Date: November 10, 2014

SASKATCHEWAN
INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT 105/2014

Community Mobilization Prince Albert

Summary: In 2011, the Information and Privacy Commissioner's (IPC) office learned of a new program in Saskatchewan known as the Hub. The Hub is part of Community Mobilization Prince Albert (CMPA) with participation from various agencies. The IPC undertook an investigation into the program early in 2013 to determine to what extent the Hub project conforms with the legislative requirements of *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), and *The Health Information Protection Act* (HIPA).

The Commissioner found that though different participating agencies had developed and/or implemented various policies, procedures, agreements and forms, none had developed all of the necessary components of a privacy program to fully address varying roles and responsibilities. A number of recommendations were made including that all partner agencies need to work together to ensure that the need-to-know and data minimization principles are consistently applied and to develop a comprehensive plan to address existing deficiencies of its privacy program. The Commissioner further recommended that when there is a review of access and privacy legislation that consideration is given to bringing municipal police services under LA FOIP.

I BACKGROUND

[1] In 2011, my office learned of a new program in Saskatchewan known as the Hub. Since that time, the number of Hubs in Saskatchewan has grown.

[2] In terms of how many Hubs are operational or soon will be in Saskatchewan, the Ministry of Justice (Justice) advised us on February 28, 2014 as follows:

> As of January 2014, Hub regions/communities include:
>
> - Prince Albert (February 2011); Yorkton (April 2012); La Ronge (November 2012); North Battleford (November 2012); Moose Jaw (January 2013); Estevan/Weyburn (May 2013); Nipawin (September 2013); Lloydminster (December 2013); and Swift Current (January 2014).
>
> As of January 2014, Hubs in the development phase and expected start up dates are:
>
> - Saskatoon (April 2014); Meadow Lake (April 2014); Onion Lake (September 2014); Fort Qu'Appelle (September 2014); Regina (September 2014); and Melfort (September 2014).

[3] This report however only considers the Hub in Prince Albert, a component of Community Mobilization Prince Albert (CMPA). CMPA is part of a broader provincial strategy called Building Partnerships to Reduce Crime (BPRC website, http://saskbprc.com/.) CMPA is overseen by an Executive Steering Committee which consists of senior decision-makers from local, regional and provincial participating agencies (Memorandum of Understanding and Agreement to Organize, p. 5).

[4] Though integrated service delivery is not new to Saskatchewan, the Hub initiative appears more sophisticated in terms of structure and dedicated resources provided by various participating agencies on an ongoing basis. This program is also unique as there is no age limit on the individuals brought to the table for discussion.

[5] In terms of outcomes, the following is noted about the program:

> One of the most important aspects of this project was ascertaining the success achieved by the Hub model. Although no quantitative data were available to empirically verify the success of Hub, a considerable amount of interview data from different respondents provides at least some indication that a number of successes have been achieved. (*Risk-Driven Collaborative Intervention – A Preliminary Impact Assessment of Community Mobilization Prince Albert's Hub Model*, May 2014)

[6] The CMPA is described as follows on its website (www.mobilizepa.ca):

> CMPA is comprised of 2 components, the Hub and the COR which work in different ways and at different levels to help address the growing needs of the community to improve community safety and wellness.
>
> The Hub meets twice weekly to address situations of elevated levels of risk for individuals or the community at large. For example, this might be an elevated risk of re-offending, relapsing on a treatment plan, becoming a victim or becoming homeless, etc. …
> …
>
> CMPA is an effective 2 tiered, integrated multi-agency team working in collaboration. The first layer, The HUB, is tasked with identifying risk of individuals and families and mobilizing appropriate services. The second level, The COR, works on a broader focus of long-term community goals and initiatives, possible systemic recommendations arrived at via experience, research and analysis.

[7] In terms of the participating agencies, the following are bound by the corresponding provincial access and privacy laws:

- Ministry of Social Services – *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Health Information Protection Act* (HIPA);
- Justice (Corrections and Policing) – FOIP and HIPA;
- Board of Education for the Prince Albert Roman Catholic Separate School Division No. 6 – *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP);
- Board of Education for the Saskatchewan Rivers Public School Division No. 119 – LA FOIP;
- Prince Albert Parkland Regional Health Authority - LA FOIP and HIPA; and
- City of Prince Albert – LA FOIP.

[8] My office has no authority over some participating agencies including the Prince Albert Grand Council (PAGC), Prince Albert Police Service (PAPS) or the Royal Canadian Mounted Police (RCMP). The RCMP is however bound by the federal *Access to Information Act* and the *Privacy Act.*

[9] Each participating agency designates personnel to participate in Hub discussions and for those that participate in it, the Centre of Responsibility (COR), but they remain employed

by their home agency. In terms of CMPA positions, an Executive Director (also Chair of the Hub discussion since February 2011), an Administrative Assistant, a Tactical Analyst and a Strategic Analyst, are funded by Justice but remain employees of the PAPS. Seconded COR members from participating agencies are subject to the direction, supervision, and management of the Executive Director.

[10] My office's investigation began in early 2013 with final submissions received from the participating agencies in early 2014. My office conducted group interviews with participating agencies and had individual program participants fill out questionnaires. We also examined case samples from 2011 to 2013. Site visits and demonstrations of information systems were also arranged.

[11] As part of this process, my office also reviewed guidelines, agreements and other materials provided and as were available on various websites. Also considered was a *Draft for Discussion Privacy Impact Assessment Community Mobilization Prince Albert: the Hub* (Hub PIA) prepared by a provincial Information Sharing Issues Working Group (ISIWG) consisting of the Ministries of Justice, Health, Social Services, and Education. That committee has been working on the broader issues of privacy as it relates to the Hub process as well as other processes.

[12] Information and Privacy Commissioner (IPC) personnel also observed a Hub meeting on Tuesday, December 10, 2013 in Prince Albert with 17 individuals from the participating agencies including CMPA staff also in attendance.

[13] This particular investigation involved looking for evidence that the Hub project conforms with the legislative requirements of FOIP, LA FOIP and HIPA insofar as it involves government institutions, trustees and local authorities collecting, using and disclosing personal information or personal health information of individuals.

[14] My office did not look for authority or lack thereof for every data transaction involved with every Hub case examined as that would have required far more detailed responses from the participating agencies and much more time to conduct the analysis.

[15] I thank all the participating agencies for their cooperation throughout this process.

II DISCUSSION OF THE ISSUES

[16] My authority for this investigation is a combination of section 33 of FOIP, section 32 of LA FOIP and section 52 of HIPA. Section 33 of FOIP provides as follows:

> **33** The commissioner may:
>
> (a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs;
>
> (b) after hearing the head, recommend that a government institution:
>
> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal information that is collected in contravention of this Act;
>
> …
>
> (d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.

[17] Section 32 of LA FOIP and section 52 of HIPA have similar wording.

1. Are CMPA practices in keeping with provincial access and privacy laws?

[18] Though not contemplated in FOIP, LA FOIP or HIPA, some jurisdictions include specific provisions enabling common or integrated programs (i.e. British Columbia, Alberta, and Manitoba). This program appears to constitute something similar but is not presently enabled by legislation in Saskatchewan. If the government were to introduce any such amendments, I would expect that the provision(s) would enable disclosure for the clearly defined purposes of a common or integrated program or service, and only if necessary for the performance of the duties of the officer or employee of the agency to whom the information is disclosed. There should be a further requirement that limits disclosure to only those parties that have entered into an appropriate written information sharing

agreement. Further, every participating agency should be integral to the program or services provided and have clients in common. Preferably, all agencies involved would be bound by an access and privacy law, provincial or federal. If this is not possible, I would recommend that at a minimum those bodies not otherwise bound by access and privacy laws, enter into written agreements to agree to compliance with FOIP, LA FOIP and HIPA.

[19] Another challenge with such a program, with so many different participating agencies, is how a breach of privacy investigation would be undertaken if a client raises a concern. My office did not find any public source of information that stated that individuals have the right to raise privacy related concerns, to whom or how.

[20] The Hub PIA states:

> 1.2.9. Openness
> …
>
> The BRPC and CMPA should include on these websites, information about the information sharing practices of the Hubs including the purpose for collection, how the information will be used and disclosed, how the information is protected, how individuals can request access and who to contact with privacy questions or concerns.

[21] I agree that this type of information should be placed on the websites of all participating agencies including CMPA's and a process needs to be developed as to how to respond to privacy complaints with clearly defined roles.

[22] When asked about the apparent lack of notice regarding a designated Privacy Officer, my office was informed that the Strategic Analyst would act as Privacy Officer for CMPA. He however does not have any specific access and privacy training and is an employee of PAPS not bound by any access and privacy law.

[23] The following description of a Hub discussion is taken from the Hub PIA:

> We were informed that the Hub meets twice weekly at 10:30am on every Tuesday and Thursday. The purpose of the meeting is to discuss situations in which 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 on reducing the possibility of the situation worsening to the point where more significant problems emerge, including more formal interventions from the police, social services, etc. It is expected that an agency only brings those situations to the Hub that the agency has determined may involve risk factors beyond its our [sic] capacity to address and thus represent situations that could be much more effectively addressed in a multi-agency manner.
>
> Part of a Hub discussion is the identification of specific tasks to be undertaken by one or more 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 could appropriately be met by those tasks or if more tasks need to be undertaken.
>
> A typical agenda for a Hub discussion will include:
>
> - Preliminary matters;
> - Review of existing situations/discussions; and
> - Introduction of new situations
>
> …
>
> 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 solution. …
>
> The meeting ends with a review of what has been decided so that agencies involved are in agreement on the actions.

[24] In terms of changes to the program over the years, we were advised as follows:

> Starting on September 4, 2012, the four filter process was implemented. This means that personal information and personal health information will only be shared verbally at the third filter. Further, personal information and personal health information may be recorded by only those agencies who have been identified to have a role to play.
> ...
>
> Matters do not end at stage four. Stage four is where the agencies who have been determined to have a role to play, discuss and strategize next steps going forward (i.e. whether a door knock is appropriate, what services they are going to offer, etc.). (Response to PIA questions, September 16, 2013, pp. 2, 5 & 6)

[25] We requested the following documentation on case samples from the participating agencies:

> Any records (information in any recorded form) presumably including memoranda, correspondence, handwritten notes, electronic records, etc that are in either the possession of the partners or outside of their possession but under their control. As clarified during the meeting, our office will be looking at any material that was produced by the partners: (a) prior to bringing a case forward to the table for discussion at HUB (i.e. demonstrates screening process); (b) any speaking materials (i.e. notes, etc) regarding cases discussed at HUB meetings; (c) any material that was produced in the course of the meeting and (d) any follow-up material generated as a result of a HUB discussion once it was identified that an agency had a role to play. We are not seeking full copies of client case files from any of the partner agencies, only that which documents the reasons for escalation, and whatever follow-up is decided by the partners.

[26] When our office was provided the case samples requested, two tables were provided. The first table titled *CMPA Records Pre September 2012 Discussions* included names and date of births (DOBs) of the clients along with an ID (case number). The second table is a printout with a footer that reads: "Community Mobilization Prince Albert…Post September 2012 files." No names and DOBs are included.

[27] It is my understanding that from September 1, 2012, to February 12, 2013, specific Hub data was saved locally on an excel spreadsheet. Starting February 14, 2013, the data was entered online into BPRC's centralized Hub database hosted by Justice (*Report on the Hub Discussion 2012/2013: A Documentation of the Prince Albert Hub Discussion Study Period: September 1, 2012 to August 31, 2013, A Submission to CMPA's Operational COR Committee* (Report on the Hub Discussion 2012/2013), October 28, 2013, p. 8). In the course of this investigation, my office learned that though the data entered into the BPRC database is not in identifiable form, other databases did exist with identifiable data.

[28] Based on what was requested, we expected to see detailed information as to each client including particular risks factors and what other traditional approaches had failed. Further, we looked to see in how many of the case samples referral forms were used. Only 25% of cases involved a referral form. We learned that not all participating agencies had or used referral forms.

[29] Screening is the first step in the process of bringing a matter to the Hub table. Referral forms offer a way to document necessary information succinctly. There is also a second risk assessment conducted at the Hub table after presentation by the originating agency that also needs to be captured.

[30] Justice provided our office with a copy of the *Hub Database Glossary of Risk Factors*. At the top of the page it states: "risk factors are conditions of presumed risk that elevate the probability of harm to a significant interest at stake. They are believed to be true; and are related to the onset of acutely elevated risk." It is a seven page table with three columns: risk variable, risk factors and definitions. At this point, there is no reference to "acutely elevated level of risk" or "acutely elevated risk" in FOIP, LA FOIP or HIPA.

[31] The following is taken from a document provided by ISIWG, *Interim Information Sharing Guidelines For Community Mobilization and Hubs* (Guidelines) dated April 2013 regarding acutely elevated risks:

> 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. Community Mobilization Prince Albert puts it this way:
>
> > …the Hub participants have adopted a threshold test for determining the substance of their 'discussions', and that threshold combines both the degree of probability of harm involved in any given situation, and the degree to which the operating risk factors involved cut across multiple human services disciplines. Taken together, these combined factors represent acutely elevated risk. Situations meeting this threshold are thus likely to benefit greatly from collective problem solving at the Hub table, and from the immediate cooperative action taken forward from the Hub meetings by the most appropriate agencies.

[32] Facebook was mentioned as a source of information regarding risk in a couple of cases examined.

[33] Personal information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

[34] The standard of accuracy in FOIP is as follows:

> **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.

[35] Section 26 of LA FOIP and section 19 of HIPA are similar to the above.

[36] The Newfoundland and Labrador IPC stated the following regarding the use of Facebook in its Report P-2012-001:

> [15] … Regardless, even where these arrangements are in place, it is the position of this Office that Facebook, and other social media websites should not be used by public bodies to collect, use or disclose personal information.
> …
>
> [18] There are numerous examples of privacy authorities in Canada and around the world, as well as the courts, dealing with the aftermath of people's assumptions about how private Facebook really is. Facebook is a great tool for municipalities to inform people about festivals, application deadlines, respond to inquiries about operating hours of facilities, etc., but it is not a means for municipalities to use or disclose personal information. No personal information should be collected, used or disclosed by a public body in any context via social media except as described above, and the collection and use of personal information through Facebook should be done minimally and only in compliance with the *ATIPPA*.
> …
>
> .... Facebook does not check nor is it able to confirm the identities of account holders in this manner. It is possible for someone to create an account in the name and likeness of someone else without consent. …

[37] An example of how Facebook may be a source of inaccurate information is the following excerpt from the Privacy Commissioner of Canada's Report of Findings #2013-010:

> A mother complained that someone had created a Facebook account in her teenaged daughter's name. While this teenaged girl didn't even have a Facebook account, the imposter made contact with schoolmates who did and made inappropriate comments about them.

[38] My office discourages the use of Facebook as a data collection tool by <u>any</u> of the participating agencies including CMPA for the reasons noted.

[39] After the screening process, the originating agency brings a client case to the Hub table to discuss. This Filter and Filter 2 are described on the BPRC slide deck provided to our office by Justice, February 28, 2014, as follows:

> Privacy Filter #1…
> - Screening applied at the agency level using internal process – referral form
> - Acutely Elevated Level of Risk?
>
> More questions…
> - Were the agency's traditional options exhausted?
> - Are the risks spread across multiple agencies?
> - Is it beyond the agency's scope or mandate to mitigate the risk alone?
> - 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 the 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?
>
> Still not sure…
>
> ***Bring it*** to the table, present it in a non-identified format, and if the Hub feels it does not meet the next filter, after the Hub consult directly with those agencies to which the risk involve.
>
> If you aren't sure whether to table a Hub discussion, there likely is an element of elevated risk that should be addressed.
>
> Privacy Filter #2…
> - The discussion first is presented to the table in de-identified format.
> - The Hub table then decides that the discussion meets the threshold of Acutely Elevated Level of Risk.
> - If filter 2 is not passed the discussion ends without having shared identifiable information.
> - If filter 2 is passed the agencies are of the opinion the discussion continues to meet the threshold of Acutely Elevated Level of Risk.

[40] In terms of sufficiently de-identifying data, my office found that participants were not always clear as to what this entails. During the December 10, 2013 meeting, actual client ages were shared instead of age ranges as indicated is the practice in the Hub PIA. This was in addition to other direct and quasi-identifiers being shared by participants. Due to the uniqueness and combination of these types of data elements along with the sheer

volume of information shared, more needs to be done to prevent early identification of specific clients at these initial stages of the Hub table discussion.

[41] From the same slide deck is the following description of Filter 3:

> Privacy Filter #3…
> - Limit the personal information relevant to the current risk
> - Agencies involved are identified
> - Does a connection to services exist?
> - 'number the discussion' and create a de-identified central record in the BPRC Hub Database.
> - Only Lead and Assisting Agencies take notes, noting the number assigned in the BPRC Database in agency Hub notebooks.

[42] Based on statistics available from the Report on the Hub Discussion 2012/2013, it appears that 21% of cases were rejected by the group as criteria were not met. If a fuller assessment was done ahead of time, I would expect virtually no cases would be screened out before Filter 3. More time spent on screening may help to alleviate this possibility.

[43] A standard referral form needs to be used by all partner agencies to ensure consistency in the screening process. In addition, all program participants should receive training in its proper use.

[44] During the Hub meeting on December 10, 2013 when name and DOB of two individuals under discussion were shared at the Hub table, none of the 17 participants left the room prior to or after the reveal. My understanding is that once name and DOB are revealed, only the lead and any assisting agencies are instructed to take notes. This nonetheless raised concerns regarding need-to-know.

[45] My office also learned that sometimes visitors attended Hub discussions. Though visitors were required to sign non-disclosure agreements, caution must be taken when allowing outsiders to attend when identifying information is to be shared.

[46] Even though personal information under FOIP and LA FOIP is defined as information about an identifiable individual in recorded form, as long as the agency that is disclosing

it verbally has that information recorded somewhere, the disclosure rules of FOIP or LA FOIP still apply.

[47] "Personal health information" is defined by HIPA as follows:

> **2**(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;

[48] The personal health information need not be recorded anywhere for HIPA to apply.

[49] Personal information or personal health information may be used for purposes for which it was obtained or compiled, for a consistent use or for purposes it may be disclosed. Section 28 of FOIP provides as follows:

> **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).

[50] Section 27 of LA FOIP and section 26 of HIPA are similar.

[51] Other authority to disclose without consent are found in subsection 29(2) of FOIP, subsection 28(2) of LA FOIP and subsections 27(2) and 27(4) of HIPA along with other disclosure provisions in each Acts' Regulations.

[52] In the case samples provided, authority for use and disclosure was rarely noted. It is important to notify clients of anticipated uses and disclosures of their personal health information as is an explicit requirement of HIPA. If not recorded or logged, how can it be later explained to a Hub client?

[53] In terms of the decision to disclose, the authority relied on under FOIP, LA FOIP and/or HIPA should be consistently documented. This way, if compliance is ever challenged, then the agency in question will be better positioned to defend its actions and decision-making. Referral and consent forms, if containing all the necessary elements, may act as a consistent way to document such decisions and authorization.

[54] A further concern I noted is that different agencies have different practices without any clear guidelines or procedures to ensure consistency in approaches to documentation and record management. In order to ensure the right information is available to the right people at the right time, this needs to become standardized as well. Included with this should be clear guidance on how to sufficiently de-identify personal information and personal health information.

[55] Further, at Filter 3 when name and DOB is going to be shared, additional information need not necessarily be disclosed by other participating agencies. The reason the individual's name is brought forward is because of *present* circumstances and the belief that the individual is *presently* suffering from an acutely elevated risk. In terms of the need for a present intervention, prior known information may or may not have any relevance.

[56] No need-to-know exists when the client under discussion (identifiable) is not one that the agency or professional has no services to offer for the "benefit of the subject individual" or "to minimize risk of harm." For example, for the study period September 1, 2012 to

August 31, 2014, one agency was only involved in 4% of cases discussed. If so rarely involved, then we would expect this professional would not often have the requisite need-to-know to be present during Filter 3.

[57] No participating agency provided us with a definitive answer regarding authority to share identifiable information with all 17 Hub participants. However, it was suggested that perhaps consent was provided to permit disclosure to the broader group in at least one of the two cases.

[58] Consent should be sought and recorded prior to bringing a client's case to the Hub table and if the decision is made that it is not reasonably practicable to obtain consent, the reasons noted for why it could not be obtained need to be recorded.

[59] The final filter is Filter 4. As described by the aforementioned BPRC slide deck:

> Privacy Filter #4…
> - This takes place after the meeting and away from the table
> - Only lead and assisting agencies participate in the discussion
> - Interventions should occur within 24-48 hours
> - The discussion ends as soon as the agencies decide that the acutely elevated risk is mitigated.

[60] Actions taken by Hub participants can include a "door knock" or "visit to an individual or family deemed to be in need of services. ... If accepted, the services are then provided by the individual agencies as part of normal business..." (Hub PIA, p. 85). Further, there is reporting by those that intervened back to the Hub table at some point. The office did not examine these practices in the course of this investigation, but recommend that authority be established and documented, if not already, to ensure any data sharing complies with FOIP, LA FOIP and/or HIPA.

[61] The focus of this investigation involved Hub discussions. However, another component of this program is that work being conducted by COR members including research.

[62] Subsection 28(2)(k) of LA FOIP is a similarly worded provision to subsection 29(2)(k) of FOIP regarding disclosures for research purposes. Subsection 29(2)(k) of FOIP provides as follows:

> **29**(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:
>
> …
>
> (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;

[63] The HIPA provision is quite different as follows:

> **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 using de-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.

[64] The office learned that sometimes COR members sit in on Hub discussions to understand the Hub and/or to fill in for a missing Hub participant. In addition, COR members may attend a door knock if the Hub representative cannot.

[65] Hub participants are involved in interventions requiring identifiable information. COR members have a distinctive role separate and apart from his or her previous position with his or her home agency. These are different roles with separate rules that apply.

[66] It appears that in some cases, COR members may have access to his or her home agency's record holdings even though acting in a different role than usual. If research is to be conducted with de-identified data only, then the COR member conducting the research should not have access to any identifiable data. Further, although COR members are still employed by its home agency, if conducting research for this program, it is doing so for an outside entity. Any pre-existing need-to-know associated with former roles no longer exists.

[67] Restricting employee access to databases, folders and other sources of data to only those that the individual has a demonstrable need-to-know is a necessary safeguard. In this regard, the following from Investigation Report F-2012-005 is helpful:

> [92] ISO recommends the following with regards to user access privileges:
>
> > Objective: To ensure authorized user access and to prevent unauthorized access to information systems.
> >
> > Formal procedures should be in place to control the allocation of access rights to information systems and services.
> > …
> > The access control procedure for user registration and de-registration should include:
> > …
> > c) checking the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 10.1.3);
> > …
> > i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4).

[68] Further, IPC personnel were present at the Hub table when a study flag was noted. It is unclear what type of data collection this entails and how it is accomplished. To ensure compliance with access and privacy laws, a PIA on uses of personal information and personal health information for secondary purposes related to the program is warranted.

2. What is the impact of law enforcement on CMPA activities?

[69] On the questionnaire that Hub participants filled out, we asked the question: "What is your understanding of the police's role in Hub?" Some responses provided are as follows:

> "Police assist with interventions & discussion regarding criminal involvement/concerns. Explain concerns from police perspective to hub discussions/individuals. Ensure safety."
>
> "There is a designated officer who attends Hub meetings and attends interventions. They access CPIC when required for addresses/criminal history etc."

> "I understand they bring the enforcement (law) perspective to the table and also help Hub clients understand what their consequences could be."
>
> "The Hub is definitely a crime reduction, police driven organization. The police (in my experience) have taken the role of lead organization."

[70] PAPS also advised us in its March 7, 2014 submission of the following:

> In the study period September 1, 2012, to August 31, 2013, PAPS was involved as lead or assisting agency in 79% of situations discussed at the Hub. These are no statistics collected on how many door knocks each agency is participating in. It is likely that in almost 100% of the situations PAPS was involved in there would have been at least one door knock per situation.
>
> The role of the PAPS member is to contribute the part PAPS can contribute to mitigate the acutely elevated risk situation which will consist of some form of policing services. What those are in detail will differ depending on the specific circumstances of the risk situation at hand.

[71] The RCMP indicated in its March 3, 2014 submission: "The only interventions that the RCMP has participated in are "door knocks". … Our main role is to keep the peace."

[72] Privacy laws in Saskatchewan contemplate circumstances in which personal information and personal health information may be disclosed to law enforcement. In reviewing the submissions from participating agencies including the case samples, legal authority for these disclosures were not noted. This is not to say that authority does not exist, rather, it was not clearly documented in the case materials provided.

[73] It was indicated that the Tactical Analyst has access to the PAPS Records Management System including CPIC to carry out her participation in the identification of situations for the Hub discussions.

[74] Suicide is a risk factor that may come under discussion. If recorded, this detail may follow the individual throughout their lifetime whether or not it is a current concern or if it was ever confirmed. What is the potential consequence of this when law enforcement is represented at the table?

[75] The Ontario IPC report dated April 14, 2014, titled *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC* speaks to this concern:

> CPIC contains a vast array of public safety information, including personal information related to criminal activity, warrants for arrest, missing persons, suicide attempts or threats, and apprehension warrants under the *Mental Health Act*. I learned that there is currently a Memorandum of Cooperation between the RCMP and the U.S. Federal Bureau of Investigation (FBI), providing the FBI with access to CPIC. I also learned that the FBI grants access to the CPIC database to the U.S. Department of Homeland Security, which includes U.S. border officials.
>
> According to the RCMP, local Police Services have complete discretion as to whether information related to a suicide attempt is recorded on CPIC. … As a result, information related to suicide attempts in these Police Services may be added to CPIC in some, but not all circumstances. The Toronto Police Service, on the other hand, exercises no discretion – their policy requires that police officers upload information related to every threat of suicide or suicide attempt to CPIC.
>
> All the mental health professionals and organizations that I consulted were opposed to such a "blanket" rule requiring the automatic disclosure of all suicide-related information via CPIC. There was a consensus among these groups regarding the extreme sensitivity of mental health-related information, the significant potential for stigma flowing from access to and use of that information, and the risk that the very information collected may be inaccurate or incomplete – all pointed to the need for this information to be treated with great discretion and considerable caution.
>
> …
>
> Information relating to our health goes to the "biographical core" of each of us and is deserving of the most sensitive treatment and highest standards of protection. The disclosure of information about our mental health can have devastating consequences, well beyond the impact of the disclosure of other medical health issues. This is particularly the case where, as in these circumstances, the information may be incomplete or open to inappropriate interpretation. Although significant strides have been made by the mental health community and others to increase the awareness of mental health issues and reduce the stigma associated with them, this stigma has not been eliminated. These circumstances justify a cautious and measured approach to any disclosure practices related to this type of sensitive personal information. (Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, April 14, 2014)

[76] If law enforcement agencies are to be involved when mental health information is disclosed, it is critical that the information in question is clearly established and necessary

to record as there may be unseen future consequences. Accordingly, I further recommend that the Ontario Commissioner's Mental Health Disclosure test be adopted here in Saskatchewan discussed elsewhere in the above noted report.

[77] My office also asked PAPS for what specific training it provides to its members participating in Hub discussions or COR work in terms of how to: de-identify personal information, protect privacy, maintain confidentiality, and adhere to the need-to-know and data minimization principles. No specific privacy related training is noted in its response.

[78] In most other Canadian provinces, adherence to privacy principles is ensured by making police services subject to the same access and privacy law as other public sector organizations. To bring law enforcement practices in alignment with other participating agencies, I recommend that when there is a review of access and privacy legislation that consideration is given to bringing municipal police services under LA FOIP. This is important as the police appear to play an integral role in Hub/COR and would therefore be bound by the same privacy provisions of other participating agencies.

III FINDINGS

[79] Though different participating agencies have developed and/or implemented various policies, procedures, agreements and forms, I did not find that any had developed all the necessary components of a privacy program to fully address varying roles and responsibilities.

IV RECOMMENDATIONS

[80] In summary, I recommend:

1. That the partner agencies work together to ensure that the need-to-know and the data minimization principles are consistently applied. This should include the following:

a. Development and mandatory use by all partner agencies of a standard referral form. It should include all the elements recommended in this preliminary analysis.

    i. All program participants must receive training on its proper use.

b. A restructuring of Hub table discussions that includes:

    i) Only those with a demonstrable need-to-know remain in the room past filter 2.

c. That authority is clarified for post Hub interventions and for any research undertaken by any partner agencies.

    i. Agencies restrict staff access to data holdings where need-to-know cannot be established.

    ii. Complete a joint Privacy Impact Assessment addressing COR activities to ensure compliance with FOIP, LA FOIP and HIPA.

d. That there is a clear segregation of duties between Hub and COR representatives.

e. All databases, lists or excel spreadsheets linking case number and client names be destroyed.

2. That a comprehensive plan is developed and implemented to ensure deficiencies pertaining to agreements, policy, procedure, notice, training and documentation are addressed in a consistent way by all partner agencies. For example, this plan should address the following:

    a. Consent. The default should be to seek consent of individuals. If consent is not sought then reasons should be documented. During Filter 1 discussions, originating agencies should indicate if consent was obtained.

    b. Notice. Information provided on partner websites should include details about CMPA information sharing practices, how individuals can request access and who to contact with privacy questions or concerns.

        i. A process needs to be developed for responding to privacy complaints and the program's designated Privacy Officer should receive access and privacy training.

    c. Accuracy. Some specific issues to address include:

        i. Facebook should not be used as a data collection tool.

ii. Unconfirmed or suspected risk factors

1. A requirement to confirm mental health information when law enforcement is involved and further to adopt the Ontario Commissioner's Mental Health Disclosure test if possible disclosure via CPIC is being considered.

d. Record keeping. Decisions and authority need to be documented.

e. Need-to-know, data minimization and de-identification.

3. That when there is a review of access and privacy legislation that consideration is given to bringing municipal police services under LA FOIP. At the same time, amendments should be introduced to clarify the rules for interagency sharing in FOIP, LA FOIP and HIPA including a requirement for partner agencies to enter into written information sharing agreements when they participate in common integrated program delivery.

[81] My office shared its preliminary analysis with the Ministry of Justice on September 9, 2014. On October 10, 2014, the Ministry of Justice advised us as follows:

> We are pleased to inform you that we accept the recommendations and intend to work towards compliance as follows:
>
> 1. The Ministry of Justice will work with the partner agencies towards improved and consistent application of the need-to-know and the data minimization principles. This will include:
>
> a. Development of a standardized referral form template to be used by all participating agencies. The intent is to develop a form that ensures consistent practice with regard to core elements of the referral (consent, authority, etc.) but allows adaptation to individual needs.
>
> b. Development of a training strategy to ensure consistent training of Hub participants and participating agencies, including ensuring program participants receive training on proper use of a standardized form.
>
> c. Modifying the Four Filter process (and thus the Hub discussions) and considering legislative amendments to ensure personal information is only disclosed as needed to support the service during the Filter 3 phase. It is the Ministry's view that central to identifying the necessary service and/or service providers that may be required to further participate in the discussion to alleviate acutely elevated risk, at some point during Filter 3, discussions on limited identifiable information may need to be shared. The proposed regulations will address this issue.

d. Clarifying authority for post Hub interventions and for any research undertaken by any partner agencies in relation to Hub/COR activities. This includes ensuring agency staff access agency data holdings only where a need-to-know is established.

2. Justice will cause a joint Privacy Impact Assessment addressing COR activities to be completed. Processes and policy will be reviewed to ensure there is a clear segregation of duties between Hub and COR representatives.

3. Any databases, lists or excel spreadsheets held at the CMPA linking case number and client names will be destroyed. A de-identified database will remain with the COR. Partner agencies will retain internal cross references to Hub cases for which they have a client relationship.

4. Justice will lead the development and implementation of a comprehensive plan to improve how access and privacy is addressed in agreements, policy, procedure, notice, training and documentation by all partner agencies, including approaches to consent, providing notice, accuracy, record keeping, decisions, documentation, need-to-know, data minimization and de-identification.

5. Legislative change will be pursued to clarify rules for interagency sharing of personal information and personal health information including a requirement for partner agencies to enter into written information sharing agreements when participating in common integrated program delivery.

6. Finally, inclusion of municipal police services will be considered as part of any future review of access and privacy legislation.

As you will know, the Ministries of Justice and Health have proposed a set of regulations to clarify authority for information sharing at the Hub, including requiring that participants enter into information sharing agreements before sharing information at the Hub. Those regulations, which were shared with your office in 2013, will be reviewed and updated as necessary in light of your analysis.

Dated at Regina, in the Province of Saskatchewan, this 10th day of November, 2014.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner