20,000 Homes
GUIDELINES for Dealing with Personal Information

The 20,000 Homes Campaign is a national movement of communities working together to permanently house 20,000 of Canada's most vulnerable homeless people by July 1, 2018. The campaign is led by the Canadian Alliance to End Homelessness (CAEH). In the course of the Campaign, partners will be required to collect, use and potentially disclose personal information. In order to protect the privacy, safety and dignity of the individuals whose information is collected the following guidelines are provided.

These general guidelines are not an exhaustive list of practices nor are they necessarily suitable in all cases for your agency and/or programs. Your agency may identify further and/or other guidelines as well as policies, procedures and protocol in order to establish best practices in the protection of personal information.

✓ What is Personal Information?

- In general terms, if information could lead to the identification of a specific individual, then it is considered to be personal information. Therefore, a birth date, a photograph, social insurance number or telephone number are all examples of personal information as a specific individual would reasonably be able to be identified through this information.
- Definitions of personal information are often contained in the protection of privacy legislation that is applicable to your entity. For example, the *Freedom of Information Protection of Privacy Act* in Alberta contains a lengthy definition. It is worth having a read through the definitions section of the applicable legislation (section 1 usually) to understand all of the kinds of information that are considered personal information. www.canlii.org is a free online, searchable database of legislation.

✓ Obtaining Consent

- Consent should be obtained from individuals who provide personal information to you. An informed consent which is read to the client is a preferred option for obtaining consent prior to collecting personal information. Where information is being collected on a form, the consent should be included in writing on the form.
- The consent typically includes a statement regarding what the collected information will be used for. If the information is then used for a different purpose, further consent should be obtained from the client before proceeding to use the information for the other purpose.
- The personal information collected should be required for the agency to perform its work. If some information fields are not required information that the agency needs to know in order to provide a client with a program or service, then these field could either be removed, or could be identified as optional information, which the client can then chose to complete if they wish.
- Where it is reasonable and possible, a client should always retain the right to revoke consent. That is, if the client provides an agency with their personal information and later decides they no longer want the agency to use their personal information, the client can make a request to revoke their consent and an agency should promptly comply with the client request where reasonable and possible. In most cases,

the revocation of consent will apply to all uses of the personal information after the request to revoke consent is received.

- In certain situations, consent may be obtained in non-traditional ways. For example, signage stating that particular video surveillance footage is being captured at a specific location for a specific purpose provides notice of the collection of the personal information along with what the personal information will be used for.

✓ **Accuracy and Correction of Personal Information**

- When collecting personal information, best efforts to ensure the information is correct and accurate should be made. If a client requests the correction of their personal information, the agency should promptly make such correction.

✓ **Need to Know**

- Not only is it recommended that an agency only collect information it *needs to know*, but within an agency, individual employees should only have access to and deal with information that they *need to know*. This requires a greater degree of vigilance internally – things like not leaving documents containing personal information lying on a desk or on the photocopy machine and not copying individuals on an email containing personal information where they do not have a *need to know.*

✓ **De-identification of Data**

- De-identified Data means client data that is not able to be reasonably retraced to a specific individual.
- When information is shared within an organization or with another agency in accordance with the purpose(s) for which consent was obtained, If the receiving party does not have a *need to know* the personal information, the information should be de-identified prior to being shared (or not shared at all).

✓ **Legal Compliance**

- Your agency should be aware of the protection of personal information and access to information legislation, both provincially and federally, that applies to your particular agency. The legislation that applies to your agency may be different to that which applies to another entity. For example, FOIP applies to public bodies but not businesses or not for profits that are not public bodies. Once you know what legislation applies to you, your organization should understand what the legislation requires in order for you to meet your legal obligations.
- In addition to legislative requirements, your agency may be contractually required to comply with certain obligations for privacy and confidentiality. A proper contract review process will aid in ensuring obligations are understood before contract terms are agreed to. Compliance with agreements should be monitored on a regular basis.

✓ **Secure Storage**

- All personal information should be stored in a secure location.
- If electronic documents include personal information, the documents should be password protected and passwords should be changed on a regular basis. Access privileges to electronic information stored

in flies should be properly set and reviewed from time to time to ensure that access is only possible by those within the organization that have a need to know.

- Where physical files include personal information, the files should be locked away. Ideally three locks (for example, main office front door locked, individual office door locked and filing cabinet locked) provide good safety guards against unauthorized access.
- An inventory of the type and location of all files containing personal information both in electronic and physical format should be maintained and updated on a regular basis.

✓ **Requirements of Personnel**

- All personnel should receive some training around the protection of personal information. Training should be refreshed/updated. Personnel who are regularly dealing with personal information or dealing with sensitive personal information should receive further and additional training
- Background checks of individuals in your organization who are accessing personal information may be appropriate.
- All employees, contractors, volunteers and directors should sign confidentiality agreements to protect the confidentiality of personal information and other business sensitive information. These agreements should clearly state the consequences of a breach of the agreement.
- Contracts with consultants/vendors should include terms and conditions regarding maintaining confidentiality and where appropriate, the expectations regarding reporting, remediating and mitigating a breach of confidentiality.
- A Privacy Officer should be appointed within your agency and the responsibilities of the Privacy Officer should be clarified.

✓ **Internal Policies**

- Having strong internal policies and procedures documented and explained to personnel will help to protect privacy and personal information.

✓ **Sensitive Information**

- Additional precautions may need to be made in relation to sensitive information. For example, where personal information is being collected and then shared regarding domestic violence clients, stricter procedures may be followed that surpass beyond legislative requirements in order to ensure the protection of the individual's safety.

✓ **Destruction of Files**

- Documents/files containing personal information which are no longer in use normally can be destroyed after a certain period of time usually set out within the legislation applicable to your agency. Recording the destruction of documents is recommended.

✓ **Access to Information**

- A client or another entity or individual may request the disclosure of certain personal information.

- Where a law enforcement agency requests the disclosure of personal information, request the agency to provide you with the grounds (usually a particular section of legislation) that enables your provision of the personal information to them. Ensure that the proper paperwork has been completed prior to the disclosure.
- Where information is provided pursuant to an access to information request, only the requested information should be provided and all other personal information or irrelevant information should be severed from the record that is disclose (information is most often severed by striking it out so that it is no longer visible).
- Maintain a log of all access to information requests including when they were received, from whom and when they were completed.
- Respond to access to information requests promptly. Also be aware that certain legislation may provide a time limit by which an agency must respond to an access to information request.