BC Society of
Transition Houses

Privacy, Security and Confidentiality:

Database Considerations for Canadian Anti-Violence Organizations

ACKNOWLEDGMENTS

Research, Writing, Editing:	*Rhiannon Wong* *Nicky Bowman* *Tanyss Knowles* *Louise Godard* *Amy S. FitzGerald*
French Translation:	*Michele Briand*
Graphic Design:	*Hannah Lee*

Sections of this guide have been adapted from, and in cooperation with, the Safety Net Technology Project at the National Network to End Domestic Violence, United States

We gratefully acknowledge the generous contributions of the following organizations and partners:
BC Housing
Citizen Lab, Munk School of Global Affairs, University of Toronto
Ishtar Transition Housing Society
National Network to End Domestic Violence, Safety Net Project
Rise Women's Legal Centre
The Women's Services Network
Women's Shelters Canada

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the BC Society of Transition Houses and do not necessarily reflect those of the OPC.

TABLE OF CONTENTS

BACKGROUND

The BC Society of Transition Houses (BCSTH) received funding from the Office of the Privacy Commissioner of Canada (OPC) to:

- Research the use of databases as a Privacy Enhancing Technology by Canadian anti-violence organizations;
- Survey database vendors about their database's security and ability to enhance privacy of women, children and youth experiencing domestic and/or sexualized violence; and
- Develop practical resources for anti-violence organizations currently using or looking to use databases in their work.

Anti-violence organizations provide a continuum of services which share a common mission: to support **women, children and youth** ***who experience domestic and/or sexual violence.***

In 2012, funded by the Office of the Privacy Commissioner of Canada, BCSTH in partnership with the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic began researching technology use and its intersection with violence against women. The first version of the "Privacy, Security, and Confidentiality: Database Considerations for Violence against Women Programs" was one of the resources that was developed from BCSTH's initial research. Increasingly, the collection and electronic storage of the personal information of women, children and youth accessing anti-violence organizations continues to be an important topic for discussion amongst Canadian anti-violence organizations and funders since our first grant in 2012.

According to anti-violence workers, databases help streamline the collection and storage of personal information[1] and make data more accessible. However, in the context of women, children and youth experiencing domestic and sexual violence, stalking, trafficking and harassment, having personal information stored in an electronic database can put their safety at risk through online interception,

[1] Personal information is the term used in the Personal Information Protection and Electronic Documents Act and is defined as "information about an identifiable individual" (see Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), Section 2(1), Definitions). A much fuller definition of personal information, including numerous examples of what constitutes personal information, can be found in the Privacy Act (R.S.C., 1985, c. P-21), Section 3, Definitions. Other terms that are sometimes used synonymously with personal information include personal data (see, for example, GDPR, Article 4(1)) or personally identifiable information (see, for example, National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010).

subpoenas, third party requests and data breaches. For these reasons, it is best practice that anti-violence organizations only collect and store the personal information of women, children and youth ***necessary*** to provide services for the time required.

Canada's Privacy Act defines personal information "as any recorded information about an identifiable individual. It can include…race; national or ethnic origin; religion; age; marital status; blood type; fingerprints; medical, criminal or employment history; information on financial transactions; home address; and your Social Insurance Number, driver's licence or any other identifying number assigned to you[2]." All commercial databases and the Government of Canada's Homeless Individuals and Families Information System (HIFIS) ask for personal information in their standard database product.

Due to the complex and sensitive nature of personal data collection, BCSTH receives inquiries regularly about electronic databases from Canadian anti-violence organizations and funders out of concern for maintaining women's privacy. To provide the necessary support to anti-violence organizations, BCSTH researched anti-violence organization's use of electronic databases and the safety and privacy impact of collecting and electronically storing the personal information of women, children and youth. In 2018, BCSTH distributed two surveys:

- "Electronic Database and Case Management System Use by Anti-Violence Organizations across Canada" online survey. This survey was distributed in both French and English to anti-violence organizations across Canada.
- "Database Questionnaire for the BC Society of Transition Houses." This was distributed to electronic database companies and HIFIS administrators that were identified by anti-violence workers and technology safety experts as being available in Canada.

This database considerations report is one of three resources developed from: the 2018 survey results, conversations with anti-violence confidentiality experts, database demonstrations by vendors, conversations with funders and consultations with provincial associations supporting women's shelters and transition houses. The purpose of this report is to help guide anti-violence organizations through the complex process of considering the implementation of an electronic database to collect and store the personal information of women, children and youth experiencing domestic and sexual violence. Anti-violence organizations, which are considering a database or are currently using one, are

[2] Office of the Privacy Commissioner of Canada. (2016). The Federal Government and Your Personal Information. Retrieved from https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/the-federal-government-and-your-personal-information/

encouraged to read this report to weigh the privacy risks and benefits of databases. This report will help anti-violence organizations make informed decisions to ensure that the safety, privacy and confidentiality of women, children and youth are protected. The interception, breach and/or unauthorized access of the personal information of service recipients accessing anti-violence organizations can put the safety and lives of women, children and youth at risk.

Throughout the report, the following privacy laws are mentioned:

- Personal Information and Protection Act (PIPA) for British Columbia based organizations;
- Personal Information and Protection Act (PIPA) for Alberta based organizations;
- Privacy Act for personal information handling practices of federal government departments and organizations;
- Personal Information Protection and Electronic Documents Act (PIPEDA) for personal information-handling practices of Canadian businesses.

Anti-violence organizations need to determine which privacy legislation applies to their organization and jurisdiction.

Finally, this report should be used in conjunction with other resources including:

- Provincial and Territorial privacy laws
- Freedom of Information and Protection of Privacy Act
  BC: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
  Ontario https://www.ontario.ca/laws/statute/90f31
- Provincial and Territorial Child Protection Legislation
- Criminal Code of Canada https://laws-lois.justice.gc.ca/eng/acts/c-46/
- Privacy Act https://laws-lois.justice.gc.ca/eng/acts/p-21/
- Personal Information Protection and Electronic Documents Act
  https://laws-lois.justice.gc.ca/eng/acts/p-8.6/
- Privacy Toolkit
  www.bchousing.org/Partners/H_S_Op/Privacy_tools
- Non Profit Records Management Toolkit
  www.bchousing.org/Partners/H_S_Op/Administration/Records_management
- BCSTH "Legal Toolkit: General Information about Legal Issues and Court Matters in British Columbia" https://bcsth.ca/publications/bcsth-legal-toolkit-general-information-about-legal-issues-and-court-matters-in-british-columbia/

- BCSTH “Use of Technology Policy Template Guide for BC’s Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) organizations for children and youth experiencing violence”

WHAT IS A DATABASE?

Databases are computer programs used to organize information in a way that can make information easy to locate, access and update. Databases can be organized in a variety of ways (alphabetically, numerically) and can include text, words, and images. Databases can be searched using a “query” (name, place or date) to find information about individuals or groups of people. Most databases have a “report” function that allows the user to run reports. For example, a report on the number of new residents or organization participants in the last month can be run or a report on the most popular resource accessed.

Databases generally allow "administrators" to set up usernames, passwords, access levels and permissions for the identified staff or volunteer who needs to access the database for their work. It is best practice that one person in an organization’s office be responsible for the database, such as the Executive Director, Program manager or Information Technology (IT) staff.

Additionally, well-designed databases incorporate audit trails to provide a detailed record of the queries and actions of each user. Databases can be designed at the outset to customize fields, reports, automatically delete specified data elements after a certain time period, and only retain the elements necessary for reporting purposes.

Types of Databases

There are two types of database options available to Canadian anti-violence organizations. The first is a Personal Information Database and the second is a Case Management Database. It is important that anti-violence organizations consider their internal capacity; number of organizations and staff users; budget and technology infrastructure; and security before making a decision about which database to implement in their organizations. Considering some of these initial issues will help organizations narrow down the type of database that will meet their needs.

A. Personal Information Database

Some anti-violence organizations prefer a database to collect only the basic personal information of women, children and youth such as name and contact information. This type of database is usually one that is hosted on an organization’s server. There are personal information commercial

databases available in Canada, however many Canadian anti-violence organizations report using databases developed in software applications such as Microsoft Access or Excel.

Another option for a personal information databases is to use the database like a card catalog to reference paper files. “Here the data is entered with a non-identifying code instead of a name. Paper files are labeled with the same code and this helps staff know which filing cabinet to go to in order to find the paper file.”[3] This helps ensure privacy because names are not directly inputted into a woman’s electronic file.

If organizations opt to use a personal information database, they must assess the privacy, confidentiality and security risks of their internal IT infrastructure prior to use. For example, if their database is located on a computer or server that is connected to the Internet, personal information stored in these databases remains at risk of being compromised by unauthorized third parties. This could happen through interception or unauthorized access of personal information if the file or database is saved in a cloud based storage facility[4].

Prior to collecting and storing the personal information of women, children and youth in a database, organizations must:

- complete an IT audit;
- purchase and install all necessary computer security applications and software;
- have a plan and budget in place to update, install and annually renew privacy and security products to ensure the personal information of women, children and youth is not at risk;
- identify storage options and risks, such as cloud storage.

B. Case Management Database

Increasingly, Canadian anti-violence organizations are exploring the use of databases as a tool for case management. In addition to storing the personal information of women, children and youth, case management databases can collect and store numerous amounts of private information about a service recipient as well as provide fields for case notes, referrals, bed management and managing staff calendars. Case management databases also have the ability to export reports. Anti-violence

[3] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Retrieved from: https://nnedv.org/mdocs-posts/selecting-a-database/

[4] For more information about risks associated with cloud based storage facilities see section: Privacy Breaches and the Storage of Personal Information: Remotely Hosted Databases.

organizations may decide to customize database fields to collect funder-required statistics and output aggregate reports for monthly and quarterly reporting.

Most case management databases are web-based and require users to access the database from a web-enabled device. Server-based case management databases are available but the computer or server that it is hosted on will most likely be connected to the Internet. The benefit of having a database accessible via the Internet is access. However, this is also one of the main privacy concerns. Having the personal information of women, children and youth accessible via the Internet makes them vulnerable to interception and unauthorized access. This can directly impact their safety.

If an organization chooses to implement a database accessible through a web-enabled device, it is best practice to have:

- policies that comply with privacy legislation
- receive informed consent from service recipients
- have the ability to permanently delete personal information
- have strict confidentiality practices to mitigate the risks of breaching confidentiality and privacy.

For example, many organizations with web-based databases have policies about what devices staff can use to access the database. In many cases, databases hosted online cannot be accessed by a personal smartphone or computers/laptops not owned by the organization.

> We encourage organizations to have secure up-to-date technological infrastructure, encryption keys, use of database policies and database administration and oversight in place before implementing the use of a database.

WHAT PROBLEM DOES A DATABASE SOLVE?

Before purchasing a database for the storage of women, children and youth's personal information, it is helpful for anti-violence organizations to clearly *identify the problem* that their anti-violence organization is trying to solve. For many organizations, the appeal of a database is the apparent ease through which outcomes can be tracked, measured, used to demonstrate organization effectiveness and to identify areas for organization improvement. For other organizations, it is a way which staff activity can be statistically monitored for reporting purposes.

There are numerous database products on the market for anti-violence organizations. Identifying the problem or goal will help anti-violence organizations choose a database that is best suited to meet their needs and may save time and money in the processes. For example:

- Is the team having difficulty locating information that you need?
    - Is there an alternative way to find it?
    - Is this information that will always be useful to track, or is the need for the information temporary?
- Are you looking for an easier way to pull reports for funders?
    - Can the funders set up a more user-friendly system?
- Is your organization going through an accreditation process?
    - Is a database a requirement of the accreditation process or merely a suggestion?
- Are organizations looking for an environmentally-friendly way to store records?
    - What is the safest way to store records?
- Will a database provide your organization with the best option to enhance women's safety, confidentiality, privacy and ability to live a life free of violence?

ASSESSING NEED

Consider the following questions before deciding if your organization needs a database:

- How will a database help you to fulfill your organization's mission statement?
- Is using a database congruent with your organization's values?
- Could using a database result in staff and volunteers working more with computers and less with women, children and youth?
- Will it require staff to ask questions of women, children and youth that may influence the nature of their relationship, either negatively or positively?
- Are you able to ensure the security, privacy and confidentiality of the data collected?
- Do you have the capacity to write database-use policy and train workers about how to use the database?
- Do you have the IT support to host a database securely?
- Is the sharing of information about women, children and youth via a database a violation of your organization's contracts with funders and privacy laws?

If your organization decides that a database is needed, consider how you will:

- Uphold a woman, child and youth's right to privacy and the ethical implications of using databases?
- Address the risks databases may have on women, children and youth's safety?
- Ensure the database set up does not inadvertently continue the violence? Could your database help perpetrators commit further acts of violence, such as through interception of information or unauthorized access?
- Articulate the direct benefits of inputting personal information into databases to the women, children and youth you serve?
- Ensure the staff have time to update the database?
- Fund the cost of the initial database and the funds needed to keep the database up to date?

DATABASE BENEFITS FOR ORGANIZATIONS

Anti-violence organizations choose a database for a variety of reasons. These benefits include:

- Databases allow organizations to analyze relationships between data and run reports on service usage.5
- Resource databases eliminate the need to recreate materials or resources and generally offer keyword searches to provide quick results.6
- Databases offer organizations the benefit of standardizing their method of data collection.
- Databases provide service providers with one system that is hopefully easily accessible to all users.

DATA COLLECTION AND CANADIAN PRIVACY LAWS

BC's Personal Information Protection Act: An Example

Due to the very real possibility of a breach of personal information, collecting and storing unnecessary data on an electronic database can increase the safety risk for women, children and youth experiencing violence if privacy breaches occur. The majority of database vendors, who provide services to anti-violence organizations, offer comprehensive "ready-made" databases that can store more personal information about a service recipient than one might normally keep in a paper file. To ensure that organizations are only collecting the information necessary to provide appropriate services, anti-violence organizations must carefully *consider each data field offered* and work with database vendors to customize the database by deciding which fields to "turn off" or "delete" to be less invasive and in compliance with privacy legislation.

Anti-violence organizations must:

- ask why each field is in a database;
- contemplate if the data field is necessary to provide services;
- consider if the field asks for data that if released may put women, children and youth at risk; and

[5] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

[6] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

- examine and delete fields that may not be in accord with the organization’s practice and purpose and have implications for the organization’s liability.

For example, in one Canadian national database, a data field asks workers to input any **suspected** mental illness or health concern. Not all service providers in anti-violence organizations have the knowledge and professional background to asses for mental illness or health concerns. In addition, this data may not be relevant to the services being provided and there be no basis in fact for this “suspected” condition. Under BC’s Personal Information Privacy Act, service recipients have a right to access, and have a copy of, their file/record as well as to ask for revisions to the file/record and this would include database records. The rapport and trust between the service recipient and anti-violence worker may be broken if she were to see that her support worker suspected a mental illness or health diagnosis and did not address that in the services provided. Another potential risk is in the case of a subpoena, if a woman’s record is requested by a third party and subsequently released, the client’s “suspected” mental illness and health concerns may have dire consequences in other settings such Family Court custody determinations. The anti-violence organization and the staff may be subject to civil and privacy complaints if they are not professionally qualified to make these assessments and this supposition causes harm to a service recipient.

It is best practice that anti-violence organizations only collect and store the personal information of women, children and youth ***necessary*** to provide services for the time needed. Provincial, Territorial or federal privacy legislation governs the records management practices of all the anti-violence organizations and provides guidance as to database usage as well.

In BC, the Personal Information Protection Act (PIPA) guides the collection of personal information. Below is a table that outlines the privacy requirements for the majority of British Columbia’s non-profit anti-violence organizations. Complying with PIPA provides a framework for anti-violence organizations to consider the need for various database fields and to think through the database customization process before adding a service recipient’s personal information into a “ready-made” database. Anti-violence organizations outside of BC are encouraged to create a similar table using their own provincial, territorial privacy or federal privacy laws.

According to PIPA BC:	Database Implications to Consider
Organizations must obtain informed consent from service recipients in order to collect, use, and/or disclose personal information.[7]	Obtaining informed consent is the law. Let the service recipient know: - that their personal information will be uploaded to a database - who has access to this database (IT, developer, staff members/volunteers) - where there data is being stored - how to revoke their consent and the risks associated with this. It is best practice for the informed consent to be written and time limited.
Organizations must offer services even when someone does not consent to the collection and electronic storage of their personal data. Organizations must not, as a condition of supplying a…service, require an individual to consent to the collection of their personal information.[8]	Organizations should have policies in place for when a service recipient decides that they do not want to have their personal information collected and inputted into the database. Service should not be denied because of one's refusal to have their personal information stored in an electronic database.
If requested, organizations must provide information on how and why the data is being used and who has access to it. On request of a past or current service recipient, an organization must provide the individual with the following: - the individual's personal information under the control of the organization;	- Is the organization's database capable of printing off a resident or organization participant's information or electronic case file without jeopardizing other service recipient's information stored in the database? - Does the organization have a policy about how the organization is using personal information stored in the database?

[7] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[8] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

• information about the ways in which the personal information...has been and is being used by the organization; • the names of the individuals and organizations to whom the personal information...has been disclosed by the organization.[9]	• Ensure that if the database developer and their staff and the companies that have been outsourced to host the organization's data (e.g. cloud storage) have access to the database, that they are included in the consent form which outlines who has access to the electronic information
Organizations must secure personal information. Organizations must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.[10]	It is best practice to **only** collect and store information necessary to provide the service a woman, child or youth is requesting for the time necessary. If the organization's database is connected to the Internet, here are some questions to consider: • Are the database files encrypted with zero-knowledge encryption? • How strong is the encryption key you are using? • What happens if the encryption can be "decrypted" by third parties? • Does your organization have firewalls and anti-virus software? • Does your organization have the budget to maintain anti-virus and security software? • What policies do you have in place if third parties do access your files, or your organization server is physically removed? • What access levels will staff have? • What security plans do you have in place for backups or disposal of old hard drives?

[9] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[10] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Organizations must destroy personal information in a timely fashion. Organizations must destroy documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that: • the purpose for which that personal information was collected is no longer being served by retention of the personal information, and • retention is no longer necessary for legal or business purposes.[11]	A computer's data can often be recovered. It is recommended that organizations have: • a map of all the places service recipient's data is stored. Consider computers, laptops, tablets, smartphones, phones, photocopiers, scanners, cloud storage centres, email, text messages and social media • have a plan to permanently destroy personal information of service recipients on all devices • Have a plan in place for when to delete a file after it has been closed and the retention period for records is over. • Discuss with the developer: ○ If deleting a file permanently is possible, if your organization is still utilizing the database. ○ How the database vendor will guarantee that women's information is permanently deleted from all places of storage?

Other considerations:

- Data and privacy laws vary from province, territory, and country. Know what privacy laws apply to your participant's files if they are stored in a jurisdiction other than your own, for example on a cloud server. If your data is being stored offsite, ask the database vendor who owns the records and what privacy laws apply.
- Have a plan in place in the event your database receives a court order or subpoena for the entire database and a plan to respond to a court order or subpoena for an individual file/record.

[11] Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

- How will you contest this court order/subpoena to protect all service recipients' personal information along with the organization's operational information?
- How will you notify all service recipients whose information is stored in the database as per privacy legislation?
- How will you ensure the safety of women, children and youth if their names, addresses, and other personal information placed into a database by your organization's personnel is breached by an unauthorized user or security lapse?

PRIVACY BREACHES AND THE STORAGE OF PERSONAL INFORMATION

According to the Office of the Privacy Commissioner of Canada, a privacy breach is the loss of, unauthorized access to, or disclosure of, personal information. This can happen in a variety of ways including being stolen, lost, or being mistakenly shared.[12] Privacy breaches are a consequence of faulty procedures or operational breakdowns.

Data security, confidentiality, and privacy breach policies and training will help anti-violence workers understand why only the data of service recipients necessary to provide service is collected and stored. Be transparent and knowledgeable about the potential liabilities to a worker and the organization if too much data is collected. The acknowledgment of the risks of the electronic storage of information to women's safety can unify an organization's framework of data collection and use of databases. Prior to implementing the use of a database, organizations must think about the possibility of an organization privacy breach, which can be life threatening for women, children and youth who are fleeing or living with the impacts of violence. Privacy breaches can also be financially costly to an organization as there are legal consequences such as privacy complaints and requirements that an organization must follow in response to a privacy breach.

With this in mind, organizations should consider how and where a database stores personal information before integrating one into your work. The way a database stores the personal information of women, children and youth is key in distinguishing the *type* of database an organization needs. Databases can either store information on an organizations server or on the Internet via a cloud storage facility.

Data Storage

The following are data storage considerations for a) Remotely Hosted Database and b) Locally Hosted Database.

[12] Office of the Privacy Commissioner of Canada. (2018). Privacy Breaches. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/

A. **Remotely Hosted Database**

The majority of databases most relevant for anti-violence organizations are remotely hosted databases. The main benefit of remotely hosted databases is that they can be accessed from almost any web-enabled device that has an Internet connection. Storing the private information of women, children and youth on the Internet via a cloud storage facility has a variety of security risks to women's information that need to be considered. These include:

- The risk of unauthorized third parties (some of whom may be hackers or advertisers) potentially accessing information through the Internet about the individuals your organization serves.
- If an organization is considering a remotely hosted database, a zero-knowledge encrypted database offers the most security. However, someone could still get unauthorized access to your files if they obtain an organization staff's user ID, password and encryption key. Please see page 24 for more information about encryption.
- If staff have access to the database outside of their workplace, it is important to consider the possibility that:
  - their user ID and passwords are being stored on public and personal web-enabled devices, such as laptops, computers, tablets and phones,
  - information may be compromised by other people accessing the computer or
  - by a third party watching a staff member enter their user ID and password.
- The possibility that laptops, phones and tablets get misplaced or stolen. Are the user IDs and passwords stored or saved on these devices?
- Some database companies have access to an organization's database in order to solve any technical issues or make updates as required. While this may appear to be a benefit of your database license, the confidentiality of service recipients can be compromised if the database company can access your database any time without restrictions. Ideally, database company employees should be barred from viewing any of your organization's confidential client-level information. If employees of the database are transferring your organization's records from your old system to your new database, have data breach plans in place and notify service recipients before doing so.

B. **Locally Hosted Database**

Locally hosted databases store personal information on an organization's server and do not require Internet access to be used. While a locally hosted database is one of the more secure database options, they can also have implications to women, children and youth's privacy as it is very difficult to provide security for data. Knowing the options and the risks of electronic databases to women, children and youth's safety and privacy is part of setting up reasonable security arrangements. Considerations for a locally hosted database include:

- If your organization's server is connected to the Internet, the personal information stored in the electronic database can still be accessible by hacking into your network or computer through an Internet connection.
- Who has access to the space where your organization's server is stored? Do volunteers, staff, external janitorial staff, utility companies, residents and organization participants or other service providers have access to the space where the server is stored? Can someone walk into your space and pick up your server and walk out with it?
- Does your organization have funds to maintain it in addition to having the funds for the database license renewal each year? Typically, databases that are stored on an organization's server will require a knowledgeable IT person to ensure the database is updated, patched and security precautions are up to date. Can an external IT consultant access the data of service recipients?
- If your IT infrastructure is up to date and consistently checked to ensure that all of the security updates are working, such as firewalls and anti-virus organizations?
- If the database is stored on your own server, consider how the database vendor has access to your database for maintenance purposes.

A Note about Biometrics Storage

Biometric identification or authentication is technology that uses aspects of the body (e.g. iris scans, finger prints or face recognition) to allow access to a digital space. Biometric authentication is often a privacy-invasive technology because the data collected is of the body. Compared to phone numbers and addresses, which can be changed; biometric data is irreversible because it is collecting information about the body. A breach of databases where biometric information is stored creates new, significant and irreversible privacy and safety risks for the women, children and youth accessing services and for staff.

Some organizations consider using biometric identification and authentication methods. These tend to be marketed as ways to ensure building security. Some databases have the option to store biometric data. No matter which product requires biometric data (a security system, smartphone or database) the personal and unique data of a person is stored "somewhere" and the privacy and safety of that information must be considered.

If the products and databases your organization is using has the capacity to store biometric data, consider the following questions:

- Is it zero-knowledge encrypted?[13]
- How can a perpetrator intercept data in a biometric database and steal personal information and/or identity?
- What happens when biometric data is deleted?
- What happens if the technology recognizes biometric data incorrectly and it allows or denies access to the wrong person?

[13] Zero-Knowledge encryption means that service providers know nothing about the data you store on their servers. Ref: Lam, Istvan. (2016). What is Zero-Knowledge Encryption? Retrieved from: https://tresorit.com/blog/zero-knowledge-encryption/

SECURITY BY DESIGN

Prior to utilizing a database, it is recommended that organizations take the time to audit their current IT systems and infrastructure. Consider hiring a trusted and skilled IT consultant or IT security company to test the security of your organization's network and data protection procedures. An external security audit can provide an in-depth analysis of what is weak or missing. Organizations may find that security software needs to be updated or implemented to ensure that women, children and youth's personal information has as much protection as possible. The following is a list of suggestions based on the National Network to End Domestic Violence's "Data Security Checklist to Increase Victim Safety & Privacy."[14]

Minimize Data Collected

Many databases come as a pre-packaged product with the ability to store an exorbitant amount of data for each service recipient. Working with your anti-violence organization staff and the database vendor to customize the data fields of the database is a great way to enhance women's confidentiality and privacy. The majority of databases have the ability to turn off, deselect and erase fields that are not necessary to carry out an organization's mandate. Minimizing what is collected to lessen the safety risks to women will also decrease your organization's liability and chances of data breach.

Review the goals of your organization and/or project and evaluate your data collection process. Consider:

- Are there less invasive alternatives to measure outcomes and streamline intake?
- How could the data you plan to collect be misused if accessed through legitimate or illegitimate means?

Develop, Train and Implement Database Policies

Before implementing a database, organizations must develop clear policies and procedures that outline privacy practices for collecting, storing and purging sensitive data. It is best practice for organizations to

[14] National Network to End Domestic Violence, Safety Net Project. (2008). Data Security Checklist to Increase Victim Safety & Privacy. Retrieved from: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5c016277575d1ff2db2060d3/1543594616517/NNEDV_DataSecurity_English08_access.pdf

provide training on these policies to all personnel and communicate these policies regularly at staff orientations and meetings.

Database policies should address:[15]

- The content of the record, how long it will exist and who may have access to it.
- What type of data is to be entered into any database.
- Why your organization collects the records that it does. Demonstrate a clear need or rationale.
- Processes for women to opt-out, inspect, withdraw or correct their data/records.
- Collection, modification, use and disclosure procedures for data.
- How someone can request to see or request edits to a record about them.
- The process for purging data if it is to be permanently deleted.
- How personal information that is retained is stored securely for the time period required under privacy laws.
- Screening, training and background check processes of individuals, who have access to sensitive information.
- On which devices the database can be accessed.
- Access levels: who can access what data, and how access is changed or revoked.
- Procedures to protect against unauthorized use and unauthorized access.
- Procedures if there is a privacy complaint made against your organization.

For sample policies see BCSTH's "Use of Technology Policy Template Guide for BC's Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) Programs for children and youth experiencing violence."

Utilize Anti-Virus Organizations and Firewalls

If you have an office network, use anti-virus or firewall programs. Anti-virus software or hardware firewalls are important security steps for any organization with Internet access. However, anti-virus organizations and firewalls are not secure enough on their own to adequately protect women, children and youth's data. Regularly scheduled updates and renewals should be planned and, upon consultation with an IT specialist, other precautions may need to be put in place.

[15] National Network to End Domestic Violence, Safety Net Project. (2011). FAQs of Record Retention and Deletion. Retrieved from: https://www.techsafety.org/retention

User ID and Passwords for Everyone

It is best practice for each employee, volunteer, student intern, work placement personnel and board member accessing an organization's computer network to have their own user ID and passwords. This will help organizations control who has access to an organization's network and database. Password management is a critical part of data security. The use of pet names, birthdays or words found in the dictionary should be prohibited. Passwords should be changed frequently and kept safe; and not kept under the keyboard or taped to the monitor. A password-activated screen-saver for employees with access to personal information helps increase data security when they step away from their computers.

Use Encryption

Encryption is the conversion of data into a form that cannot be easily understood by unauthorized users. Encryption is not the solution to all security concerns; it is a small piece of a comprehensive security solution. Databases that use zero-knowledge encryption are the most secure option to encrypt people's information. Ensure from the vendor that all data inputted into and stored on the database and backup systems are zero-knowledge encrypted. If it is not zero-knowledge encrypted ask more about their encryption method and who is able to un-encrypt your organizations records. Organizations must have a plan in place if data becomes "unencrypted" by the vendor or a third party.

Access levels

Access levels within a database enables an administrator to set up who can access database information and set the level of access to personal information for each user. Individualize *Levels of Access* for each employee, volunteer, student intern, work placement personnel and board member who has access to the database. Do administrators, staff, volunteers and management need access to all files if they are not working with women, children and youth directly? Many do not and therefore access levels for each person can enhance the privacy of service recipients.

For example, the system administrator could establish access levels so that a few staff see all the information in a database, and other users only see the information relevant to the role of the user. Limiting the number of users who are authorized to view personal identifiable and sensitive information can help organizations reduce confidentiality breaches. When determining access levels for each user, consider the safety risks if the data is shared internally within one organization or across many. It is critical to review the privacy laws that stipulate who can access the data of women and children accessing your organizations.

It is recommended that organizations determine:

- Who needs to access the data?
- What level of access is appropriate for each user?
- How access to the data will be limited to these authorized persons?
- Who can input information into each file (how to track who inputted information)?
- Who can delete information from files?
- How records will be deleted?

Update the Operating System
It is recommended that organizations have policies in place in regards to regularly updating the operating system and assign someone to regularly download all the latest patches and updates for your operating systems. This is extremely important for locally hosted databases as updates and patches will have to be installed by a staff member, IT consultant or database vendor.

Back Up Data
Most databases have backup systems in place. It is best practice to secure backups at the same level of security as the original source.
It is recommended that organizations:

- Have plans for system backup and security
- Ensure backup data is encrypted.
- Consider contracting with a computer security professional to assess the penetrability/security of the system, and to recommend improvements.

Audit for Quality Assurance
Doing an audit of a database is a process of evaluating the information that has been collected and removing any incorrect information. At a minimum, staff responsible for the day-to-day entry of information should not be in charge of the audit. Audits should include random samples of information collected about service recipients to help assess quality, accuracy, and to identify if inappropriate data is being collected or shared.

Use Skilled Technology Professionals
Most anti-violence organizations are underfunded and do not have the resources to support a full-time Information Technology (IT) staff. It is imperative that organizations collecting personal information and

often-sensitive electronic data have qualified professional technical support. To limit cost, organizations can:

- ask other organizations about their databases and their overall design.
- ask other organizations about the possibility of contracting them to use a copy of the database they have customized.
- ask your provincial or territorial women's shelter or transition house association for assistance as a starting point.

Seek Ongoing Education

Creating opportunities for staff to attend issue specific trainings or bringing a consultant to your organization to speak about privacy legislation, data security and women's safety can help maintain security of the database. With high turnover of staff in some anti-violence organizations, it is especially important to offer regular training & education to maintain the security of personal information for the privacy and safety of the women, children and youth working with the organization.

DESTRUCTION OF RECORDS

In Canadian provinces and territories there are privacy laws that dictate how long an organization must retain the personal information of women, children and youth. This is true for information stored in a database because the collected data about the service recipients is considered their personal record. Anti-violence organizations must comply with provincial and territorial retention and destruction provisions in the specific jurisdiction's privacy laws.

Most databases have the ability to store data until an organization decides to stop using the database. Even then, some cloud-based databases have the ability to keep an organization's data even if an organization ceases to use the database. Organizations can reduce the risk of liability and potential breaches of data collection by working with a database vendor to customize or design a database and a process that follows the retention and destruction laws of the province or territory under the applicable privacy laws.

Organizations must ensure the following in the databases:

- The ability for records to be permanently deleted after the required time.
- The ability for records to be permanently deleted from the server and all cloud-based storage.
- The ability for all backups of records to be permanently deleted.
- The inability of the database or database vendor to automatically retrieve a service recipient's past record once it has been permanently deleted.

MAINTAINING CONFIDENTIALITY

An organization's use of database policies and practices should allow for women to be able to opt out of having their personal information stored in an electronic database. In some provinces and territories, privacy laws specifically state that organizations must receive informed consent from a service recipient before personal information is collected and stored. If your organization is using a database, staff must obtain ***written, informed and time limited consent*** from women acknowledging that they have been informed of, and consent to:

- their personal information being stored in an electronic database
- who has access to the their data
- the security and confidentiality risks associated with this method of data collection and storage.

Some additional recommendations for additional information that should be included in the informed consent form and discussed with a service recipient include:

- How many people and who has access to the electronic database;
- What information is mandatory and what is optional when entered into the electronic database;
- How many places is her personal information being stored in;
- What provinces, territories, countries are her personal information being stored in;
- What are the risks of storing her personal information in a database;
- What is the organization obligated to do if there is a data breach;
- How and when will the organization permanently delete /destroy her personal information;
- What are the policies regarding third party requests , court orders and subpoenas;
- What is the organization willing to do on the woman's behalf if there is a data breach?

Because the storing of information on electronic databases involves many steps and can be stored on many different servers in different parts of the world, it can be hard to guarantee that a service recipient's record will not be breached or compromised at some point.

When considering the liability of databases for organizations and the potential safety risks to women and her children, it is critical to think through the confidentiality implications that databases have on the safety and privacy of women, children and youth. **It is important that organizations collect only the information necessary to provide services for the necessary time period.** Database representatives typically showcase how much information their database can store in one place such as storing photos, Facebook account information, names, and addresses of the abuser and immigration and ethnic status. Collecting personal information that is not necessary for the services provided can pose risks to women's confidentiality, privacy and safety. Prior to launching your database, work with the database developer to ensure that only necessary fields are included in your database. Some funders of anti-violence organizations in Canada do not require women to give their actual personal information to access services -- for instance, they serve "Jane Does". Other Canadian funders do not require that the service recipient's information is stored in a record of any kind in order to access services. Anti-violence organizations should determine what records collection system is best suited to the purpose and mandate of their work and the women, children and youth they support.

Confidentiality considerations when selecting and designing a database and when developing organizational database-use policies:

- What happens if Citizenship and Immigration Canada serves a court order on the organization for your organization's data and finds that you are serving individuals without immigrant, refugee or Canadian citizenship status in your organization?

- Some ready-made databases ask organizations to collect information that is not necessary for the services provided for the time period required. The database collection of irrelevant information that is not based in fact does not support the purpose of the anti-violence organization's work, which is based on providing confidential appropriate support services.

- The collection of biometrics may not allow the flexibility to protect a woman's confidentiality. For example, if your organization has a security system that requires a resident to provide her fingerprints in order to access transition housing or shelter, there will be a record that she accessed services at your organization on a specific date.

- Does an organization's decision to use and store biometric data or photos as a security mechanism outweigh the possibility of putting women and their children at risk of "unintended consequences"? *See Biometrics, page 20.*

- What are the risks for women's safety if a woman's ex-partner, or an associate of her ex-partner, works for the database company that is hosting her data?

- What are the risks for women's safety if a woman's ex-partner, or an associate of her ex-partner, works for an organization that has access to your organization's data such as a regional networked homeless shelter database?

- Consider the significant privacy implications of collecting too much data, such as social media accounts, pictures of service recipients and their children, Social Insurance Numbers, and immigration status.

- How vulnerable is your database to theft, hacking or abuse? Is the database located on a computer connected to the Internet?

- If a service recipient's file is subpoenaed, do you have a way of isolating the necessary information to share? How will you ensure that all other records on the database are not compromised?

- What are the implications of having an electronic trail of your organization that may never be completely deleted?

For sample forms please see BCSTH "Legal Toolkit: General Information about Legal Issues and Court Matters in British Columbia" https://bcsth.ca/publications/bcsth-legal-toolkit-general-information-about-legal-issues-and-court-matters-in-british-columbia/

QUESTIONS TO ASK DATABASE VENDORS

When communicating with database vendors about their product, it is important that, at a minimum, anti-violence organizations ask the following privacy questions to vendors about their databases.

- Does the database have the capacity to delete or modify data fields?
- Who outside the vendor organization has access to the stored data?
- What security measures are in place to protect your organization's data and services? For example:
  - Is the data encrypted, and if so, what kind of encryption is used and who has the encryption key?
  - Is the database zero-knowledge encrypted, meaning no one but the user can see the data you store?

    Note: at the time of writing and from the databases reviewed in the research, zero knowledge appears to be the most secure form of storing personal information.
- Is the data stored in Canada?
- Is the data stored in one storage facility?
- It is best practice to ensure that database vendor employees DO NOT have access to an organization's database? Often, database vendors will confirm that vendor employees do have access, but that they have signed a confidentiality waiver. It is important to ask the vendor questions about what happens if a vendor employee breaches that confidentiality agreement.
- If a vendor hosts an organization's data, can a vendor deny an organization access to their data if their business closes down or they experience technical problems?
- Have organizations clarified in a written contract who owns your organization's data and who has access to it, once it is stored on the vendor's server or in a cloud database system.
- Does the vendor have policies about what happens if they get subpoenaed or provided with a court order for your records?
  - Will they let your organization know if they get a subpoena or a court order for records?
  - Is there a timeframe they will contact you by?
  - What is their policy?

Under Canadian privacy laws, anti-violence organizations are responsible for the records management of personal information uploaded into a database and for the developer's actions with the personal information once stored in the database. Review the vendor's database contract with a lawyer and revise to ensure that the written contract with the vendor reflects the privacy laws of your jurisdiction and includes protections regarding maintaining the privacy and confidentiality of the personal information of women, children and youth the anti- violence organization serves.

The US based National Network to End Domestic Violence has produced a resource titled “Selecting a Database” which provides additional guidance to anti-violence organizations as to the implementation of women-centred database systems. For more information: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/59e13157b1ffb6025f1804d1/1507930456484/NNEDV_SelectingDatabase_Chart_2011.pdf

FINAL THOUGHTS

Implementing an electronic database for the collection and storage of the personal information of women and their children accessing anti-violence organizations is complex. Risks of data breaches are a constant possibility when storing personal information electronically. A privacy breach of personally identifiable data at an anti-violence organization can put the lives of women, children and youth at risk. In order to address these concerns and realities, anti-violence organizations should collect the minimal amount of information necessary to provide the service that women, children and youth consent to for the time required. The collection and storage of the service recipient's personal information must do no harm. Women, children and youth trust anti-violence organizations with their personal information as part of the confidential critical support services that are being provided. Women have a right to be fully informed of the potential security and privacy risks of storing their personal information electronically. Obtaining written, informed, time-limited consent to collect and store personal information in a paper or electronic database system is a recommended practice and the law in most Canadian provinces and territories.

Privacy, safety and security concerns for the women, children and youth supported by anti-violence organizations must be addressed by database developers before an organization executes a contract that implements a database. If an anti-violence organization determines a need for a database, the organization should consider all the available vendors to determine which best meets the needs of the organization and is consistent with the purpose and mandate of the anti-violence organization. Customizing a database is part of these negotiations and a contract should only be signed if the organization's concerns regarding privacy, confidentiality and security have been met. The majority of database vendors agree that integrating a database cannot happen overnight. Giving your organization and database developers' time to develop a clear implementation plan and customize the database to ensure compliance with privacy legislation can be key to ensuring that the persona information of women, children and youth is safeguarded given the current day privacy breach risks of the electronic storage of personal information.

Anti-violence organizations also have to incorporate and plan for the hidden costs of an electronic database. Even if the database is free, there can be prohibitive costs associated with IT infrastructure, research, human resources, policy development, training and annual fees. All of these costs should be assessed when the anti-violence organization is determining if a database is needed and consistent with the organization's purpose and mandate.

Having adequate funds, access to resources and time to create and follow a database implementation plan will make the difference in maintaining the privacy of women, children and youth accessing anti-violence organizations. The resources listed below will provide organizations additional information to make informed choices about implementing electronic databases for their organization.

RESOURCES

Privacy Legislation
BC's Personal Information and Privacy Act:
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01
Alberta's Personal Information and Privacy Act:
http://www.qp.alberta.ca/documents/Acts/P06P5.pdf
Canada's Privacy Act:
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/
Canada's Personal Information Protection and Electronic Documents Act:
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Cloud Computing
PIPEDA: Cloud Computing for Small and Medium- sized Enterprises:
https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/
PIPA and PIPEDA:
Guidelines for Cloud Computing:
https://www.oipc.bc.ca/guidance-documents/1437

PIPEDA Compliance
PIPEDA compliance and training tools:
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/
Accessing your personal information:
https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/accessing-your-personal-information/

Privacy Breaches
PIPEDA:
What you need to know about mandatory reporting of breaches of security safeguards:
https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

PIPA:
Privacy Breaches: Tools and Resources:
https://www.oipc.bc.ca/guidance-documents/1428

Information Technology Security
Securing Personal Information: A Self-Assessment Tool for Organizations:
https://www.oipc.bc.ca/guidance-documents/1439

Database Information for anti-violence organizations
Selecting a Database:
https://nnedv.org/mdocs-posts/selecting-a-database/ or https://www.techsafety.org/selecting-a-database/

REFERENCES

Lam, Istvan. (2016). What is Zero-Knowledge Encryption? Retrieved from: https://tresorit.com/blog/zero-knowledge-encryption/

National Network to End Domestic Violence, Safety Net Project. (2008). Data Security Checklist to Increase Victim Safety & Privacy. Retrieved from: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5c016277575d1ff2db2060d3/1543594616517/NNEDV_Data

National Network to End Domestic Violence, Safety Net Project. (2011). FAQs of Record Retention and Deletion. Retrieved from: https://www.techsafety.org/retention

National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Retrieved from: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

Office of the Privacy Commissioner of Canada. (2018). Privacy Breaches. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/

Office of the Privacy Commissioner of Canada. (2016). The Federal Government and Your Personal Information. Retrieved from https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/the-federal-government-and-your-personal-information/

Province of British Columbia. (2013). Personal Information Protection Act. Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01