BC Society of Transition Houses

Understanding Database Options for Canadian Anti-Violence Organizations

ACKNOWLEDGEMENTS

Research, Writing, Editing: *Rhiannon Wong*

Nicky Bowman

Louise Godard

Amy S. FitzGerald

Graphic Design: *Hannah Lee*

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

1. BACKGROUND

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, the BC Society of Transition Houses (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 is 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. 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.

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

[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).

[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/

put their safety at risk through online interception, 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.

Due to the complex and sensitive nature of personal data collection, BCSTH regularly receives inquiries about electronic databases from Canadian anti-violence organizations and funders out of concern for maintaining women's privacy. In 2018, 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.

To research the capabilities, benefits and risks of databases available to Canadian anti-violence organizations, BCSTH distributed two surveys[3]:

- "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 report, "Understanding Database Options for Canadian Anti-Violence Organizations," is one of three reports developed from: the 2018 Database Vendor Questionnaire 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. All of the database developers who completed the "Database Vendor Questionnaire for BC Society of Transition Houses" were invited to provide BCSTH with a demonstration of their product. The purpose of this

[3] Survey tools used have been adapted from and in cooperation with the Safety Net Technology Project at the National Network to End Domestic Violence, United States.

report is to summarize and discuss findings from the "Database Vendor Questionnaire for the BC Society of Transition Houses."

Anti-violence organizations, who are considering a database or are currently using one, are encouraged to read this report to weigh the privacy risks and benefits of databases. Database developers wishing for their product to be used in Canada are encouraged to read this report to understand the complex needs of Canadian anti-violence organizations. 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.

In the last sections of this report: Discussion, Recommendations and Resources, we provide practical suggestions for anti-violence organizations, funders and database vendors regarding the collection and storage of personal information in electronic databases. We encourage anti-violence programs to use the recommendations in this report in conjunction with our "Privacy, Security and Confidentiality: Database Considerations for Anti-Violence Programs" resource and "Electronic Database and Case Management System Use by Anti-Violence Organizations across Canada" report found on the www.bcsth.ca website. We hope that our research will provide credible, evidence-based considerations for anti-violence programs and the women, children and youth they support, so that both can make informed choices about the collection and electronic storage of personal information.

DATABASE VENDOR QUESTIONNAIRE SUMMARY REPORT

1. Product and Vendor Information

Nine database vendors responded to the questionnaire. The information provided regarding product and vendor names and locations is displayed in Table 1[4].

Table 1: Database products and database vendors

Name of Product	Name of Vendor	Location of Product	Location of Vendor
Outcome Tracker	VistaShare	Not given	Not given
iTracWSIS FCI	Accelerated Solutions Inc.	Canada	Canada
Women In Safe Housing (W.I.S.H.)	Grasp Software Corporation	Canada	Canada
PIMSY EHR	SMIS, Inc.	US and Canada	US
Osnium: Agency	Osnium Software Inc.	Canada	Canada
Collaborate	Network Ninja	US	US
EmpowerDB		Staff in US and Canada. Hosted in US.	Not given.
CAP60	CAPLUCK, INC.	US	US
Penelope	Athena Software	Canada	Canada

All respondents reported that their product is available in all Canadian provinces and territories.

2. General Features

Respondents were asked to provide information about their product's general features, such as user friendliness and customizability.

All respondents reported that their system is user friendly, describing features such as being purpose built for the sector and 'non-tech savvy or tech-enthusiastic individuals'; being customizable for

[4] Throughout our research, BCSTH reached out to the Government of Canada team developing and disseminating the Homeless Individuals and Families Information System (HIFIS) database. We were unsuccessful in our attempts to connect with them. For anti-violence agencies considering HIFIS, it is important to be aware of some potential privacy and security risks for women, children and youth experiencing violence.

organizations and individuals; offering support and training; and having features such as pop-up messages, wizards, and calendar control.

Eight of the nine respondents reported that the interface is customizable. The customizable features described included the ability to change the interface, create and remove fields, add field labels, change the font size, themes and colours, and having configurable security settings and forms/reports/activities.

The length of time it takes an average user to complete a new client profile ranged from 15 seconds to under five minutes, depending on the amount of information being entered.

All but one respondent said the number of individuals (Log-In User IDs) that can use the system at the same time is unlimited, of whom three added that this is in accordance with the number of licences purchased. The remaining respondent said this is determined by the number of licences purchased.

Seven out of nine respondents said that the database is a cloud-based system.

3. Customization

Table 2 displays an overview of the customizable features available across all nine database products.

Table 2: Customizable features

	Yes	No
Can the organization edit items in the drop-down lists?	9	0
Can the organization set which fields are required?	9	0
Can the organization add fields?	8	1
Can the organization completely hide fields?	8	1
Can the organization remove fields?	8	1
Can the organization change the text of fields?	7	2
Can the organization change the labels of fields?	8	1
Are there other customization features available to the organization?	9	0

Four respondents, who mostly answered yes to these questions, added that there are some limitations and one respondent, who mostly answered no, commented that forms and reports can be customized to do most of these things.

Other customizable features noted were the ability to customize intake forms and other forms and reports; the ability to customize other documents, system settings, pick lists, assessments, measures

and questionnaires; the ability to create roles, relationships, forms, tabs, activities, queries, surveys, portals, and messages; tailoring workflows to meet program requirements; and adding programs and services, appointment types, demographics and other fields.

4. Privacy and Safety

All respondents said that third parties are not able to retrieve or view organizations' data, of whom four added that exceptions to this would be if the organization has granted permission, requested custom functionality or if it was required by law. One also commented that the database vendor's support staff typically have access to an organization's data.

4.1 Notification of requests for data or records

All but one respondent reported that the vendor notifies the organization of subpoenas, warrants, law enforcement requests or any civil or administrative requests for data or records, of whom one added *'unless required by law not to'*. They also said that the vendor gives the organization an opportunity to resist disclosure before responding to such requests. The remaining respondent answered that this is not applicable because they do not host or have access to the organization's data – organizations house and store their own data. A further two respondents added that this scenario would be unlikely because they do not have/see or own and manage the data. One commented that the data belongs to the organization and that the ownership and release of the records is the responsibility of the organization, therefore subpoenas for records should be directed to the organization, not the vendor.

When asked <u>when</u> notice is given, respondents answered as soon as is feasible/possible, immediately, as soon as is legally allowed, or within 72 hours. One left a further comment explaining that there are some situations in which the US government forbids the vendor from notifying anyone else about their request for information. Therefore, they have a 'zero knowledge encryption setup', which prevents data from being readable to any outside party without the organization's unique encryption key.

When asked <u>how</u> notice is given, responses included by phone call and/or email or in writing. Some specified that this would be directed to the main contact or the organization's security contact. One respondent added that in the case of an investigation of the organization itself,

the vendor must comply with a valid court order and would notify the organization in writing unless legally bound to do otherwise.

4.2 Disclosure of data to third parties

Respondents were asked if the vendor retains discretion to disclose organizations' data or records to third parties' requests. Responses were mixed. Five said that it does not; one said this does not apply because they do not host/have access to the data; one did not answer; and two said that it does. Those who answered yes were asked in what circumstances they might do this. One stated *'only when the customer licences a module that exchanges data with a third party system',* adding that these types of modules are not typically licenced by domestic violence organizations. The other gave the example a government entity request and explained that any data they would provide would not be readable to an outside party because they would not have the organization's unique encryption key. They also stated that they would fight any request to the fullest of their abilities and work with the organization to determine the best course of action for resisting the disclosure.

4.3 Professional and legal confidentiality obligations

All but one respondent reported that the vendor agrees to be bound by the same duty of professional and legal confidentiality obligations as the organization they are providing the product to. One did not answer, and one added *'to the extent that legislation is applicable to [the vendor]. For example, [vendor] is PIPEDA-compliant'.*

When asked to describe <u>how</u> this is formalised in the contract for services, responses included that this is outlined in the Terms of Service; by signing the organization's non-disclosure/confidentiality agreement; or altering the vendor's contract to fit the organization. One respondent explained that they fall under the guidelines of HIPAA and other US Federal Regulations and that their contracts reflect these privacy regulations, state the ownership of the records falls on the organization, and that the vendor's staff and business associates will abide by all applicable confidentiality laws. Three respondents added further comments explaining that the Terms of Service may not specifically name confidentially obligations that the organization is bound to; that without first knowing the obligations of a client they cannot agree to be bound by them; and that having a zero knowledge encryption setup mitigates any

risk of protocols being broken or mistakes being made that expose data.

4.4 Written policies for responding to requests for data or records

Two of the nine respondents had written policies about the vendor and company's response to domestic and foreign subpoenas, warrants, law enforcement requests or any civil or administrative requests for organizations' data or records. One made these publicly available on their website, and the other stated that they do not share copies with the organization. One respondent did not answer this question and one said this was not applicable as they do not host or have access to the organization's data. The remaining five respondents did not have these written policies.

4.5 Data encryption

Four respondents reported that organization's data is available to the vendor in an unencrypted format, and four said it is not. One added that this is only for fields specified as non-encrypted, and another stated that this is necessary for them to be able to support each organization properly. Five respondents said the data is available in an encrypted format, and three said it is not, of whom one added that an exception to this would be if it was provided for a specific purpose such as data conversion. The remaining respondent said this was not applicable because they do not host or have access to the organization's data.

When asked who is responsible for encryption key management, four respondents said this is the vendor's responsibility, two said this it the organization's responsibility, and one said both the vendor and the organization are responsible. The remaining two respondents did not answer this question.

5. Technical Support

All respondents said that technical support is available for the organization.

5.1 Description of technical support offered

Descriptions of the support available varied. Where **hours of operation** were provided, these ranged from business hours (9), weekends (5), evenings (5) and 24/7 (3). Almost all respondents added that support outside of business hours was for urgent matters only/had to be arranged in advance/was offered on a contractual basis or was available for a fee.

Some respondents provided information about the **amount of support** available, which included options ranging from a package of support for an annual fee or an hourly format (1), unlimited support and maintenance for a monthly fee (1), and live technical support and training at no cost (1).

In terms of **accessing support**, options included via phone (4), email (3), webinars (2), ticketing (2), live chat (1), and submitting questions via a Help Desk portal (1). One respondent said they have a support system built into the database, and one said support for the use and configuration of the software is often done with staff and/or the organization's IT support team to handle installation of the software.

The **type of support** available included standard and premium support packages (1), emergency support (4), webinars and webinar trainings (2), training videos and user guides (1), access to a support community (1) and an online bug reporting system (1).

Finally, a couple of respondents also provided information regarding **response times**, with one stating that they attempt to answer calls and emails in real-time, but if they cannot they will be responded to within an average of thee business hours. Another explained that guidance and assurance regarding response times is provided in their Service Level Agreement and varies according to issue type and severity.

5.2 Description of training offered

All respondents reported that the vendor provides training for organization staff before using the product.

Most commonly, respondents stated that online training is included in the initial purchase (4), with details of training hours ranging from a 4-hour webinar to an extensive 24-hour 'Train the Trainer' model offered over six weeks. Two respondents added that trainings can be recorded for future reference. Most respondents also added that in-person training can be provided for

a fee (4), with one stating that most companies find the live web trainings sufficient, and another choosing which method to offer based on the size of the group (with in-person trainings being carried out with larger groups).

Training costs varied according to the format chosen, factoring in seasonal, travel and accommodation costs for in-person training. One respondent stated that the typical total cost for in-person training is around $2,500 for a 1-day session.

Descriptions of training formats were often tailored to the organization, for example a project manager leading trainees through the implementation process and including configuration based on their data collection needs, training, and data conversion; offering different types of training, for example system administrator training, end user training, etc.; trainings that cover both custom and standard functionality; and creating role specific lesson plans for all trainees.

One respondent added that some organizations choose to handle their own trainings.

6. Data Retention

Table 3 summarizes the responses to questions about data retention.

Table 3: Data Retention Summary Table

	Yes	No	Not answered
Can data be permanently deleted by the organization?	8	1	0
Can data be purged from all locations where backed-up?	6	3	0
Can some types of data be purged before others?	6	2	1
Is it possible to schedule routine removal of data?	8	1	0

All but one respondent reported that data can be permanently deleted by the organization. One answered no, explaining that this is because any data that has existed since the vendor's last weekly backups were taken will have made it into the vendor's alternate server where they keep backup data, and that data cannot be deleted by the organization. However, they added that the organization can make a request to them to delete all backups if there is an extreme need for this.

Six respondents stated that data can be purged from all locations where backed up. Of these respondents, one specified that this could only be done by the vendor via written request. Another

added that since backups are snapshots of the database as it existed at a certain point in time, removing *specific* data is not possible. However, older backups are routinely deleted when no longer needed, and all backups can be deleted at once if a client terminates their agreement with the vendor. The remaining three respondents said data could not be purged from all locations where backed up. One stated that it is not feasible to delete data from backups but added that all backups are encrypted. Another added that this is only done if custom functionality exists and the third stated that off-site backups are retained for 30 days by default, but a request can be made to expire off-site backups before the 30-days.

Six respondents said that some types of data can be purged before others. Four added that the order in which data is purged is up to the organization, and one specified that this is the case for live data, but not backup data. Two respondents said this is not possible, with one adding 'unless custom functionality exists', and one stating that any purging of data is done manually by the organization and there is no option to automatically purge data.

Eight of the nine respondents said that it is possible to schedule routine removal of data, with one stating that this is dependent on the removal processes being defined and another adding that this is only possible for live data, not backup data. One respondent said this is not possible.

7. Ownership and Control

All respondents stated that the organization owns the data inputted into the database. Table 4 displays responses when asked a) who has physical custody of the data and b) who owns the hardware used to store the data.

Table 4: Ownership and control (respondents were asked to select all that apply)

	Who has physical custody of the data?	**Who owns the hardware used to store the data?**
The vendor	1	1
The organization	2	2
3rd party contractors in Canada	3	3
3rd party contractors outside of Canada	1	2
Cloud based storage	4	0

All respondents stated that, upon termination of the business relationship between the organization and the vendor, the organization can determine where their data goes, with two people adding further comments including that the organization can extract their data and instruct the vendor to remove the data from the live servers, and that the organization's data resides on the organization's server and they have complete control of it, so they can decide what happens to it.

8. Reports and Report Designer

Table 5 provides an overview of the reporting and report design features available across the different vendor's databases.

Table 5: Reporting and report design features

	Yes	No
Can data reports be exported to Word?	5	4
Can data reports be exported to Excel?	9	0
Can data reports be exported into other reports for specific funding sources?	8	1
Can the organization design their own reports?	8	1
*Can the organization modify existing reports in the database?**	7	2
Is a report wizard built in allowing the organization to extract only certain data?	5	4

*A few respondents who answered yes to this question, also described limitations to this feature such as *'standard reports can be copied, and only the copies can be modified', 'some existing reports are open to the system administrator to be able to make modifications'* and *'reports that the organization has created can be modified by the organization. Reports that we've created for the organization can only be modified by us'.*

Other report features that respondents highlighted included running queries, crosstab reports, filtering data and creating charts and aggregates. One respondent added that they provide access to Tableau as an add-on module. Some described the option to create flexible and tailored reports, for example by matching reports to a particular form, enabling the organization to pull certain information based on specifically chosen parameters, and custom building reports according to identified data and filter needs with the option to "lock down" identified fields to be standardized.

One respondent stated that there are too many reporting features to list, while another stated that they have over 100 grid reports included in their system and over 40 printable reports. A third said they have

over 500 reports available that cover a multitude of categories including case management, service, offenders/victimization, volunteers, staff, demographics and more. Finally, one respondent stated that they offer a report designer, although most of their clients do not use it.

9. Access to Data

Table 6 summarizes the responses to key questions asked about access to data.

Table 6: Access to Data Summary Table

	Yes	No	N/A
Must all users have passwords?	9	0	0
*Does the database require two-factor authentication to log into the database?**	3	6	0
Does the database require two-factor authentication to access records in the database?	2	7	0
Are all data entries tracked back to a user?	9	0	0
Can the vendor set up a system so that access to information can be restricted to certain users?	9	0	0
*Does the vendor's system give any party/parties outside of the organization staff access to the organization data?***	1	8	0
Does the vendor maintain a list of names of all individuals physically or remotely that have access to the server/s, where organization data is stored?	4	4	1
Is an Internet connection necessary to access the organization's data?	6	3	0
Is the vendor willing to enter into any Service Level Agreements with the organization?	8	1	0

*Of the six respondents who said two-factor authentication is not required to log in to the database, two said that it is available and another stated that logging in does require an additional security key.

**The respondent who answered yes, stated that the vendor's staff would be able to access the data, but only with the expressed written consent of the organization's security and compliance officer, and only on a per-incident basis. Another respondent also commented that exceptions to this would be a) if the organization licenced a module that exchanges data with another system, or b) if the organization grants another organization user access to their database.

9.1 Systems restricting access to information

Respondents were asked for further details regarding systems that restrict access to information to certain users. Answers included:

- Configuring and assigning security groups to users (usually defined by role/position) and granting permissions according to user groups e.g. blocking access to certain information such as specific notes, entire client files, or restricting users to certain screens;
- Having unlimited user Profiles that are customizable by the organization, with the organization controlling which Profile they assign to each user;
- Having broadly-defined authorization levels available that can restrict users by site, program/service and/or to their own active clients; and
- Enabling IP filtering and blacklisting to limit what IP addresses are allowed to access the database then further restricting traffic by role/position.

One respondent commented that around 100 other optional detailed security settings are available that refine the role-based access on a 'need to know' or 'need to do' basis.

9.2 Access to the server on which organizations' data is stored

Respondents were asked to indicate the companies whose staff can access the server on which organization data is stored. Results are displayed in table 7. Five respondents said that only the vendor's staff have access to this server, and two selected both vendor and 'others'. 'Others' specified were a) third party contractors in Canada and b) staff at Google's data centers who have access to their own servers, but are unable to read the data because it is encrypted. One respondent did not answer this question, and another said it was not applicable because they do not host or have access to the organization's data - they house and store their own data.

Table 7: Companies whose staff can access the servers on which organization data is stored

Companies	Number
Vendor	7
Vendor sub-contractors	0
Vendor independent contractors	0
Outsource partners	0

Others	2

9.3 Service Level Agreements (SLA)

Respondents were asked to provide details of the Service Level Agreements (SLA) they are willing to enter with an organization. Responses included being willing to consider an SLA if it were proposed; having a standard End User Licence Agreement (EULA) which can be revised and customized on a case by case basis; having a standard Annual Support Agreement that outlines the SLA but also being willing to discuss signing a different SLA if requested by an organization; spelling out the SLA in the product's Software Subscription and Licence Terms and Conditions; the standard contract being the SLA; being willing to create an SLA to meet an organization's needs; and having a standard SLA available on the vendor's website.

10. Data Storage

10.1 Servers and data storage

All respondents said that the data stored on the server belongs to the organization. Three also said data is stored on a dedicated server belonging to the vendor, five said it is not, with one commenting that *'data is stored in a dedicated database. There could be multiple dedicated databases on a shared server',* and one respondent answered this and all other questions in this section as 'not applicable' because they do not host or have access to the organization's data (organizations house and store their own data).

Five respondents stated that data is stored on various servers as chosen by the vendor. When asked to provide details, responses included using US-based servers for US customers and Canadian-based servers for Canadian customers; choosing a company to host the vendor's platform and then choosing which of that company's data centers the platform should be on; and, having production and backup servers at production and backup data centres. Two respondents who said that data is *not* stored on various servers as chosen by the vendor left further comments, including that data is always stored on the organization's server, whether it be a dedicated server, desktop computer acting as a server, or online server; and that the vendor hosts the product on Amazon Web Services (AWS) in Canada and chooses and configures the machines that will be used to host the system, but does not control which physical servers are used for the hosting services.

10.2 Outsourcing data storage

Seven respondents said that the vendor outsources data storage to third parties. Further details provided included that data is stored on:

- Amazon Web Services (AWS) in the US or Canada;
- Microsoft Azure servers in Canada and the US;
- Rogers Cloud Services in Canada;
- Google data centers; and
- SaskTel's Managed Hosting product portfolio.

Six respondents said that the vendor requires an external data centre to comply with the terms of it's contract with the agency.

Table 8 displays the jurisdictions in which respondents stated the data is stored.

Table 8: Jurisdictions in which data is stored

Country and province/state	Number
Canada	**6**
Saskatchewan	1
Quebec	1
Ontario	1
Alberta	1
Unspecified	2
US	**4**
N Virginia	1
Iowa	1
Unspecified	2
Other	1 (Cloud)

Four respondents said that organizations can choose or exclude storage in certain jurisdictions. Four said they could not. Further details given included that this is possible at the country level only, not the state or province level; that the data is always stored on an organization's server, whether it be a dedicated server, 'desktop computer acting as a server,

or online server; and that by default the vendor stores data via Amazon Web Services (AWS), in the US however they can use the Canadian region instead if required.

10.3 Data storage security

Six respondents said the organization's data is stored on the same server as data from other organizations, agencies or companies. The following methods were described regarding how this is managed:

- Logically separating the data from different organizations;
- Storing the data within individual databases;
- Storing the data in a separate SQL schema;
- Segregating the data by Access Control Limits (ACL) so that users can only see their own organization's data.
- Storing the data on a centralized Storage Area Network (SAN) and dedicating Logical Unit Numbers (LUNs) that are allocated to the database server (and never storing an organization's data on local server disk storage);
- Accommodating an individual server if requested by an organization.

All eight respondents stated that servers are physically secured 24/7, and provided further details as follows:

- The datacenter is highly secured, and even the vendor does not have physical access to it.
- The data center does not provide the vendor with details of their security measures, but is audited and produces System and Organization Controls (SOC) reports, which are independent third-party examination reports that demonstrate how the data centre achieves key compliance controls and objectives.
- The vendor uses Nessus to both remotely and locally scan servers and their associated software for security vulnerabilities each night, with critical and high risk vulnerabilities patched as soon as possible, and notifying the organization if downtime is required. Using tools like etckeeper and Zabbix to monitor other factors in real-time.
- Having multi-tier security measures in place.
- Always storing the data on an organization's server, whether it be a dedicated server, a desktop computer acting as a server, or an online server.

- One respondent listed the following features:
  - Unmarked data centres with single secure entrances
  - High-level access security
  - Two-stage authentication process
  - Individually locked cabinets / doors / cage /suite
  - Monitored and staffed 24x7x365
  - Advanced fire suppression systems
  - Redundant HVAC, environmental and power
  - Networked security cameras (low-light technology)
  - PCI DSS, ISAE 3402 Type II, SSAE 16 Type II, CSAE 3416 Type II, SOC 2 Type 2, HIPAA, GLBA compliance
  - N+1 power redundancy
  - Redundant Uninterrupted Power Supply (UPS)

10.4 Emergency power backup

When asked if the location(s) housing the server(s) have emergency power backup for at least three days, six respondents answered yes. Of the six, one clarified that AWS state that their data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and although they do not specify three days, the vendor assumes that is the case. Two respondents did not answer this question, of whom one explained that Google does not make this information public, but they have full faith that Google has taken all possible efforts to protect their business against all manner of power failures.

10.5 Exporting data

When asked if the organization can export all of its data to another data storage system by itself without contacting the vendor, three respondents said it can and six said it cannot. Two who answered yes added that custom scripts needed to be in place, or that the vendor's staff are usually involved to ensure the data is uploaded and adjusted appropriately for the organization's database design. Of the six who said no, one stated that every data conversion project they have done has been unique and complex, and they do not believe

there could be a tool built to allow an organization to do this themselves in an easy and reliable way. Another three respondents also left further comments, including that:

- Each conversion is done by the vendor's development team and is a customized process to make data from another format and system fit into their data structures and meet their minimum requirements.
- The vendor asks the organization to upload a complete export of its data, and then works with them to analyze their data mapping needs, requiring an export from each site planning to migrate data, along with their specific requirements.
- The data has to be provided in SQL format or Excel/CSV data has to be "cleansed" for an unduplicated clients report.

11. Security Practices

Table 9 summarizes the responses to security practices questions.

Table 9: Security Practices Summary Table

	Yes	No	N/A**	No Answer
Does the vendor implement standard security systems such as anti-virus or anti-malware?	6	2*	1	0
Does the vendor implement standard security systems such as host-based firewalls or centralized firewalls?	7	1	1	0
Does the vendor use encryption for data at rest?	7	1	1	0
Does the vendor have capability to decrypt an organization's data?	4	2	2	1

*One of these respondents explained that servers do not get viruses, they get hacked, and said they make other efforts that constitute their defense strategy against being hacked.

**One respondent answered 'not applicable' to all of these questions because they do not host or have access to an organization's data – the organization houses and stores their own data.

12. Hosting

Respondents were asked what their backup system/procedure is. One said this was not applicable as they do not own or have access to the data, and another stated that the data is always stored on an organization's server, whether it be a dedicated server, desktop computer acting as a server, or an online server. They added that once the backup is developed they will release this information. Of the remaining seven, all respondents said backups are performed daily, with one stating that they primarily use functionality that allows for instances to be backed up in real-time via snapshots. Further details provided about this process included naming the data centre service used e.g. AWS, MS Azure or Rogers Cloud Services; stating the length of time that backups are stored for, with responses ranging from one week to two years (with daily backups often being stored for shorter time lengths and weekly/monthly backs ups being retained for longer); explaining where backups are stored e.g. on the vendor's server initially and on a separate server for longer term retention such as an S3 account/bucket, alternate server or Amazon's Glacier service; and explaining how data is transferred e.g. via an encrypted tunnel that stores only encrypted files. A couple of respondents stated that they carry out database transaction logs or archive logs that can be used to do point-in-time recovery, and one also described 'mirroring' each production database to its respective secondary database server. Finally, one respondent explained that they encrypt backups, which are then backed up to a separate availability zone.

Six respondents stated that their backup systems are off-site with the following details provided as to location:

- Secondary data centre in Regina, Saskatchewan
- Off-site via encrypted S3 buckets
- Amazon S3 Ashburn, Virginia
- Cloud-based AWS
- Separate Rogers production and backup facilities in different provinces (Canada)

13. Customer-Provider Relationship

Six respondents said the vendor offers SLAs to guarantee the quality of the service. Two said they do not, of whom one added that the vendor posts service availability goals, but they are not part of the contract per se. One respondent did not answer any of the questions outlined in this section of the report.

Respondents were asked *how* the vendor notifies organizations of the following circumstances regarding changes to security and privacy policies, security incidents and data breaches (one respondent simply answered 'yes' to these questions, therefore the answers summarised are from six respondents):

1. **Changes to the company's security policies and privacy policies**

Methods identified included email, phone, in writing or via the vendor's General Announcements Admin Message Board. One respondent added that they rarely change security or privacy policies as the organization's data is not stored on their servers. One stated that they do not notify clients of changes to their Security Policy, and that details comparable to a privacy policy are included in their licence agreement, noting that this is not a shared service offering. Another stated that security policies are mostly at the discretion of the organization, so the organization actually implements security policy changes in their database. They also said that they do not have a formal policy about privacy policy notifications as their privacy policy has remained stable over the years.

2. **In cases of security incidents and data breaches**

One respondent stated that they have never experienced a security incident or data breach, and another pointed out that since they do not have the organization's data, they do not have security incidents. They added that in the case that they did have a security incident for any reason, they would let the organization know via email and phone call. Another simply said that this is done as detailed in their Licence.

The remaining three respondents identified methods such as telephone, email and writing, having the support team contact the organization's administrator, or via the Admin Message Board if the incident related to the entire system and not a specific organization. In relation to security incidents, one respondent said the vendor ensures that organizations' data is not accessed by vendor staff (unless specifically requested or required by law) and that it is the responsibility of organizations to ensure their staff comply with organizational policies and procedures relating to this. They added that the vendor logs any incidental or otherwise unauthorized users and disclosures associated with an organization in their security incident-tracking tool, but did not specify how the organization is notified. In relation to a data breach, the same respondent explained that they would notify the Customer's Security Contact as soon as practicable, but within no more than 72 hours, and that notification would include (i) identification of the records accessed, (ii) the date of discovery, and (iii) a general description of the nature of the incident.

One respondent reported having experienced a data breach in the past (one did not answer and the remaining seven said they had not). When asked what measures were taken in response to this, the following two scenarios were outlined:

1. *We had a situation where a security feature was not configured to be active in a customer's database. As a result, one user potentially saw data about one record. We identified the data that was potentially accessed and the user who potentially saw it and contacted the customer's administrator.*
2. *A query displayed data to a user that was outside of the user's permissions. The query bug was immediately addressed and hot-fixed. We sent to the customer's administrator a detailed report of the data accessed and the user who saw it.*

Measures they identified to prevent data breaches going forward included carrying out a detailed analysis of what caused the issue and implementing necessary procedures to avoid the problem recurring. They also stated that they carry out security measures and tests to identify potential vulnerabilities to cyber attack and have never found indication or evidence of a data breach via a hacker.

14. Company and Contract

Eight respondents said that their company had been in business for more than ten years. The other reported that it had been in business between 1-10 years.

When asked about the company's procedure for protecting and returning an organizations' data should the vendor cease to operate, answers included adding each new customer to an escrow agreement, or having this option available for a fee; returning the data to the customer in the form of a SQL Backup file or other secure means of their choosing (with one adding that remaining archives would be deleted and drives physically destroyed); enabling the organization to download a backup of their data via an administrative tool and supplying the source code and instructions on how to host the system in a separate document. Two respondents explained that the vendor does not have the organizations' data therefore; it would not be affected should the vendor go out of business. Another did not specify their procedure for this, but stated that they would provide this document on entering a contract with an organization.

Table 10 summarizes the responses to questions regarding contracts and policies.

Table 10: Contracts and policies summary table

	Yes	No	N/A	No Answer
Does the vendor make any formal assurances concerning the security of data which the vendor retains?	4	2	1	2

Does the vendor make any formal assurances concerning the security of data which the processes?	4	2	1	2
Does the vendor's standard contract retain the right to change the terms of the contract without advance agreements from both parties to the contract?	3[a]	3	1[b]	2[c]
Does the vendor have written privacy policies?	5[d]	3	0	1
Does the vendor have written security policies?	6[e]	2	0	1

[a] One added that changes are made with notification and their Terms of Service have been updated once (2015) to include provisions for organizations to agree to track only what is needed and to not violate email spam laws.
[b] One said they generally don't have a contract as the organization is purchasing a product not a service.
[c] One said this is outlined in their licence agreement.
[d] Four said they share this with the organization.
[e] Four said they share a copy of this with the organization

Six respondents said that when an organization deletes data from their system, the data is actually deleted from their **system**, of whom one added that it is removed from the database but history tables remain intact for auditing and support purposes. One stated that the data is also deleted form their **backup system**. The remaining five said it is not, most of whom explained that it is not possible to remove selected data from backups, but that they will eventually be rotated out. One added that an organization can request to have all of their backed up data removed or can change their encryption key (making all of the vendor's backups unreadable to anyone). Another explained that their backups are *'mainly used to restore data back to the Production database as per their client's request.'* Four respondents also stated that the data is deleted from their **server system**. Of the remaining three respondents, one did not answer these questions and two commented that they do not have the organization's data.

When asked if the vendor discloses any organization data or metadata to partners or other third parties as part of their business practices, seven of the nine respondents said they do not. One did not answer and the remaining respondent said that they do, commenting that this would only happen if the customer licenced a module that integrates with a third party, giving the example of Constant Contact for emails.

SUMMARY AND DISCUSSION

Nine database developers took the time to respond to BCSTH's Database Vendor Questionnaire. Database developers shared their product's privacy and security features and protocols that will help Canadian anti-violence organizations make an informed decision about which database will best meet their needs. When starting the process of selecting a database, at minimum, it is recommended that Canadian anti-violence consider the following:

- Agency server or cloud based database
- Customization abilities of the pre-packaged "standard" database product
- Number of users and ability to assign access levels
- Location of where the data is kept
- Data storage access and outsourcing
- Is service recipients data encrypted and if so what kind of encryption is used
- Data breach policies
- Request for records from third policy policies
- Ownership of data
- Level of technical support
- Level of training
- Security policies and
- Additional cost to the organization in staff time, IT upgrades, policy development and training.

Based on the results of the "Database Questionnaire for the BC Society of Transition Houses", the majority of commercial databases:

- allow for the customization of the "standard" database product to varying abilities. This can include deleting, turning off or changing the language of data fields that are not necessary to provide service.
- report being able to set records to permanently delete after a certain period of time as per Canadian privacy legislation.
- offer guidance about the minimum level of security and IT infrastructure requirements for purchasers. However, during database demonstrations, most vendors confirmed that this is only done if asked for by the purchaser. This could be an easy mandatory requirement for commercial database vendors and government databases wishing to sell/have their product used by Canadian anti-violence programs.

- have the capacity to assign each employee their own User ID and password. Note: some databases charge for additional User ID's. It is best practice for each employee/volunteer to have their own User ID as each User ID can be assigned levels of access to records.

RECOMMENDATIONS

A breach of personal information (data) for women, children and youth experiencing violence could put their safety and lives of at risk. With many database options available to Canadian anti-violence organizations, it can be challenging to choose a database that best meets the high level privacy and security needs of those accessing anti-violence support services. Based on the research, all database developers could work to enhance their products and services to better support Canadian anti-violence organizations by:

- supporting them to develop an implementation plan with resources, IT security recommendations and training to better prepare them for the use of a database, and
- understanding Canadian privacy laws and security concerns.

The following section summarizes recommendations for Canadian anti-violence organizations and database developers when working together to implement a database that meets the unique privacy and security needs of both the anti-violence organizations and women, children and youth experiencing violence.

Privacy by design

CUSTOMIZATION

It is best practice for Canadian anti-violence organizations to collect and store the minimal amount of information that is required to deliver the service or program that the recipient has consented to. The databases of vendors that completed our questionnaire have standard data fields that have varying capability to be customized to varying capacities. For example, with some database products, purchasers cannot delete or hide fields, only change the descriptor of the data field title, e.g. from "gender" to "preferred pronoun." Other database developers allow purchasers to pick and choose which data fields should be kept, customized and deleted and others require users to input personal information in a mandatory number of data fields in exchange for a free database.

All of the database developers that completed our questionnaire confirmed that entering data into data fields are optional, however, without organizational policies, training or prompts within the database itself to not collect all the information, having unnecessary fields present can mislead workers to collect information that is not needed. It is recommended that:

- Canadian anti-violence organizations consult with applicable privacy laws to understand the guidelines of what data can be collected;
- Canadian anti-violence organizations consult with their funder contracts to determine what database fields are necessary to provide service and only collect the aggregate data required by funders;
- Database vendors develop a customized database for Canadian anti-violence workers with data fields available from an "opt-in" approach; and,
- Database vendors have each data field as an "option" that can be removed if deemed not necessary to provide services by an organization.

NUMBER OF USERS AND ACCESS LEVELS

Each employee, volunteer, student intern, work placement personnel and board member who has access to the database should have their own User ID and password. The database developers that completed the survey reported that their database has the capacity for all personnel within an organization to have their own User ID. Having a unique User ID not only allows the database to track which files each User ID has accessed but also allows for the ability of each User ID having personalized 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. It is best practice to individualize *levels of access* for each employee, volunteer, student intern, work placement personnel and board member who has access to the database. Limiting the number of users who are authorized to view personal identifiable and sensitive information can help organizations reduce confidentiality breaches.

The database vendors who completed the questionnaire confirmed that their databases have the capability to assign access levels to each user. Though having a unique User ID and access level for each personnel is a positive feature, some database developers create barriers for underfunded anti-violence organizations to follow best practice guidelines by increasing the cost of the database as the number of users increase.

It is recommended that database developers encourage anti-violence organizations to assign User ID and access levels for each personnel accessing their database by:

- training an organization's database administrators to create User ID and access levels for each employee, volunteer, student intern, work placement personnel and board member who has access to the database;
- make the process to create User ID and access levels user friendly;
- not charge anti-violence organizations more money for additional number of User IDs.

DESTRUCTION OF PERSONAL INFORMATION

Canadian provinces and territories have privacy laws that dictate how long an organization must retain and destroy the personal information of service recipients. This is true for information stored in a database because the collected data about the service recipient is considered their personal record.

Based on the questionnaire results, databases have the ability to store personal information until an organization decides to stop using the database. One concern is that even when an anti-violence organization does stop using a cloud-based database, the permanent removal of data from a third party cloud storage facility is not guaranteed.

It is recommended that database developers/vendors:

- allow for the customization or design of a database that follows the retention and destruction parameters outlined in privacy laws. Database products available in Canada should have to have the capacity to permanently delete data. This would help programs be able to comply with privacy legislation.
- work with anti-violence organizations to determine a timeframe for closed files to be permanently deleted off the database
- work with any third party server and cloud-based storage company to ensure that anti-violence organization's data can and will be permanently deleted
- product has the ability for all backups of records to be permanently deleted
- prevent the database or database vendor from having the ability to automatically retrieve a service recipient's past record once it has been permanently deleted.

Data storage and retention

OWNERSHIP

All respondents to our questionnaire reported that the anti-violence organization owned the data stored in the purchased database. This may not be the case for all databases used or available to Canadian anti-violence organizations. Anti-violence organizations are encouraged to ensure they are the owners of their data before purchasing or agreeing to use a database.

LOCATION OF DATA

All questionnaire respondents disclosed the location of where their company stores data. With privacy laws varying from country to country and within each country, it is recommended that if database developers are to sell their database product within Canada, that the option to store data on a Canadian server is available.

THIRD PARTY ACCESS

Seven questionnaire respondents contract the storage of data to a third party. In their licensing/purchasing agreements with Canadian anti-violence organizations, database developers should be transparent about:

- the name of the storage sub-contractor;
- location of the storage sub-contractor;
- how many servers the organization's data is stored on;
- who within the storage sub-contractor has access to the anti-violence organization's data;
- steps the database developer and storage sub-contractor will take to protect the organization's data; and,
- guarantee of permanent data destruction.

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 personal information. It is recommended that database vendors be transparent about the type of encryption

their database uses and its benefits and risks. For example, if the database does not zero-knowledge encrypt data, details about the encryption method and who is able to un-encrypt an anti-violence organization's data should be discussed before an anti-violence organization purchases a database.

Training and policy development

TRAINING

All questionnaire respondents provide training in some capacity about how to set up, administer and use their database. This varies from pre-recorded videos, webinars, conference or video calls and in-person training. When participating in database demonstrations, it was asked if developers provide training about the needs of an organization's IT security infrastructure. All of the database developers verbally confirmed that this is possible but not offered or done unless asked. It is recommended that:

- training about how to use the database is available for all of the organization's personnel;
- training about the minimum level of IT security infrastructure needed to ensure security of service recipient's personal information with practical recommendations take place prior to granting a database license to enhance due diligence;
- training about any privacy and security risks of the using the database such as third party access, location of storage, database developer access to personal information takes place with each person that has access to the database.

DATABASE USE POLICY DEVELOPMENT

Before implementing a database, it is recommended that anti-violence organizations develop clear policies and procedures that outline privacy practices for collecting, storing and purging sensitive data[5]. Developing a written 'use of database' policy can be time consuming for anti-violence organizations who do not have the resources to develop one or the technical knowledge to translate the database into a plain language policy document. It is recommended that database developers provide Canadian anti-violence organizations with a written resource about their database to help guide an organizational use of database policy.

[5] For more information see BCSTH's Legal Toolkit https://bcsth.ca/projects/legal-education-resources/

BREACH OF PRIVACY POLICY

All database developers should have a data breach policy that they can share with those interested in purchasing their database. It is recommended that database developers make these policies available to anti-violence organizations in the beginning exploration stages to ensure complete transparency about how far the developer will go to protect an anti-violence organization's data. In addition to providing organizations with the database developer's privacy breach policies, it would be helpful for database developers to provide guidance to organization about the development of their own breach of privacy policy.

FINAL THOUGHTS

There will always be concerns about breach of data and confidentiality when personal information is stored online. Being informed about the capabilities and risks of each database before storing service recipient information on online is just the beginning of the due diligence process.

BCSTH is pleased by the amount of responses we received to our questionnaire. We appreciate the time that database vendors took to complete the questionnaire and provide the team with demonstrations of their database.

BCSTH does not endorse any product. It is clear from the submitted responses that the database developers who participated in the survey have good intentions. However, only a few are designed with the goals of developing a product with the privacy and security of women, children and youth experiencing violence at the forefront.

APPENDIX: Database Vendor Questionnaire for the BC Society of Transition Houses

DATABASE VENDOR QUESTIONNAIRE FOR THE BC SOCIETY OF TRANSITION HOUSES

PRODUCT & VENDOR INFORMATION	DETAILS
Name of Database Product & Name of Vendor	
In case we have follow-up questions, please provide representative contact details:	Name & Title:
	Phone:
	Email:
Date Questionnaire Completed (mm/dd/yyyy)	
What country are you located in?	Product:
	Vendor:
Is this product available in Canadian provinces and territories?	☐ Yes ☐ No
	If "Yes" please check the relevant Canadian Provinces and Territories: ☐ Alberta ☐ British Columbia ☐ Manitoba ☐ New Brunswick ☐ Newfoundland and Labrador ☐ Northwest Territories ☐ Nova Scotia ☐ Nunavut ☐ Ontario ☐ Prince Edward Island

	☐ Quebec ☐ Saskatchewan ☐ Yukon

Please provide us with information about your product and fill in your responses to the best of your ability. Some of the questions ask for Yes/No answers, text answers and in some circumstances both. The questionnaire refers to "organization/s" as being the client/s accessing your product. Thank you for your cooperation and time.

GENERAL FEATURES	ANSWERS
Is your system "user friendly"?	☐ Yes ☐ No If "Yes", please describe the features that make the system "user friendly."
Is the individual user interface customizable?	☐ Yes ☐ No If "Yes", please describe the customizable features (e.g. font---size, color, etc.)
How long does it take an average user to complete a new client profile?	

Does the system check for duplicated clients?	☐ Yes ☐ No
Can additional data be entered into the record once the client profile is created?	☐ Yes ☐ No
Does the system allow for temporary "shift change notes" separate from a client's record?	☐ Yes ☐ No If "Yes", can the temporary "shift change notes" be routinely destroyed in a short time-frame such as a digital post-it?
Can the paper files be replaced with notes and narratives with the digital system?	☐ Yes ☐ No If "Yes", can the narrative notes be automatically purged at a set time?
Does the system allow attachment of scanned documents?	☐ Yes ☐ No If "Yes," can the scanned documents be automatically purged at a set time after a client is no longer accessing the program?
How many individuals /Login User Id's can use the system at the same time?	
Is this a "cloud- based" storage system	☐ Yes ☐ No

CUSTOMIZATION	ANSWERS
Can the organization edit items in the drop down lists?	☐ Yes ☐ No
Can the organization set which fields are required?	☐ Yes ☐ No
Can the organization add fields?	☐ Yes ☐ No
Can the organization hide fields?	☐ Yes ☐ No
Can the organization completely remove fields?	☐ Yes ☐ No
Can the organization change the **text** of fields?	☐ Yes ☐ No
Can the organization change the **labels** of fields?	☐ Yes ☐ No
Are there other customization features available to the organization?	☐ Yes ☐ No If "Yes", please describe:
PRIVACY AND SAFETY	**TEXT ANSWERS**
Can data be retrieved for a single client?	☐ Yes ☐ No
Are third parties able to **retrieve** organization data?	☐ Yes ☐ No If "Yes", who are the third parties?
Are third parties able to **view** organization data?	☐ Yes ☐ No If "Yes", what kind of data is shared?

Does the vendor notify the organization of subpoenas, warrants, law enforcement requests or any civil or administrative request for data or records?	☐ Yes ☐ No If "Yes", when is notice given? If “Yes”, how is the notice given?
Does the vendor give the organization an opportunity to resist disclosure before the vendor responds to subpoenas, warrants, law enforcement requests or any civil or administrative request for data or records?	☐ Yes ☐ No
Does the vendor itself resist the disclosure of organization data or records containing personally identifiable information stored by the organization?	☐ Yes ☐ No If “Yes”, how?
Does the vendor retain discretion to disclose organization data or records to third parties’ requests?	☐ Yes ☐ No If “Yes”, in what circumstances? If “Yes”, how does the vendor inform the organization of this discretion?

Does the vendor agree to be bound by the same duty of professional and legal confidentiality obligations as the organization they are providing the product to?	☐ Yes ☐ No If "Yes", please describe how this formalized in the contract for services:
Does the vendor have a written policy about the vendor's and company's response to **domestic** subpoenas, warrants, law enforcement requests or any civil or administrative requests for organization data or records?	☐ Yes ☐ No If "Yes", does the vendor share a copy of this policy with the organization? ☐ Yes ☐ No If "Yes", can the vendor please share a copy of that policy with BCSTH by emailing it to rhiannon@bcsth.ca or provide a link here to the policy.
Does the vendor have a written policy about the vendor's and company's response to **foreign** subpoenas, warrants, law enforcement or any civil or administrative requests for organization data or records?	☐ Yes ☐ No If "Yes", does the vendor share a copy of this policy with the organization? ☐ Yes ☐ No If "Yes", can the vendor please share a copy of that policy with BCSTH by emailing it to rhiannon@bcsth.ca or provide a link here to the policy.
Is organization data available to the vendor in an **unencrypted** format?	☐ Yes ☐ No
Is organization data available to the vendor in an **encrypted** format?	☐ Yes ☐ No
If organization data is encrypted, who is the responsible for the encryption key management?	☐ Vendor ☐ Organization

	☐ Both vendor and organization Please provide details:
TECHNICAL SUPPORT	ANSWERS
Is technical support available for the organization?	☐ Yes ☐ No If "Yes", please describe:
Will the vendor's technical support install software for the organization?	☐ Yes ☐ No
How many technical support staff does the vendor have?	☐ 1 ☐ 2-5 ☐ 5-10 ☐ More than 10
What are the hours the vendor technical support staff are available?	Check all that apply: ☐ 24 hours a day ☐ Office hours e.g. 9am-5pm ☐ Evenings ☐ Weekends Other:
Is there a test/training version of the vendor's product that the organization can access before contracting with the vendor?	☐ Yes ☐ No If "Yes", please provide details:

Does the vendor provide training for organization staff before using the product?	☐ Yes ☐ No If "Yes", please provide details including training format (webinar/in person) and cost:
DATA RETENTION	ANSWERS
Can data be permanently deleted by the organization?	☐ Yes ☐ No
Can data be purged from all locations where backed-up?	☐ Yes ☐ No
Can some types of data be purged before others?	☐ Yes ☐ No If "Yes", what types?
Is it possible to schedule routine removal of data?	☐ Yes ☐ No
OWNERSHIP AND CONTROL	ANSWERS
Does organization own the data inputted into the database?	☐ Yes ☐ No
Who has physical custody of data? Please check all that apply.	☐ Vendor ☐ Organization ☐ 3rd party contractors in Canada ☐ 3rd party contractors outside of Canada ☐ Cloud-cased storage
Who owns the hardware used to store the data? Please check all that apply.	☐ Vendor ☐ Organization ☐ 3rd party contractors in Canada ☐ 3rd party contractors outside of Canada

Upon termination of the business relationship between the organization and the vendor, can the organization determine where their data goes?	☐ Yes ☐ No
REPORTS	ANSWERS
Can data reports be exported to Word?	☐ Yes ☐ No
Can data reports be exported to Excel?	☐ Yes ☐ No
Can data reports be exported into other reports for specific funding sources?	☐ Yes ☐ No If "Yes", please provide details:
REPORT DESIGNER	ANSWERS
Can the organization design their own reports?	☐ Yes ☐ No
Can the organization modify existing reports in the database?	☐ Yes ☐ No
Is a report wizard built in allowing the organization to extract only certain data?	☐ Yes ☐ No
Are there other report features to highlight?	☐ Yes ☐ No If "Yes", please provide details:
ACCESS TO DATA	ANSWERS
Who creates log-ins?	☐ Organization staff ☐ Vendor ☐ Both organization staff and vendor

Does each individual user create their own log-in password?	☐ Yes ☐ No If "No", please provide details:
Must all users have passwords?	☐ Yes ☐ No
Does the database require two-factor authentication to log into the database?	☐ Yes ☐ No
Does the database require two-factor authentication to access records in the database?	☐ Yes ☐ No
Are all data entries tracked back to a user?	☐ Yes ☐ No
Can the vendor set up a system so that access to information can be restricted to certain users?	☐ Yes ☐ No If "Yes", please describe details:
Can the vendor control who can **create** each type of data?	☐ Yes ☐ No
Can the vendor control who can **edit** each type of data?	☐ Yes ☐ No
Can the vendor control who can **delete** each type of data?	☐ Yes ☐ No
Can the vendor control who can **view** each type of data?	☐ Yes ☐ No
Do staff of the vendor have access to the data in readable form?	☐ Yes ☐ No
Does the vendor's system give any party/parties outside of the organization staff access to the organization data?	☐ Yes ☐ No If "Yes", please provide details:

Please indicate the companies whose staff can access the servers on which organization data is stored. Check all that apply.	☐ Vendor ☐ Vendor sub-contractors ☐ Vendor independent contractors ☐ Outsource partners ☐ Others: _____
Does the vendor maintain a list of the names of all individuals physically or remotely that have access to the server/s, where organization data is stored?	☐ Yes ☐ No
Is an internet connection necessary to access the organization's data?	☐ Yes ☐ No
Is the vendor willing to enter into any service level agreements with the organization?	☐ Yes ☐ No If "Yes", please describe the details of the agreements:
DATA STORAGE	ANSWERS
Does data stored on the server belong to the organization?	☐ Yes ☐ No
Are backup systems included or are they available?	☐ Yes ☐ No
Is data stored on a dedicated server belonging to the vendor?	☐ Yes ☐ No
Is data stored on various servers as chosen by the vendor?	☐ Yes ☐ No If "Yes", please provide details:
Does the vendor outsource data storage to third party/ies?	☐ Yes ☐ No If "Yes", please provide details as to whom:

Does the vendor require an external datacenter to comply with terms of its contract with the agency?	☐ Yes ☐ No
In which jurisdictions is data stored? Please list all:	Country(ies): Canadian Provinces and/or Territories: US State/s: Others:
Can organizations choose or exclude storage in certain jurisdictions?	☐ Yes ☐ No If "Yes", please provide details":
Is the organization's data on the same server as data from other organizations, agencies or companies?	☐ Yes ☐ No If "Yes", please provide details:
Are servers physically secured 24/7?	☐ Yes ☐ No If "Yes or No", please provide details of security measures:

Does the location/s housing the servers/s have emergency power backup for at least 3 days?	☐ Yes ☐ No
Does the location/s housing the server/s have "redundant internet connections"?	☐ Yes ☐ No
What is the vendor's backup procedure?	
Can data be imported from an older system?	☐ Yes ☐ No
Can the organization import the data itself without contacting the vendor?	☐ Yes ☐ No If "No". please provide details:
Can data be exported for the organization to another data storage system?	☐ Yes ☐ No
Can the organization export all of its data to another data storage system by itself without contacting the vendor?	☐ Yes ☐ No
If the organization exports all its data, is it in a common format?	☐ Yes ☐ No If "Yes", which format?
Are there limits on the number of records the system can handle?	☐ Yes ☐ No If "Yes", what is the limit?

Does your system have other data storage features to highlight? If so please provide details.	
SECURITY PRACTICES	ANSWERS
Does the vendor have a dedicated security team?	☐ Yes ☐ No If "Yes", how many staff are on the team? ☐ 1 ☐ 2-5 ☐ 5-10 ☐ More than 10
Does the vendor implement standard security systems such as file integrity monitoring software?	☐ Yes ☐ No
Does the vendor implement standard security systems such as intrusion detection systems?	☐ Yes ☐ No
Does the vendor implement standard security systems such as anti-virus or anti-malware?	☐ Yes ☐ No
Does the vendor implement standard security systems such as host-based or centralized firewalls?	☐ Yes ☐ No
In order to determine security gaps, does the vendor perform penetration testing?	☐ Yes ☐ No
In order to determine security gaps, does the vendor perform regular vulnerability assessments?	☐ Yes ☐ No If "Yes" how regularly are vulnerability assessments conducted? ☐ Weekly ☐ Fortnightly ☐ Monthly ☐ Quarterly ☐ Bi-annually ☐ Annually Other:

Does the vendor incorporate security in your software development lifecycle, specifically threat modeling?	☐ Yes ☐ No
Does the vendor incorporate security in your software development lifecycle, specifically security code reviews (OWASP code review top 9)?	☐ Yes ☐ No
Does the vendor incorporate security in your software development lifecycle, specifically independent audits?	☐ Yes ☐ No
Does the vendor operate any systems or software that is outdated and no longer gets security updates from their respective vendors?	☐ Yes ☐ No If "Yes", please provide details:
Does the vendor follow security notices and CVEs?	☐ Yes ☐ No
Does the vendor apply security updates on your infrastructure in a timely manner?	☐ Yes ☐ No If "Yes", please define "timely".
What kind of physical security measures do you implement for access control?	
What kind of physical security measures do you implement for sign-in process for visitors?	
What kind of physical security measures do you implement for facilities' monitoring?	

Does the vendor perform regular system logs audits looking for unusual events?	☐ Yes ☐ No
Does the vendor perform regular system logs audits looking for failed access attempts?	☐ Yes ☐ No
Does the vendor review accounts and access permissions on a regular basis?	☐ Yes ☐ No
Does the vendor delete or decommission unnecessary accounts or systems?	☐ Yes ☐ No If Yes, please provide further detail.
Does the vendor use encryption for data at rest?	☐ Yes ☐ No
Does the vendor use encryption for data in transit?	☐ Yes ☐ No
Does the vendor have a document describing which encryption and authentication methods are implemented in your infrastructure?	☐ Yes ☐ No If "Yes," does the vendor share a copy of this document with the organization? ☐ Yes ☐ No If "Yes", can the vendor please share a copy of this document with BCSTH by emailing it to rhiannon@bcsth.ca or provide a link here to the policy.
Does the vendor store passwords in clear-text?	☐ Yes ☐ No
Does the vendor hold a copy of the encryption keys?	☐ Yes ☐ No
Does the vendor have the capability to decrypt an organization's data?	☐ Yes ☐ No
If using a third party company to host the infrastructure, does the third party have access to decryption keys?	☐ Yes ☐ No

If using a third party company to host the infrastructure, does the third party have access to unencrypted data?	☐ Yes ☐ No
Does the vendor default to HTTPS for every web connection?	☐ Yes ☐ No
Does the vendor encrypt data backups?	☐ Yes ☐ No
HOSTING	ANSWERS
What kind of infrastructure is used to host applications and data?	
Does the vendor manage their own infrastructure?	☐ Yes ☐ No If "No, "is the infrastructure hosted with a third party or cloud provider such as AWS, Google Cloud, etc.? Please provide details:
If the system is self-hosted…	…is it a multi-tenant infrastructure? ☐ Yes ☐ No
	…how do you segregate data from other tenants and ensure access control?
	…is the infrastructure hosted in its own datacenter, or in a secure cage in a shared datacenter?
	…where are the data centers located? Please list all: Countries:

	Canadian Provinces and/or Territories: US State/s: Others:
Is the system built using a third party company	☐ Yes ☐ No
Does the vendor have a formal change control process?	☐ Yes ☐ No If "Yes" please specify:
Are your systems built, configured, and deployed using modern processes and technologies such as version control?	☐ Yes ☐ No
Are your systems built, configured, and deployed using modern processes and technologies such as continuous delivery and deployment?	☐ Yes ☐ No
Are your systems built, configured, and deployed using modern processes and technologies such as infrastructure as code or configuration management?	☐ Yes ☐ No
Does the vendor's infrastructure design include network segregation?	☐ Yes ☐ No
Does the vendor use a DMZ to separate the public facing web servers and the database servers?	☐ Yes ☐ No
Does the vendor's infrastructure design include high availability and redundancy?	☐ Yes ☐ No

Does the vendor have a disaster recovery plan?	☐ Yes ☐ No If "Yes" please provide details and when it was last tested:
Have you implemented monitoring and alerting systems for your infrastructure?	☐ Yes ☐ No If "Yes", how do you monitor? How frequently do you monitor? ☐ weekly ☐ fortnightly ☐ monthly ☐ quarterly ☐ bi-annually ☐ annually Other:
What is your backup system?	
How frequently is your infrastructure backed up by your back up system?	☐ daily ☐ weekly ☐ fortnightly ☐ monthly ☐ quarterly ☐ bi-annually

	☐ annually Other:
Is your backup system on-site or off-site?	☐ Yes ☐ No If your backup system is offsite, please provide details as to location.
CUSTOMER-PROVIDER RELATIONSHIP	ANSWERS
Does the vendor offer service-level agreements (SLA) to guarantee the quality of the service?	☐ Yes ☐ No If "Yes", does the vendor share a copy of the SLA with the organization? ☐ Yes ☐ No If "Yes", can the vendor please share a copy of the SLA with BCSTH by emailing it to rhiannon@bcsth.ca or provide a link here to the policy.
Does the vendor offer service-level agreements (SLA) to guarantee the availability of the service?	☐ Yes ☐ No
How often do you plan…	…downtime for service upgrades?
	…downtime for applying patches?

How do you notify customers regarding…	…**scheduled** downtime?
	…**unscheduled** downtime?
Does the vendor have a service status page?	☐ Yes ☐ No
How can organizations contact you in case of outage or other service disruption?	
Do you have a web-based ticketing system?	☐ Yes ☐ No
Can you describe your organization support escalation procedures?	
How does the vendor notify organizations when changing the company's…	**…security** polices?
	…**privacy** policies?
How does the vendor notify organizations in cases of…	**…**security incidents?

	…data breaches?
Has your company had a data breach in the past?	☐ Yes ☐ No If "Yes", What measures were taken to respond to the data breach? What measures were taken to prevent data breaches going forward?
COMPANY & CONTRACT	ANSWERS
How long has your company been in operation as a business?	☐ Less than 1 year ☐ 1-10 years ☐ More than 10 years
Will the vendor provide references from similar organizations, agencies, companies that are located in Canada that currently use the vendor's product?	☐ Yes ☐ No
What is the company's procedure for protecting organization's data if the vendor ceases to operate as business?	
What is the company's procedure for returning data to the organization if the vendor ceases to operate as a business?	

Does the vendor's standard contract disclaim any warranties related to provision of database and data storage services?	☐ Yes ☐ No If "Yes", what are the disclaimed warranties?
Does the vendor's contract limit liability for breach of contract?	☐ Yes ☐ No If "Yes", what are the liability limitations?
Does the vendor's contract contain a choice of law clause?	☐ Yes ☐ No If "Yes", what is the choice?
Does the vendor make any formal assurances concerning the security of data which the vendor either retains?	☐ Yes ☐ No
Does the vendor make any formal assurances concerning the security of data which the vendor processes?	☐ Yes ☐ No
Does the vendor's standard contract retain the right to change the terms of the contract without advance agreements from both parties to the contract?	☐ Yes ☐ No
Does the vendor have written **privacy** policies?	☐ Yes ☐ No If "Yes", does the vendor share a copy of this policy with the organization?

	☐ Yes ☐ No If "Yes", can the vendor please share a copy of this policy with BCSTH by emailing it to rhiannon@bcsth.ca or provide a link here to the policy.
Does the vendor have written **security** policies?	☐ Yes ☐ No If "Yes", does the vendor share a copy of this policy with the organization? ☐ Yes ☐ No If "Yes", can the vendor please share a copy of this policy with BCSTH by emailing it to rhiannon@bcsth.ca or provide a link here to the policy.
Please describe what organization activities are logged by the vendor?	
Does the vendor have access to the organization activity logs?	☐ Yes ☐ No
How long are the logs maintained by the vendor?	
When an organization deletes data from your system, is the data actually deleted from your…	…system? ☐ Yes ☐ No If "No", please provide details:
	…**backup** system? ☐ Yes ☐ No If "No", please provide details:

	…**server** system? ☐ Yes ☐ No If "No", please provide details:
What is the vendor's process for return of organization data in case of service termination?	
Do you disclose any organization data or metadata to partners or other third parties as part of your business practices?	☐ Yes ☐ No If "Yes", please provide details: