request to access information collected in the provincial Hub database, CMPA is forwarding the request to the Hub discussants of the relevant agencies in order for their agency to determine if the application is meeting their requirements and if there is a Hub record on the individual. If any of the participating agencies can confirm both of those criteria they will provide CMPA with the relevant Hub discussion number in order for CMPA to be able to provide the agency with the Hub database information attached to that number.

As CMPA is not equipped to receive agency clients or to identify individuals presenting at the CMPA office, the relevant agency provides the applicant with the requested Hub database information according to agency protocol. The applicant can request that any errors in the data be corrected. The relevant agencies and CMPA will make any corrections an agency approved based on such request.

In the event of a privacy breach

In the event of a privacy breach the Privacy Breach Guidelines apply as described on the website of the Office of the Saskatchewan Information and Privacy Commissioner (http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines.pdf).
Prince Albert, March 30, 2016

Appendix 5 | Information Sharing Checklist

Typically, the following should be in place when an integrated service delivery program addresses information sharing issues:

- Documented privacy practices including policies, protocols, procedures or guidelines for collection, use and disclosure of personal information and personal health information.
- A senior employee is identified as a privacy officer with responsibility for managing compliance with privacy obligations.
- Employees are trained in privacy matters and understand the policies related to the information within their control or access.
- Mechanisms for managing access requests by individuals to their own information, for addressing potential privacy incidents, for reviewing new initiatives, etc.
- Contracts / information or data sharing agreements that manage the organization's interactions with partners and third parties.
- The specifics of this "privacy framework" will vary depending upon the size and scope of the organization, but the basic controls should exist.

Appendix 6 | Sample Policy: Prince Albert Parkland Health Region

SECTION:	**GENERAL**	**NUMBER**: **10-10-46**
TOPIC:	**PRIVACY: DISCLOSURE OF PERSONAL HEALTH INFORMATION TO HUB**	**DATE APPROVED**: **March 5, 2012**
APPROVED BY:	**SENIOR MANAGEMENT TEAM**	**REVIEW DATE**:
REVISED DATE: January 15, 2013		

a) Policy Statement

The Prince Albert Parkland Health Region (PAPHR) participates in an interagency group (called the HUB) to provide coordinated services to the general public in the Prince Albert area. The HUB is composed of, but not limited to:

- Social Services (child protection, income security);
- Corrections and Public Safety (adult and youth probation services);
- Health (Acute care, Addiction, Mental Health, Public Health);
- Education;
- Police Services (City and RCMP);
- Prince Albert Grand Council (justice unit);
- Fire services; and
- City of Prince Albert.

Personal health information disclosed to the HUB by the PAPHR will be in accordance with this policy.

b) The HUB

The HUB is an entity of Community Mobilization Prince Albert (CMPA). CMPA is a multi-layered and multi-partner strategy to build safer and healthier environments through investments in individuals, families, neighborhoods, businesses, schools and the overall community. The strategy is accomplished through the prevention, intervention and suppression of crime and violence, the reduction of victimization and its effects, and the integrated treatment of the conditions which give rise to both.

The aim of the HUB is to coordinate agencies and their resources through a central process to meet client needs within a 48-72 hour period. The HUB exists to bring services to clients as opposed to clients finding the services.

The HUB provides immediate coordinated and integrated responses through the mobilization of resources to cases of individuals and / or families in the Prince Albert area with acutely elevated risk factors which place people in imminent danger, as recognized across a range of service providers.

c) Definitions

Personal Health Information (PHI)[10]: with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information

Personal Information[11]: personal information about an identifiable individual that is recorded in any form and includes information that relates to health care that has been received by the individual or to the health history of the individual. All references in this policy to personal health information include personal information.

Client means patient, client or resident.

d) HUB Participation

Programs within the PAPHR shall work to resolve client issues internally first. When all options within a program have been exhausted or the need to coordinate multiple service providers exists, and there is a belief that disclosure to the HUB is required to minimize danger to the client, the program can prepare to bring the client's case to the HUB.

The programs participating formally in the HUB under the Prince Albert Parkland Health Region include, but are not limited to, Acute Care, Home Care, Mental Health, Public Health and Addiction Services. Other programs may refer a client to the HUB as necessary.

[10] HIPA Section 2 (m)
[11] LAFOIP Section 23 (1) (c)

Each program area is responsible for developing an internal process for preparing a client's case to present to the HUB in compliance with this policy.

e) Disclosure of Personal Health Information

Step 1 - Disclosure <u>with</u> Consent

Client consent will be obtained and documented prior to disclosure of personal health information to the HUB. The client shall complete the *Consent for Disclosure of Personal Health Information to a Third Party* form. This applies when bringing cases forward to the HUB or when another agency in the HUB brings forward a case and PAPHR is aware of relevant personal health information.

If written consent is not practical (i.e. client is only available by phone), verbal consent may be obtained but must be noted in the client's health record.

When seeking consent is not considered practical (i.e. client is not accessible or an immediate response is required in HUB setting), follow protocol in Disclosure without Consent section.

Disclosure <u>without</u> Consent

<u>Personal Health Information</u>

Before a health care provider is authorized to disclose a client's personal health information without the client's consent, the health care provider must review their program's process for disclosure of personal health information to the HUB, as well as the legislation applicable to their program.

As per clause 27(4) (a) of HIPA, PAPHR may disclose personal health information *where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person.* All of the following factors criteria must be met:

- <u>Must be a reasonable expectation of probable harm</u>
  Reasonable expectation of harm refers to a confident belief that harm will occur to an identifiable person(s). The likelihood of the occurrence of harm must be genuine and conceivable. In other words, the probability of the harm must be more than a cautious approach to the avoidance of any risk.

- <u>Harm must constitute damage or detriment and not mere inconvenience</u>
  The degree of anticipated harm must be significant. The harm must relate to serious physical injury or mental trauma or danger to an identifiable individual(s).

- <u>Must be a causal connection between the disclosure and the anticipated harm</u>
  There must be a clear and direct link between the disclosure of specific information and prevention and minimization of the alleged harm. PAPHR must be able to provide an explanation as to how or why the disclosure will prevent or minimize the expected harm.

In specific situations, other section of HIPA may apply. In cases where the above criteria are not met and client consent is not practical, please contact your supervisor and the PAPHR Privacy Officer.

Prior to referring a client to the HUB without consent, the HUB referral form (Appendix A) must be completed.

Disclosure at HUB – Other Agency Cases

If another agency refers a client to the HUB and PAPHR has relevant personal health information related to the client, information may be released based on the above criteria using professional judgment when the disclosure is time sensitive and requesting consent is not practical. Steps 7 through 9 must be followed when this type of disclosure occurs.

Mental Health Information

As per section 18 of *The Mental Health Service Regulations* (Sask), information may be disclosed to assist the client to receive other services which are necessary to maintain or restore the mental health of the client. Mental Health Providers wishing to refer a client to the HUB must seek consent where practical. Where not practical, the "Authorization to Disclose" form in Mental Health/Addiction Programs' Disclosure of Client Information Policy 160-30-05 must be completed.

Public Health Information

As per clause 65(2)(a)(i) of *The Public Health Act* (Sask), disclosure is permitted to administer *The Public Health Act*, the regulations or any bylaws made pursuant to the Act.

f) Good Faith Clause

All Disclosures of personal health information without consent must be made in good faith, in accordance with this policy, HIPA, other relevant Acts and Regulations of the program area, and applicable professional and ethical guidelines.

As per Section 61 of HIPA, trustees and employees of trustees are protected from legal action if the disclosure in made in good faith.

g) Multi-Agency Client Meeting

A member of the HUB may decide to attend a meeting (commonly referred to as a "door knock") in emergent circumstances. Involvement is appropriate when:

- The criteria for harm is met; and
- In the health care provider's professional judgment, this intervention will not negatively affect the client/provider relationship.
    a. In such cases, a healthcare provider who has not been involved in the care of the client may be assigned to attend.

Upon attendance at the meeting, agreement to participate from the client will be sought.

h) Documentation of Disclosure

Disclosures of personal health information to the HUB (with or without client consent) must be documented in the client's chart, specifically:

a) The name of the **person(s) / organization(s)** to whom the care provider disclosed the personal health information to;
b) The date and time of the disclosure;
c) The purpose of the disclosure;
d) A description of the personal health information disclose; and
e) Documentation of patient/client/resident consent (if applicable).

Where the disclosure is made without consent, the care provider must take reasonable steps to ensure that the client is informed that their personal health information was disclosed.

i) Need-to-Know and Minimum Amount of Information

When disclosing personal health information to the HUB, the health care provider must ensure that:

- The personal health information is disclosed on a need to know basis only; and
- Only the minimum amount of personal health information that is reasonably necessary to benefit the health or well-being of the patient/client/resident.

Note: The Section 10 Referral Form Appendix from this policy has been removed for the purposes of these Guidelines.