BC Society of Transition Houses

Electronic Database and Case Management System Use by Anti-Violence Organizations across Canada

BC Society of Transition Houses

ACKNOWLEDGMENTS

Research, Writing, Editing:

Rhiannon Wong
Nicky Bowman
Amy S. FitzGerald
Louise Godard

French Translation *Michele Briand*

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.

BC Society of Transition Houses

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[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, "Electronic Database and Case Management System Use by Anti-Violence Organizations across Canada," is one of three reports 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. This report summarizes and

[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/

[3] The 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.

discusses findings from the "Electronic Database and Case Management System Use by Anti-Violence Organizations across Canada" online survey.

Anti-violence organizations, which are considering a database or are currently using one, are 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.

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 also provide suggestions for programs who are currently using a database, as we know most database vendors are open to supporting changes to existing systems to enhance the privacy of personal information. 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 "Understanding Databases Options for Canadian Anti-Violence Organizations" 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, youth and children they support so that both can make informed choices about the collection and electronic storage of personal information.

ELECTRONIC DATABASE AND CASE MANAGEMENT SYSTEM USE BY ANTI-VIOLENCE ORGANIZATIONS ACROSS CANADA ONLINE SURVEY SUMMARY REPORT

Respondent Information

One hundred and eighty-three anti-violence workers responded to the Electronic Database and Case Management System survey, of whom 145 (79.2 per cent) responded to the English version of the survey, and 38 (20.8 per cent) responded to the French version.

Survey respondents worked in anti-violence organizations located across eleven provinces and territories in Canada, the majority of which were in British Columbia (44.8 per cent), followed by Quebec and Ontario (20.4 per cent and 11.6 per cent respectively) (figure 1).

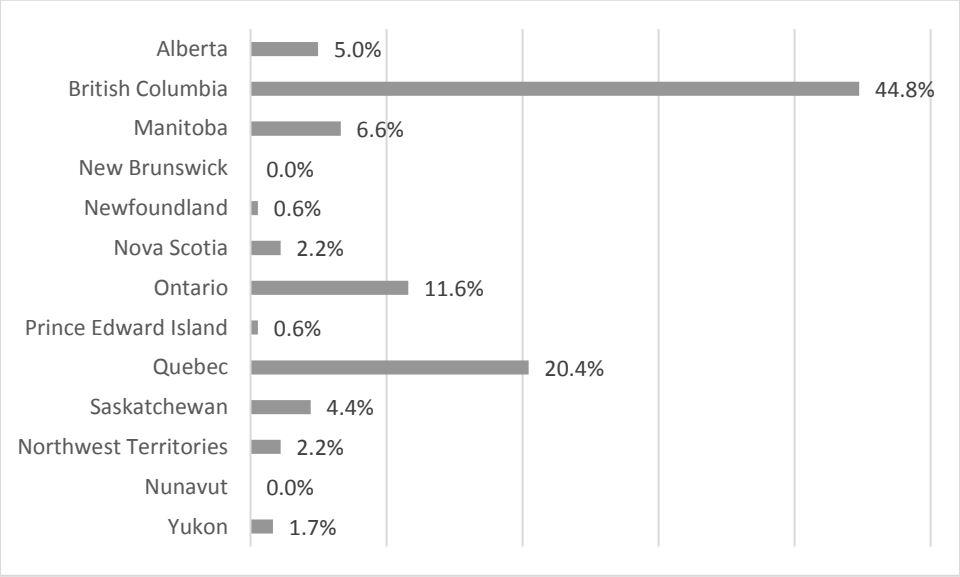

Figure 1: Where is your anti-violence organization located? (n = 181)

Figure 2 displays the type of anti-violence organizations that respondents worked at. Most commonly, respondents worked at Women`s Shelters/Transition House Programs (58.8 per cent), followed by Police

Based Victim Service Programs (10.5 per cent), and Children and Youth Exposed to Violence Programs (9.9 per cent).

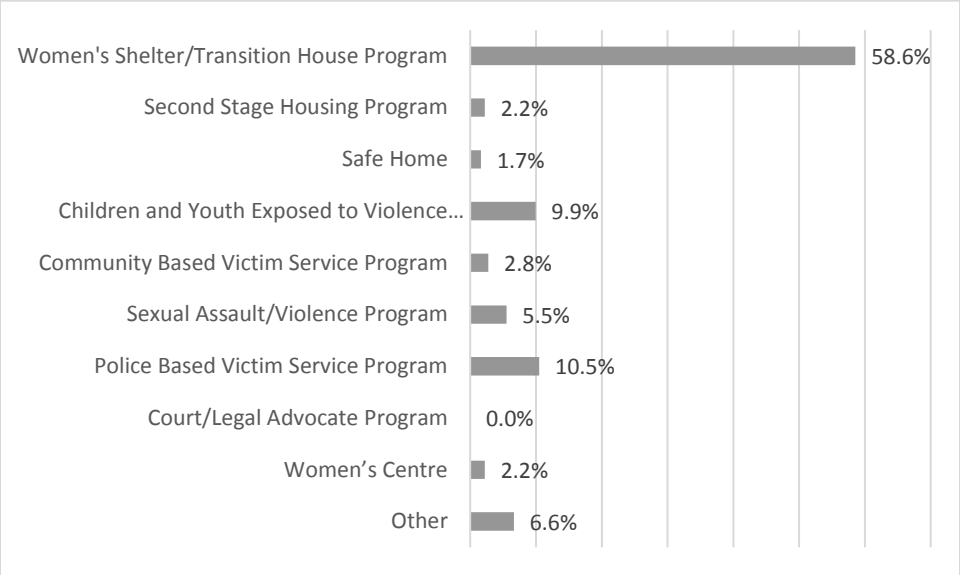

Figure 2: What type of anti-violence organization are you responding to this survey on behalf of? (n = 181)

Of the twelve people (6.6 per cent) who selected 'other', many reported being from multi-service agencies (appendix 1).

Just over half of respondents (52.5 per cent) worked for an organization that provides combined sexualized and domestic violence support for women and/or children; 43.7 per cent worked for an organization that supports women and/or children who have experienced domestic violence, and the remaining seven people (3.9 per cent) worked for an organization that supports women and/or children who have experienced sexualized violence (two people did not answer this question).

The vast majority (95.1 per cent) worked for non-profit organizations; three (1.6 per cent) worked for for-profit organizations and six (3.3 per cent) were not sure.

Record Keeping

95 respondents (51.9 per cent) said they use an electronic database or client case management system *in their practice*, 82 (44.8 per cent) said they do not, and six (3.3 per cent) were unsure (figure 3).

Of the 95 respondents who reported using a database *in their practice*, 61 (64.2 per cent) also stated that *their organization* uses a hybrid system i.e. they keep both electronic and paper files.

Of the 82 respondents who said they are not using a database or client case management system *in their practice*, 65 (79.3 per cent) said that *their organization* keeps only paper files, and 16 (19.5 per cent) said *the organization* uses a hybrid system. One was unsure.

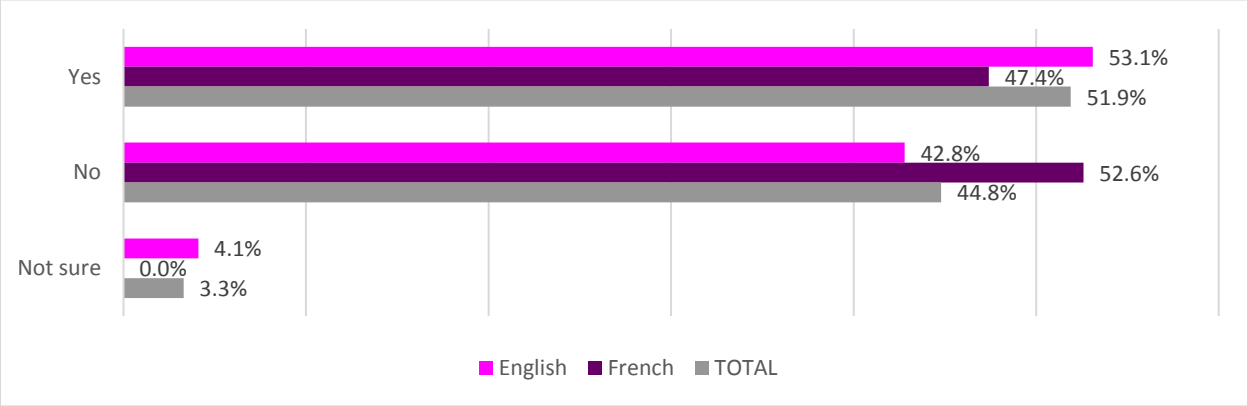

Figure 3: In your practice, are you using an electronic database or client case management system? (n=183: 145 Eng and 38 Fr)

Respondents were asked for further details on how their organization practices record keeping.

Exactly one third of respondents (46 English and 15 French) said their organization keeps only paper files and does not have an electronic database.

Just under a third (30.1 per cent) of respondents (52 English and 3 French) said the names and other personally identifiable information and case notes are kept in an electronic database or case management system.

18.5 per cent (26 English and 8 French) said the names and other personally identifiable information are kept in an electronic database but case notes or notes are kept as paper files.

2.7 per cent (3 English and 2 French) were unsure.

The remaining 15.3 per cent (18 English and 10 French) selected 'other' and provided further comments (see appendix 2 for the full list of comments). The majority of these comments related to keeping a combination of both electronic and paper records, for example:

We use basic Excel spreadsheets with very minimal contact information only. Other details are kept on paper.

We use a combination of electronic and paper forms. We do most case notes electronically, but often print off notes to ensure we have a paper copy as well.

Combination - we are only using our WISH database at a minimum but will be using it more [for] case notes. We have a client running log that is not a counselling record plus paper files for each counselling session/contact. We also have the original inventory log of names, sins, date of admission in an Outlook file, not shared on any network.

All files are entered into our electronic database, however only certain staff have access, other staff/volunteers record notes on a paper file that is then eventually destroyed once the info is logged electronically.

Many explained that they store names/personally identifiable information and case notes in different ways, such as:

Names/personally identifiable information and case notes are kept in electronic database; paper file contains printed notes, all client's consents and sometimes artwork for children.

Names and personally identifiable information are kept only as paper files; basic non-identifying information is kept electronically.

The names and other personally identifiable information and case notes are kept digitally but separately. Case notes refer to a client number stored in a separate spreadsheet. Paper files have notes and limited personally identifiable information.

In some cases, respondents stated that they were in the process of moving from paper to electronic record keeping, and that was why they currently kept both electronic and paper records:

> *We are in the process of moving to a fully electronic system but still have some paper files.*
>
> ***Working on setup of an electronic database this year.***
>
> *Counselling program is separate from shelter and has moved to electronic files only.*

A couple of respondents said they store electronic copies of Word documents:

> ***Primarily, we use software like Microsoft Excel and case notes are often saved in Word files. Save on a cloud service.***
>
> *We do not have an electronic database or case management system. We keep electronic case notes or notes electronically in Word, and paper files.*

Respondents were asked, if they were not using an electronic database of any kind, if their organization is considering implementing an electronic database or case management system in the future. Results are displayed in figure 4.

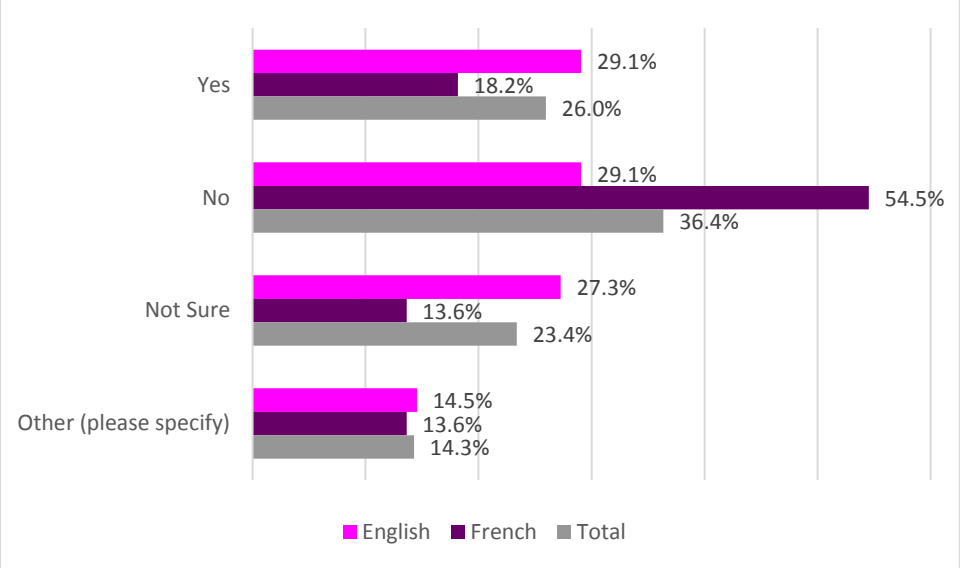

Figure 4: If you are not using an electronic database of any kind, is your organization considering implementing an electronic database or case management system in the future? (n=77: 55 Eng and 22 Fr)

Of the six respondents (14.3 per cent) who selected 'other', four said this is because they lack the resources (financial and/or human) to implement one, and two suggested they may get one in the future:

1. *Yes if we could afford software costs and staff training.*
2. *I have been asking for one for years but we cannot afford one so we continue with paper only.*
3. *We want it but not possible because they lack the financial and human resources in this area*
4. *We do not plan to set up a system. However, if one already exists, we would be interested. This is clearly a need in our shelter.*
5. *It has been discussed in the past and the decision was made at that time to not use one but I expect it will be re-visited in the future.*
6. *Not at this time.*

Database or Client Case Management Systems

The remainder of this report summarises responses from 122 respondents who reported that their organization uses an electronic database or case management system (99 English and 23 French respondents in total).

Respondents were asked why their organization decided to implement the use of an electronic database/case management system (selecting as many reasons as applied from a multiple-choice list). The most common reasons were to streamline the record keeping process (48.4 per cent) and to assist employees with record keeping obligations (43 per cent) (figure 6).

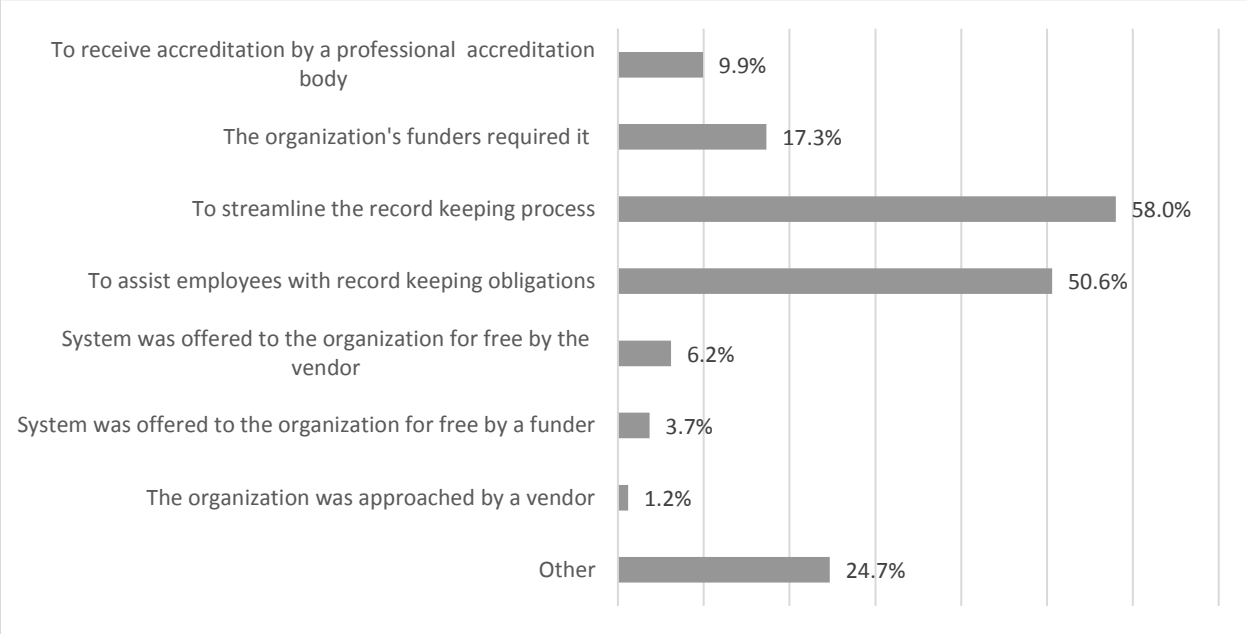

Figure 6: Why did your organization implement the use of an electronic database/case management system? Please check all that apply (n=81; 70 Eng and 11 Fr)

Of those who said 'other', the following responses were provided:

1. *The Provincial Coalition offered a provincial-wide database with support for a small fee (this database is used by most shelters in Alberta).*
2. *Set up prior to opening through Alberta Council of Women's Shelters (ACWS)*
3. *Unsure*
4. *I was not part of the decision, nor was I at this agency when we went electronic, but I imagine it was to streamline records and be more efficient with storage, as well as environmentally friendly.*

5. *Use police record management system.*
6. *We developed our own that worked for us.*
7. *To eliminate the need for paper files that take up a lot of space as well as to make client records available to all shelter programs the client may access. A client may access emergency shelter, second stage and/or outreach services.*
8. *The data base system we use is not a case management system for all residents in our transition house. It is a database required for providing Homelessness Prevention Program funds to women in our transition house, second stage, and outreach programs.*
9. *The need had been identified for years and the organization worked with the PVS workers to ascertain the needs and then developed a program across Canada.*
10. *To access statistical data.*
11. *Safety of files for clients and best practice.*

Those who said that the organization's funders required it, or that the system was offered for free by a vendor or funder, were asked to specify which funder/vendor. Responses are listed below:

1. *Provincially implemented but required RCMP reliability security screening*
2. *RCMP E-Division implemented and developed policy*
3. *E-Division RCMP created VSIS and mandated its use*
4. *RCMP Victim Services Information System all electronic*
5. *RCMP E Division requires us to use the electronic file system provincially.*
6. *Requirement by E Division*
7. *RCMP*
8. *RCMP*
9. *Homeless Individuals and Families Information System (HIFIS) was offered by the federal government*
10. *Homeless Individuals and Families Information System (HIFIS)*
11. *Homeless Individuals and Families Information System (HIFIS)*
12. *Provincial Justice requires funded shelters to use WSIS, and we use HIFIS as it is a free database for our other programs to access.*
13. *Provincial government and Alberta Council of Women's Shelters (ACWS)*
14. *Government of Alberta's Human Services is main funder; ACWS is professional body, which requires database Outcome Tracker as part of membership.*
15. *Ministry of Community and Social Services*
16. *MCSS*
17. *Health funder*
18. *BC Housing*

19. *Government of Saskatchewan*
20. *CARF-MCFD*

Figure 7 shows the responses given when asked to estimate the length of time it took the organization to decide on an electronic database/case management system before implementing. Almost a third of respondents (31.3 per cent) said 0-6 months, and just over a third (37.5 per cent) said 'other'.

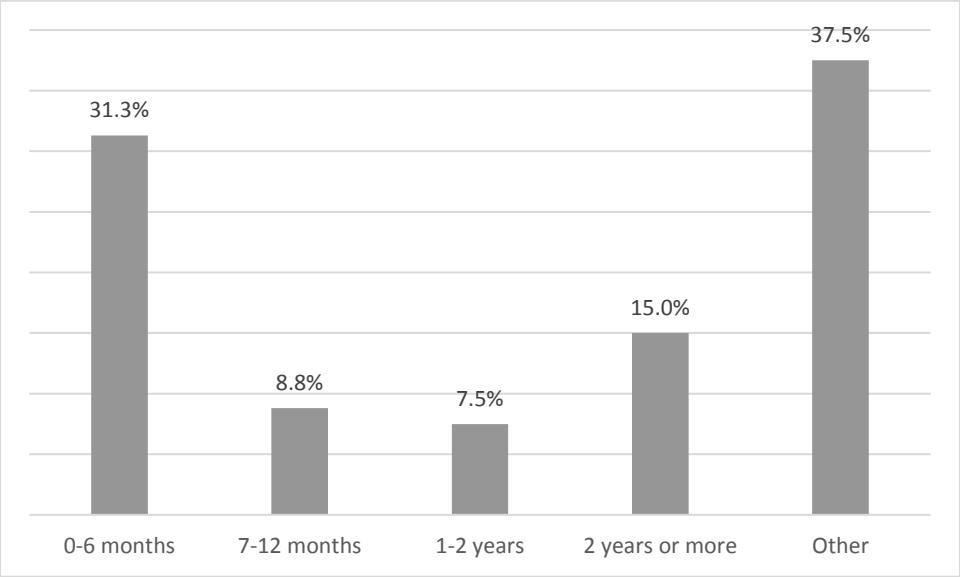

Figure 7: Please estimate the length of time it took for your organization to decide on an electronic database or case management system before implementing it (n= 80; 70 Eng and 10 Fr).

Of those who said 'other', fifteen respondents stated that they do not know how long this took, of whom four explained this was because either they were not involved or it was implemented before they worked there. Others said it was decided outside of the organization e.g. provincially decided/required by a funder, or that it took many years:

1. *Implemented an Access database in 1999.*
2. *Database in use by shelter system preceding inception of organization.*
3. *Had no say in implementation (required by funder).*
4. *It was not our decision to make.*
5. *Provincially decided.*
6. *None - it was required by the Ministry of Justice*
7. *Already set up through ACWS*
8. *Ongoing, as we developed it ourselves.*

9. *RCMP E-Division took years to approve and create the first version of VSIS*
10. *10 years*
11. *Discussions were held over many years, with the major concern being confidentiality, safety and the right to privacy.*
12. *The organization has existed for about 30 years and we have paper house stats since always, we electronically entered the data from the moment our stay was two years in 1998 and we have a stats system provided by the federation women's shelters for about ten years.*
13. *Destruction of paper file from women. We keep the scanned data for two years.*
14. *Consolidation of houses for women victims of domestic violence.*

Respondents were asked which database they use. The most common responses were Microsoft Excel, Women in Safe Housing (W.I.S.H.) and Victim Services Information System (VSIS) (Table 1).

Table 1: List of databases respondents reported using

Database	Number of respondents
EXCEL	14
Women In Safe Housing (WISH)	13
Victim Services Information System (VSIS)	11
Homeless Individuals and Families Information System (HIFIS)	9
Outcome Tracker by VistaShare	6
ACCESS	4
Women Shelters Information System (WSIS)	4
Other	3
Penelope	2
Sharevision	2
ALICE	1
BC Housing Connections	1
Caseworks	1
EZNet Scheduler	1
Google docs	1
Nucleus	1
Pimsy	1
RCMP custom designed for security	1
Système de Gestion Statistiques FMHF	1
Verasaderm Record Management System	1

Table 2 gives a breakdown of the databases used across different provinces.

Table 2: Databases used across different provinces

Where is your anti-violence organization located?	**What electronic database or case management system is your organization currently using?**	**Total**
Alberta	Outcome Tracker by VistaShare	6
	Pimsy	1
British Columbia	VSIS	11
	WISH	10
	EXCEL	7
	HIFIS	2
	ACCESS	2
	Penelope	2
	Sharevision	2
	BC Housing Connections	1
	Nucleus	1
	RCMP custom designed for security	1
Newfoundland	HIFIS	1
Nova Scotia	HIFIS	4
Ontario	WISH	2
	Verasaderm Record Management System	1
	EXCEL	1
	ACCESS	1
	Google docs	1
	Caseworks	1
Prince Edward Island	EXCEL	1
	HIFIS	1
Québec	EXCEL	3
	Other	3
	Système de Gestion Statistiques FMHF	1
	ALICE	1
Saskatchewan	WSIS	4
	EXCEL	2
	HIFIS	1
	EZNet Scheduler	1
Yukon	ACCESS	1
	WISH	1

Five respondents who selected '*other*' when asked which database their organization uses, left the following comments:

1. *System of the federation of which I do not know the database.*
2. *Housekeeping system for case management and statistical software of the Federation of Transition Houses for the compilation of statistics only.*
3. *Digitized information sheet in PDF version.*
4. *Home base.*
5. *Home database.*

Just over half of respondents (59.3 per cent) said that their organization a) owns the electronic database or case management system and b) owns or controls the server(s) where the organization's records and data are stored (figure 8).

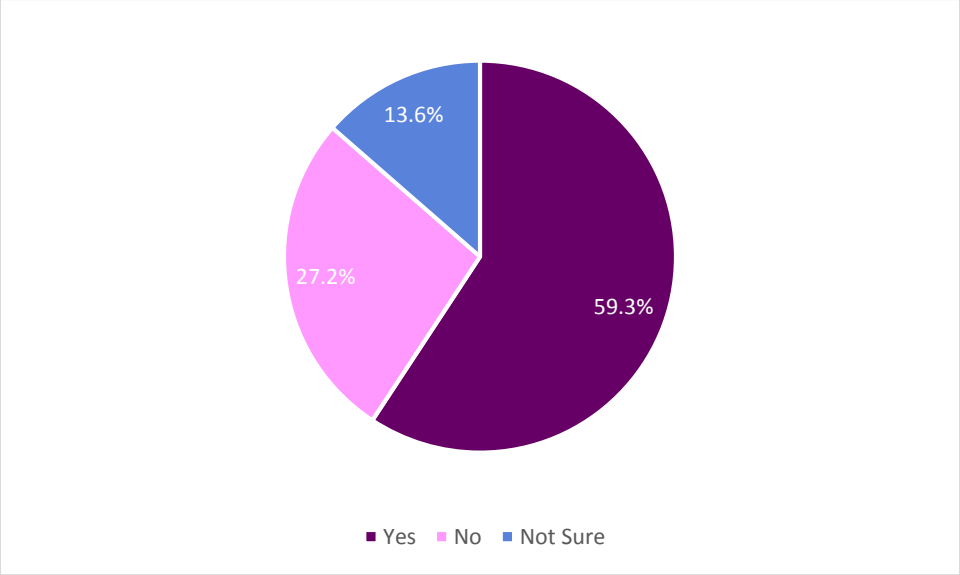

Figure 8: Does your organization own the electronic database or case management system? (n=81; 71 Eng and 10 Fr)

The vast majority of respondents (93.8 per cent) said that each system user has their own individual password-protected account to access the electronic database or case management system, and that the organization ***does not*** have one system account and one password that is shared by many employees (87.3 per cent).

When asked how long it takes, on average, for an employee's database account and password to be deleted or changed after they leave the organization, the most common response was *the day they leave* (34.6 per cent), followed by *within a week of their exit* (18.5 per cent) and *within a day of their exit* (17.3 per cent) (figure 9).

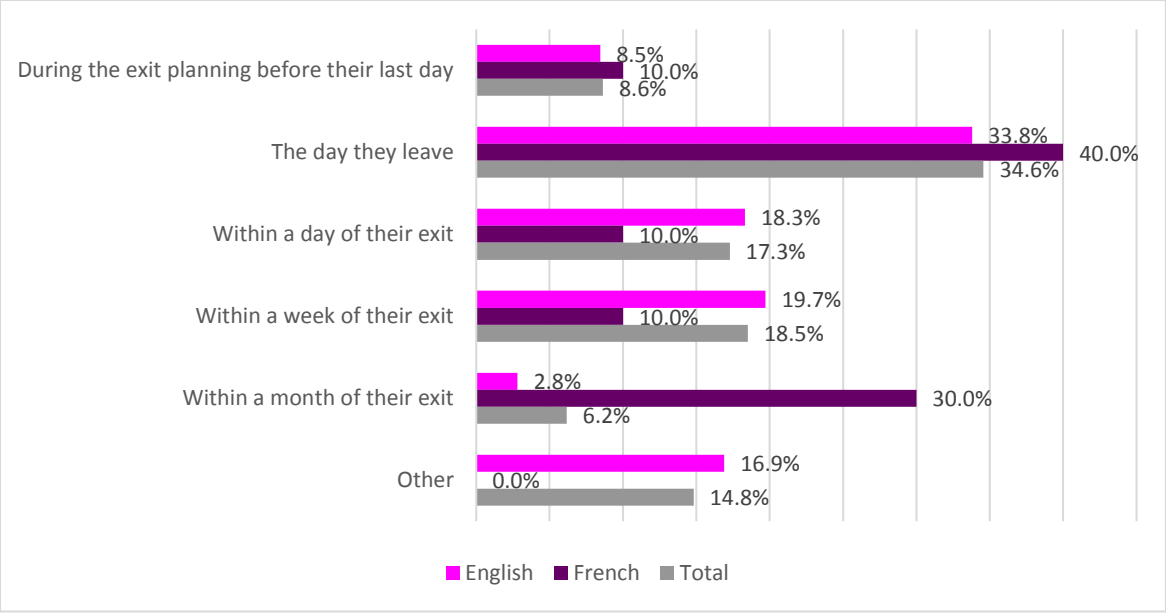

Figure 9: When an employee leaves the organization, on average how long does it take for the employee's database account and password to be deleted or changed? It happens... (n=81; 71 Eng and 10 Fr).

Of the 12 people who said *'other'*, six were unsure, and six left the following further comments:

1. *We have not had an employee leave but we will implement a policy that it happens on their last day.*
2. *No policy in place so it varies between a few days and...never being done/being done months later.*
3. *As soon as we inform BC Housing the employee has left.*
4. *They are immediately no longer given access to our buildings, so effectively their access to everything is immediately cut off. Our building is entirely passcode access and we can revoke someone's passcode from any location in the world, 24 hours a day.*
5. *When the new employee takes over their desk*
6. *Only house manager has password.*

Respondents were asked further questions regarding the capabilities of their organization's electronic database or case management system, including whether they can isolate individual records, hide data fields, reorder questions or make them optional, whether records are encrypted and if they can be accessed remotely by employees or the system vendor. Results are displayed in figure 10.

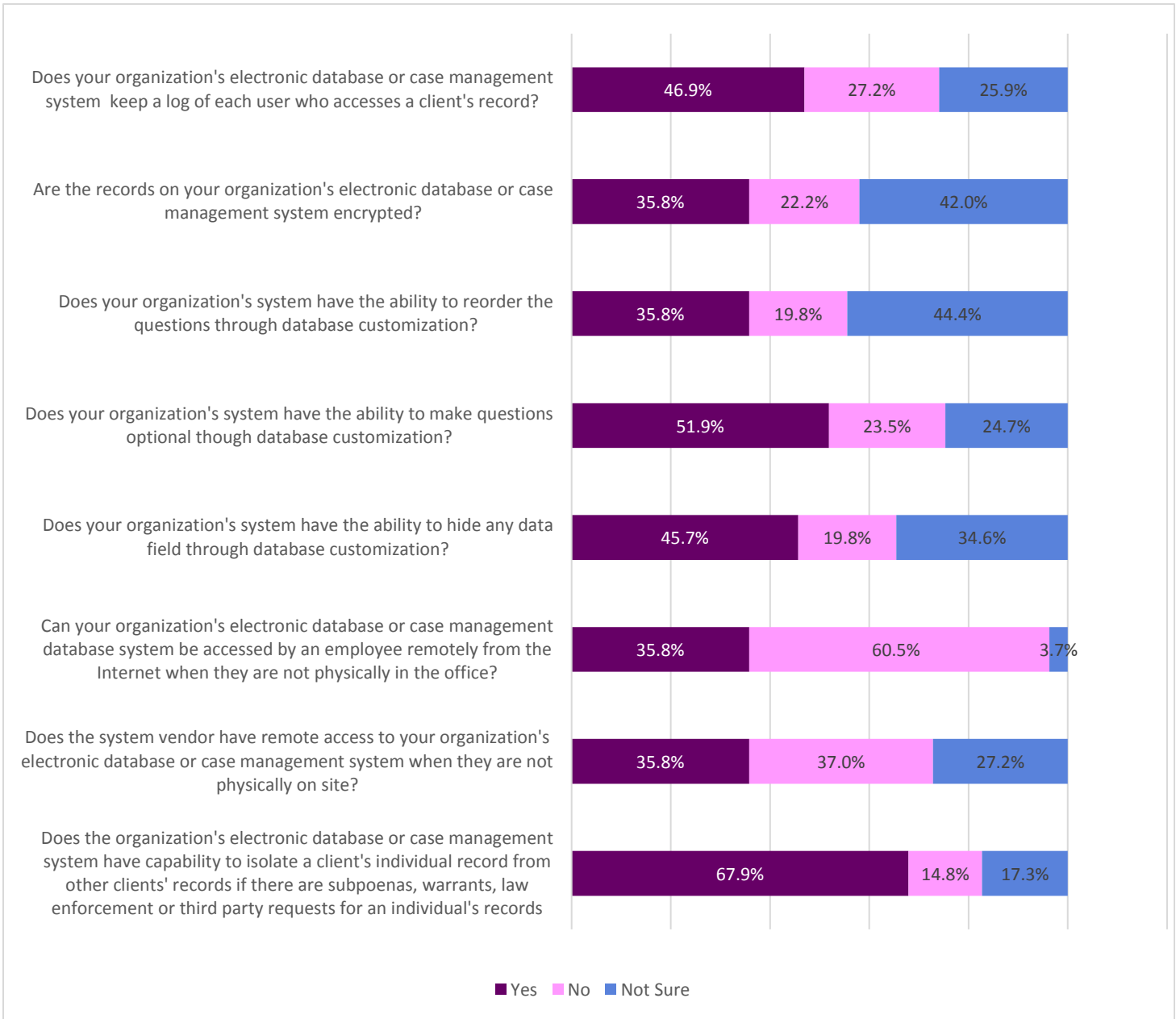

Figure 10: Further capabilities of electronic databases and case management systems (n=81: 71 Eng and 10 Fr)

When asked how often the organization's electronic database or case management system is backed up, the most common response was *daily* (51.9%), followed by *not sure* (27.2%) (figure 11). One person said *'other'* and commented '*15 mins'.*

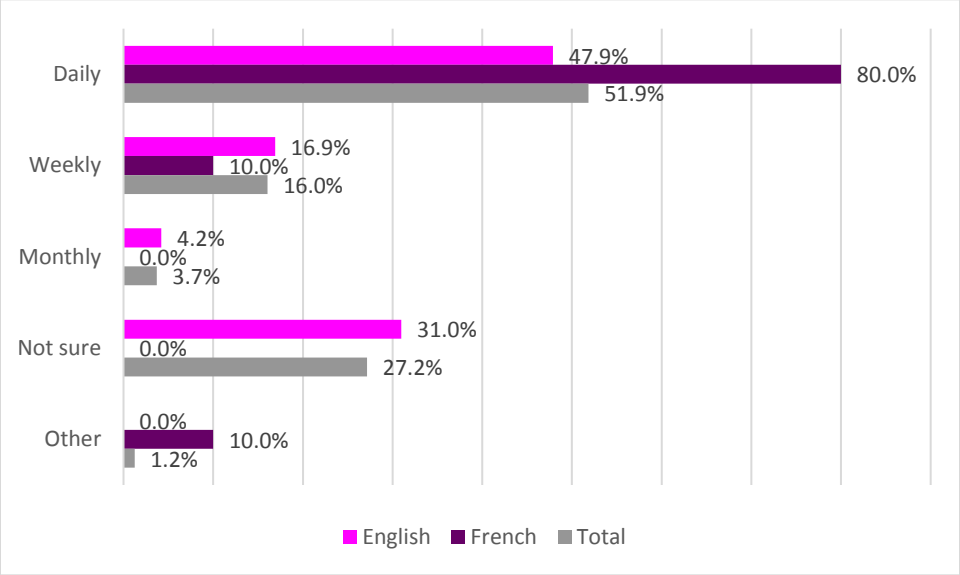

Figure 11: How often is the organization's electronic database or case management system backed up? (n=81: 71 English and 10 Fr).

Just under a third of respondents (30.9 per cent) reported that a client's record and data are purged immediately from the electronic database or case management system as a routine practice as soon as the organization determines the record can be destroyed. Slightly more than a third (35.8 per cent) reported that they are not, and the remaining 33.3 per cent did not know (figure 12).

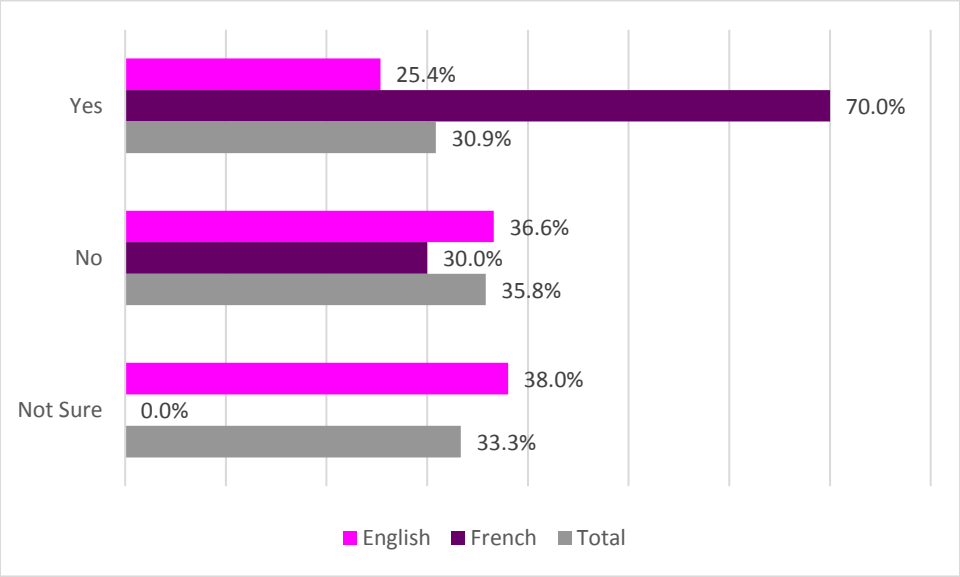

Figure 12: Is a client's record and data purged immediately from the electronic database or case management system as a routine practice as soon as the organization determines the record can be destroyed? (n=81: 71 Eng and 10 Fr)

Those who answered no were asked what their organization's approach to the destruction of records is (see appendix 3 for full list of responses). Responses ranged from destroying *paper* records annually to every 10 years. Some simply stated that records are destroyed every five or seven years, but did not specify whether this related to paper or electronic records, or both. The majority of responses stated that a process was not yet in place for the destruction of electronic records, or that electronic data is not destroyed. A few stated that they do not destroy client records (again without specifying whether this related to paper or electronic records or both).

Respondents were asked where the client's record or data that the organization enters into the electronic database or case management system is stored. The most common answer was *on a server owned by our organization on site*, with one third of respondents selecting this option (33.3 per cent). The next most common response was *not sure* (30.6 per cent) (figure 13).

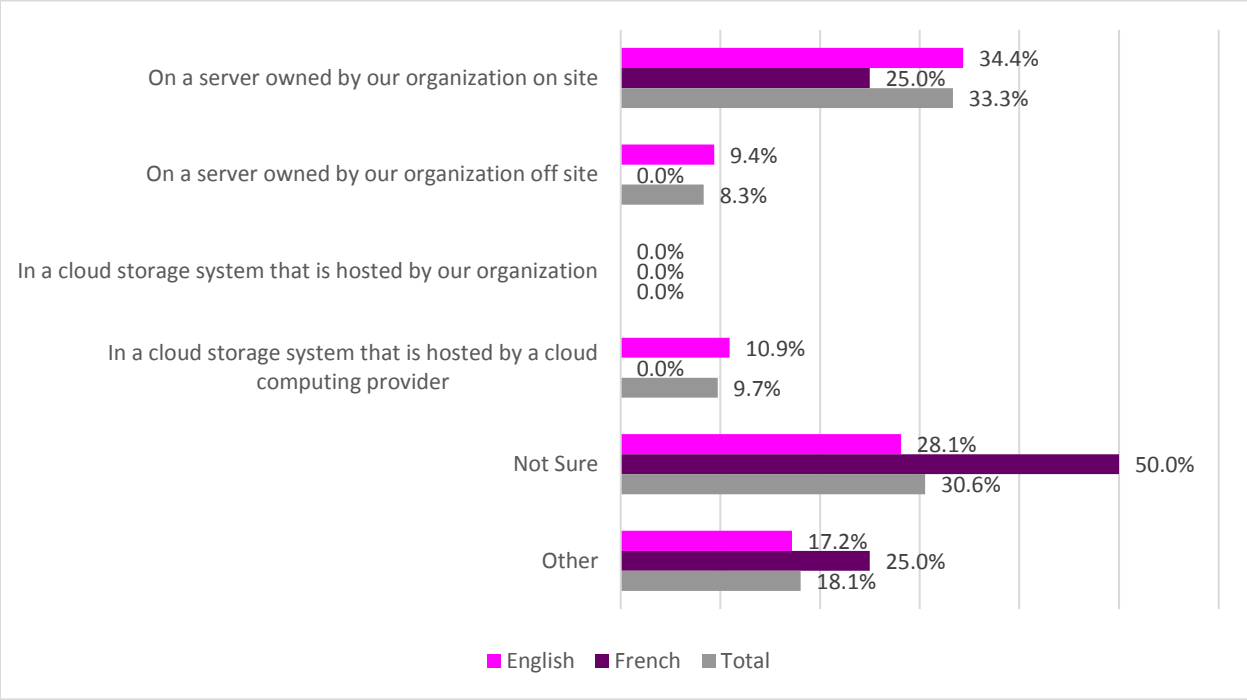

Figure 13: Where is the client's record or data stores that your organization enters into the electronic database or case management system? (n=72; 64 Eng and 8 Fr)

Those who said '*other'*, gave the following responses:

1. *On a server owned by the company who operates the site.*
2. *On a server owned by a partner (School District)*
3. *On a server not owned by our organization off site in Canada*
4. *Stored by BC Housing; cloud storage system hosted by servers in Canada?*
5. *Athena*
6. *HIFIS Server*
7. *Our own server, and an offsite backup server.*
8. *On an internal server - daily back up is hosted externally*
9. *On the computer, backed up to USB and Carbonite*
10. *External disk plugged in for consultation only*
11. *Presently we are on our own server but we are hoping to move to a cloud base server so all provincial shelters can access it.*

12. *For most of our records they are currently on a server; however, we are in the process of moving to a cloud storage system. For WSIS that is stored on a government server that we sign into through the internet.*
13. *At the moment our data is being entirely stored on our own server but Athena software is moving to a cloud based system and we will not have access to services or software updates unless we do so. We have undergone an extensive process by which we satisfied ourselves with Athena's data management, storage, facility locations, staffing, security clearances for staff, encryption, etc. As such, by the end of 2018 we will be moving to this cloud based system.*

Respondents were asked, if their organization uses a cloud storage system that is hosted by a cloud computing provider, where the cloud storages system is sited. Just over half of respondents (51.9 per cent) reported that they were not sure where it is sited. Just over a quarter (25.9 per cent) said it is sited in Canada, and a further four people (7.4 per cent) said it is sited in the organization's province or territory. On person said the United States of America, and the remaining seven people (13 per cent) selected *other country,* five of whom commented 'not applicable', one who said '*it's ours on our site managed by us'* and another who explained that '*if we move to the cloud version we are planning on using a company in Canada.'* (Figure 14.)

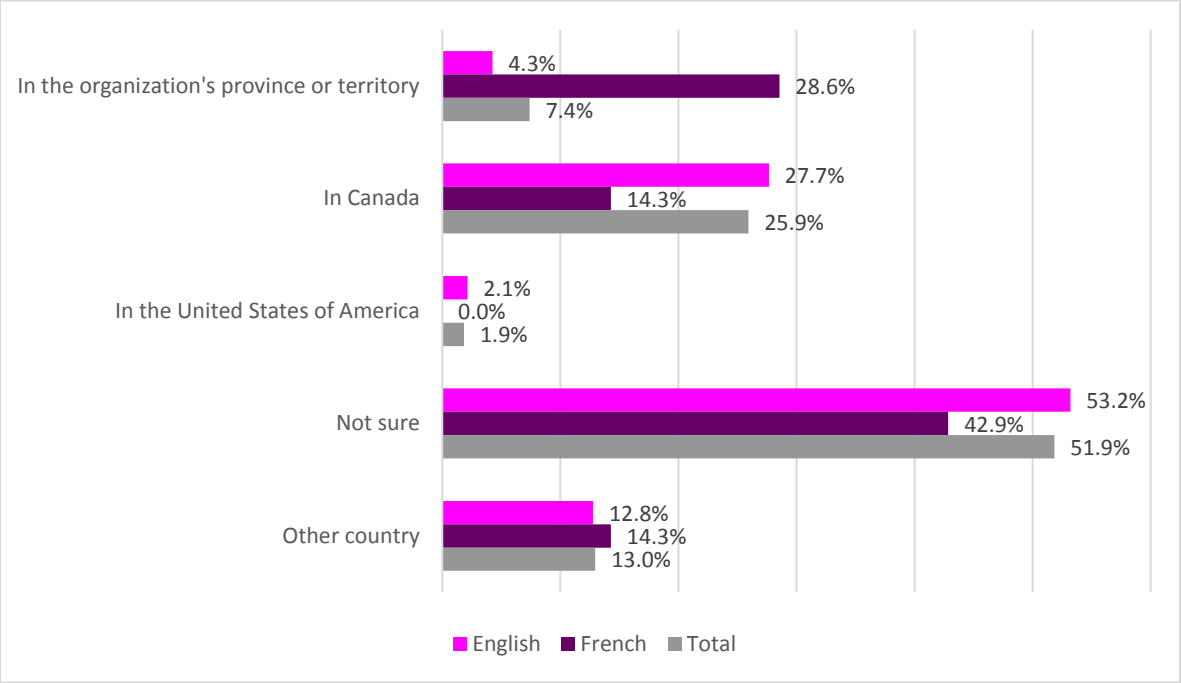

Figure 14: If your organization uses a cloud storage system that is hosted by a cloud-computing provider, where is their cloud storage system sited? (n=54; 47 Eng and 7 Fr).

Of the 72 people who answered, the vast majority (91.7 per cent) reported that the computer, laptop, tablet or mobile device that is used by an employee to access the electronic database or case management system is connected to the Internet. Of the remaining six people, four (5.6 per cent) said it was not, and two (2.7 per cent) were unsure.

When asked what records employees have access to in the electronic database or case management system, 50 per cent of respondents reported that employees have access to all the records of women and children stored in the database/case management system. A further 18.1 per cent said employees have access to records of the women and children that access the specific program they work for, and 13.9 per cent said employees only have access to the records of the women and children who they conducted the intake and opened the record for (figure 15).

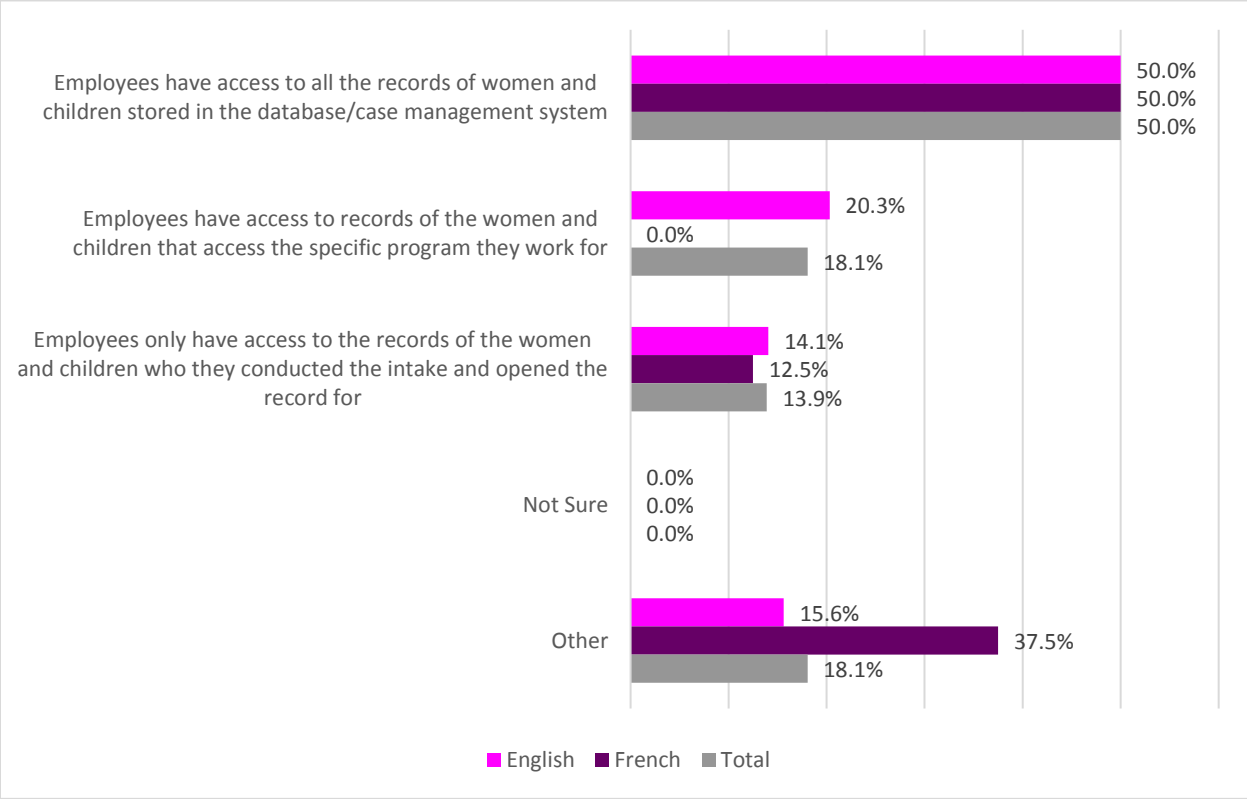

Figure 15: What records do employees have access to in the electronic database or case management system? (n=72; 64 Eng and 8 Fr)

Of the 13 respondents (18.1 per cent) who selected *other,* some said only certain employees have access to the database; others explained that restrictions can be put on some records:

1. *Only one person has access to the database*
2. *Only the Admin Assistant, who inputs information as our Outcome Tracker Administrator and the Executive Director have access to the records.*
3. *Database is only accessible by 2 admin staff. Program workers receive print outs specific to their program only.*
4. *Only two managers have access to the database.*
5. *Only certain employees have access.*
6. *Only certain employees have remote access.*
7. *Employees have access to records which have been assigned to them by the Coordinator.*
8. *Only to their assigned case load unless they do intake then it is only to that program area.*

9. *Employees have access to all the records of women and children stored in the DB but we have the ability when needed to restrict access of a clients file to a designated staff person due to conflict of interest or if a higher level of confidentiality is needed.*
10. *Employees have access to all records unless protected by ED.*
11. *BC Housing Connections: access to all records of organization; HIFIS: access to all records in organization, limited by region.*
12. *Have access to the scanned information sheet in the last 2 years. Current records are kept on paper.*
13. *Employees have access only to paper records stored for 5 years*

Informed Consent

Just under half of respondents (45.8 per cent) reported that their organization's informed consent process does *not* state that the organization uses an electronic database. Slightly fewer (40.3 per cent) reported that it does.

Just more than half of respondents (51.4 per cent) said that clients *cannot* opt out of having their personally identifiable information and records entered and stored in an electronic database or case management system as part of the organization's informed consent process. Just over a third (34.7 per cent) said they can.

Just over a third of respondents (36.1 per cent) reported that client's records *can* be purged from the organization's database or case management system if, after agreeing to this record keeping they then withdraw their consent to having their information stored in an electronic system. A quarter (25 per cent) said they cannot and the remaining 38.9 per cent were unsure. (Figure 16)

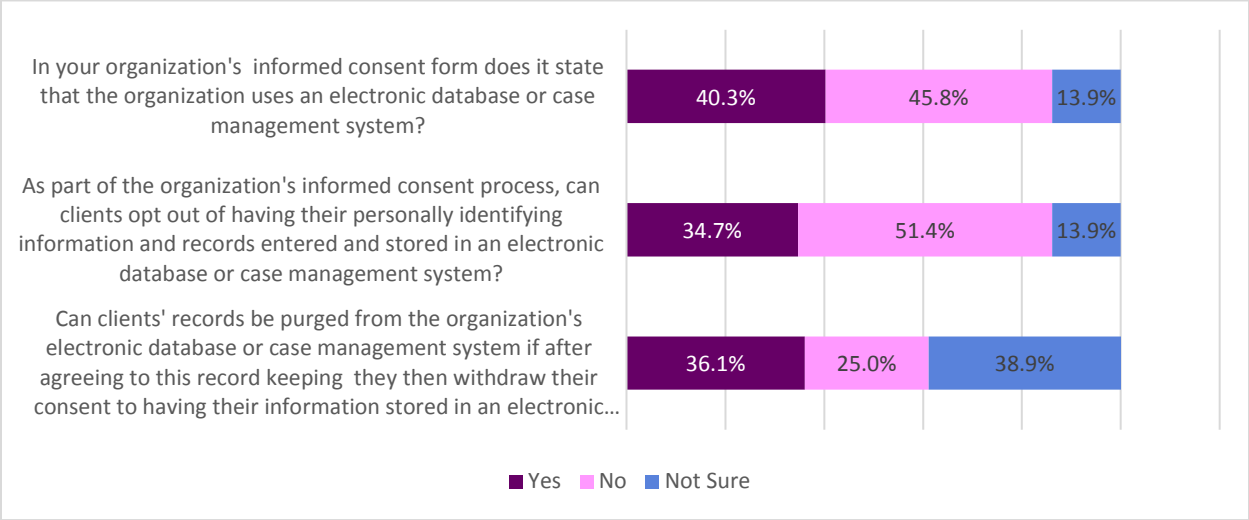

Figure 16: Questions regarding informed consent (n=72; 64 Eng and 8 Fr)

When asked how long it takes for a client's record to be permanently deleted from the electronic database or case management system, the majority or respondents were not sure (58.2 per cent). The next most common answer was within a day (16.4 per cent) (figure 17).

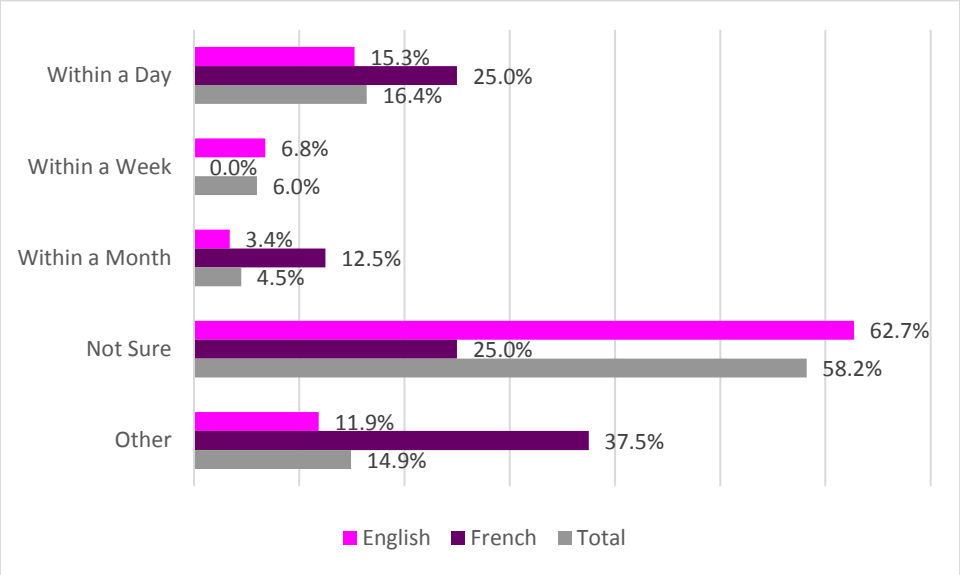

Figure 17: If the organization is able to purge a client's record, what is the time frame for the permanent deletion from the electronic database or case management system? (n=67 (59 Eng and 10 Fr).

Those who selected *'other'* left the following comments:

1. *According to RCMP file retention policy*
2. *We do not have an electronic database or a case management system. The digitization of the information sheet meets a need for archiving. The digitized information is destroyed after two years.*
3. *3 years*
4. *7 years*
5. *Database contains name and dates only and is kept indefinitely*
6. *We can only deactivate*
7. *We are not there yet*
8. *No one has ever requested it, but we would do it immediately*
9. *NA*
10. *NA*

Just over two thirds (67.1 per cent) of respondents were unsure whether, if the organization has requested that a record be purged, the electronic database or case management system provides notification to the organization once the record is purged. Just under a quarter (22.9 per cent) said it does not (figure 18).

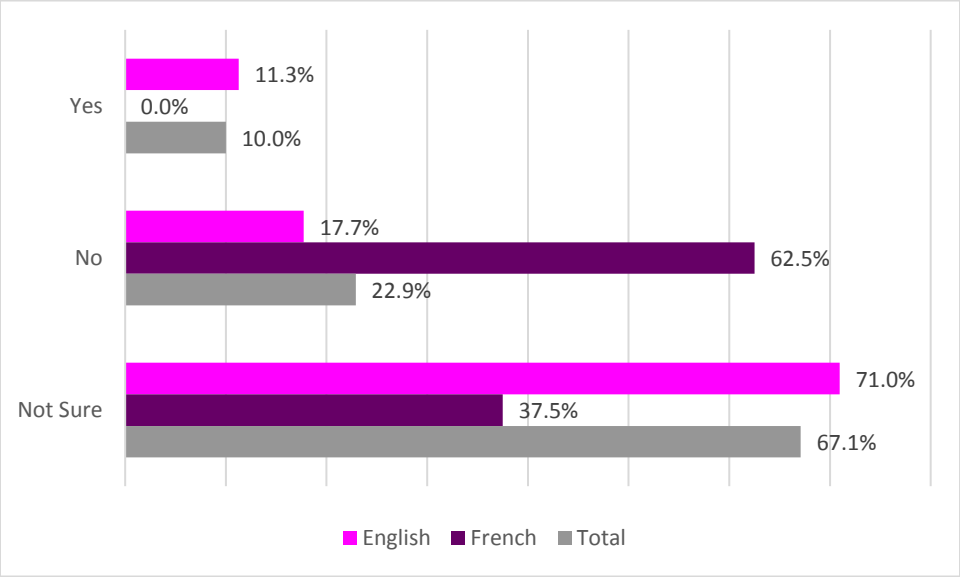

Figure 18: If the organization has requested that record be purged, does the electronic database or case management system provide notice to the organization once the record is purged? (n=70; 62 Eng and 2 Fr).

Just under half of respondents (45.1 per cent) said their organization does not have a policy or protocol requiring notification to a client if there is a breach of their electronic database or case management record. 39.4 per cent were unsure, and the remaining 15.5 per cent said it does (figure 19).

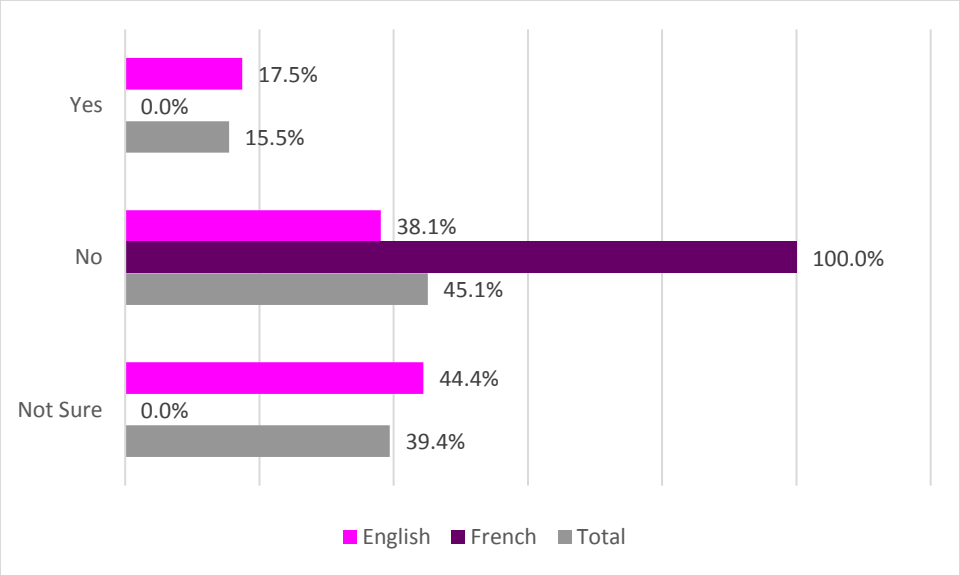

Figure 19: Does your organization have a policy or protocol requiring notification to a client if there is a breach of their electronic database or case management record? (n=71; 63 Eng and 8 Fr).

Positive Outcomes that Result from Using an Electronic Database or Case Management System

Respondents were asked what the positive outcomes that result from using an electronic database or case management system are. Sixty-two people left comments (appendix 3), of which over half related to ***increased efficiency***:

Statistics are calculated by the system, making manual stats no longer necessary. All notes are legible and organized. Saves staff time.

Faster data entry control and record keeping - can create import diary dates and flags.

Easily searchable, particularly for emergency contacts (which would normally only be available in the paper file). Assists in keeping track of file closure/archive dates. …Previously we would start each client from the beginning of the DV counselling process, now we can easily track what counselling topics have been provided and after the crisis management stage the shelter can pick up where they left off (after a review of course). This is producing positive comments from clients and staff are feeling more productive. Another benefit has been the follow up process, we know clients have better outcomes if they retained contact with the shelter upon being discharged after the 30 days but we didn't have a reliable mechanism to maintain contact and service provided. Staff are finding it quicker to use the computer then having to write everything out, at least those who can type. Additionally, what paper files are kept are now small so some shelters have been able to reduce storage space which is a huge bonus and staff mentioned that it's a relief not to always be searching for a file or a lost document. Staff also mentioned that it was much easier and less time consuming when preparing for court as all the data was available and easy to find using the database…

Increased efficiency was partly attributed to ***improved access to information***, including quick access, remote access, all staff being able to access information, and being more easily able to locate specific information:

All staff can access the files from their desk, write notes and read notes.

Less time spent documenting, easier to locate specific information quickly, easier to document specific information in a standard way, easier to look back at past stays to provide documentation that enables women to access services and benefits.

Able to access client info quickly through SV, helpful for safety reasons.

Professionalization of record keeping and standardization of record keeping practices. Time savings. Ease of finding client file, whether current or historical.

It was also attributed to ***more consistency and accuracy in record keeping and reporting procedures:***

Efficient record keeping, allowing for accurate reporting.

Accuracy, time saving for month end stats for funder, less paper, smaller files easier for limited storage space.

Ease of record keeping, environmentally friendly (paperless), accessing info is quicker and less prone to error.

Accuracy was felt to be improved due to ***clearer and more legible case notes, ease of gathering statistics,*** **and** ***consistency in information gathering:***

More clear case notes and easier access to information. More accurate stats collection.

Documentation is legible and easy to read by anyone who needs to access the file information. Data and statistical information is easily accessible when required applying and reporting to funders etc.

Mandatory information is not missed as unable to proceed until filled in. Time savvy, errors easily fixed.

Legible notes - time stamped notes - inability of staff to edit or change notes after a week – consistency.

A separate theme to emerge was that having an electronic database or case management system enabled ***more consistent client support,*** by making it easier to ***share information between staff in the organization:***

Ease of access. History of client kept. Connected to police system easy access to historical information accessible by all of unit for team approach to service delivery.

HIFIS: easier for information sharing among workers and case management; multiple people assisting one client can access same information.

Ease of communication and consistent client support.

Case notes are in order and easier to read than hand written notes. With HIFIS we can share information between departments - so for individuals beginning work in outreach, their file can be accessed by the new support worker and provide more continuity of service. Our community is in the process of building a shared database to better serve folks in the community facing all kinds of homelessness.

Some felt this is beneficial for clients as it means they do not have to repeatedly tell different staff about difficult experiences:

> *Access to information across all programs - minimizing trauma to clients by asking questions only once…*
>
> *Allows workers in other programs to assist the client without having to make the client go through duplicated paperwork. It also completes the whole picture of services needed through our organization to help give the client better assistance.*

Improved consistency in client support was also attributed to being able to ***track client's journeys,*** both by being able to access historical information and transfer information forward:

> *Keep tracks, statistics, updates on client's journey.*
>
> *…ability to quickly and efficiently match up clients to past program use, and include their children and the children's program use. Ease of record keeping for staff and ability to report better to funders.*
>
> *More secure control over personal information (as opposed to paper records) and ability to share files with different VS programs if the client moves to another town.*
>
> *Makes record keeping more efficient. Are able to transfer clients to another region if needed. All documents kept together.*

Some also added that this helps them to ***provide more tailored services to clients***:

Easy access to prior recent records - allowing workers to tailor the program/services to the woman's need - and an opportunity to deal with possible difficulties in communal living that may occur.

Lessens the amount of information we are keeping about clients. Lessens the amount of paper records on hand and the need to find safe storage. Allows us to print reports to help shape our program to meet the needs of the women and children we serve.

Justification of our grants -Statistics taken from the databases of the houses allowing a better awareness / activism of our group - More understanding the profile of the women using our services to improve them and to adapt them to the specific needs of the latter.

Another positive outcome associated with the use of an electronic database or case management system was that it enables ***safer storage of information,*** both in terms of ***physical safety*** and ***data protection security:***

Data compilation is simple and available immediately, if paper files are damaged or lost (i.e. in a fire) we still have the data stored electronically.

Consistency of information gathered and stored, peace of mind that if there were a fire or other such incident, we have backup e-files and not just paper…

Files are able to be secured so that only workers who need to access the file are able to. This guarantees confidentiality of the client.

Records are in a highly guarded RCMP program and no paper copies of any records are kept - so unless you have given permissions to see other files they are not accessible to anyone.

…As we are connected to a secure database there are extra measures in place to ensure that clients information is safe.

Respondents also appreciated that using an electronic database is ***greener*** and ***increases physical storage space***:

Accuracy, time saving for month end stats for funder, less paper, smaller files easier for limited storage space.

…Lessens the amount of paper records on hand and the need to find safe storage…

Quick, efficient, easily legible, can store a lot of information without using a lot of physical space, ease of access.

Facilitates writing, reading No waste of paper (greener) Facilitates data collection, cross-tabulation, multi-year comparison etc.

Speed and fewer papers to keep.

Finally, some felt that using an electronic database or case management system ***increases staff accountability:***

Managers and staff can review what work they have done with a client or throughout a specific time frame. Some staff don't like that but it has helped to weed out staff who were not doing the work. Management often didn't have time to find and review all the paper files to monitor.

Provides accountability for the caseworker to ensure service provided is client centered and steps are not missed. Files are QA on a regular basis to ensure Client is receiving all the support they may need.

Improved staff communication and accountability.

It keeps all staff members accountable because only the individual staff member can make log notes under their name. Less chance of records being forged or edited.

Negative Outcomes that Result from Using an Electronic Database or Case Management System

Respondents were asked what the negative outcomes that result from using and electronic database or case management system are. Fifty-nine people left comments (appendix 4). An overarching theme of ***lack of control*** emerged here***:***

> *Women's information is entered into a database that we have no control over.*
>
> *Lack of control, employees can access the system off site.*
>
> *Worries about breaches of privacy; controlling access to records.*

This included a lack of control in relation to the ***risk of a privacy breach:***

> *Always the concern of a privacy breach. We currently use a laptop that is password protected, does not leave the office and is locked in a cabinet when not in use. We are exploring further the idea of using the system for case management but want to be sure we understand and can mitigate the risks.*
>
> *If not secured or encrypted can be hacked or corrupted, ensuring confidentiality.*
>
> *We still have paper as we don't trust some documents on the computer.*
>
> *My worry would be that it's cloud based...*
>
> *Files are never deleted or could be hacked into.*
>
> *Occasionally technology issues and breakdowns, and uncertainty of ability to protect women and their information…*

A few people mentioned concerns around privacy in relation to ***misuse of information*** by staff:

> *Although staff aren't supposed to, some access information about clients at our adult-only shelter.*
>
> *Our organization has a policy that client information is only accessed on a need to know basis. Therefore, it is more difficult for management to monitor when staff who should not be accessing this information do so.*
>
> *Concern that information is inappropriately accessed.*

There was also concern around a lack of control in relation to ***loss of data***:

> *Risk of data loss (deletion).*
>
> *Loss of data per bug or human error.*
>
> *System crash stops our record keeping/potential for loss if system fails and or if security is broken.*

And a lack of control due to ***limited understanding:***

> *Obviously I don't know much about the security of the database, and many other staff probably don't either. We don't understand the implications of an online system. If we don't, the clients probably don't either.*
>
> *Difficult to maintain as we have no IT person…. We also aren't using WISH to its full capacity.*

The next most common negative outcome identified was ***technical issues resulting in inability to access records***:

> *If internet down, unable to access system. Glitches causing the program to not work properly, i.e. book appointments for outreach.*
>
> *If we can not access the electronic files for some reason - we have no way of updating or referring to reports.*
>
> *If repairs or upgrades are being done it interferes with your work day.*
>
> *…power outage leaves you stranded.*

The ***time and cost of training staff*** on how to use the database was also mentioned here:

> *Constant retraining required to insure consistency in the way data is entered, concern that information is inappropriately accessed.*
>
> *Some staff are not versed in using electronic databases.*
>
> *…Also training for staff and lack of consistency across the sector.*
>
> *Access by unauthorized persons - Employees who do not master the electronics adapts very hard - several training and reminders needed.*

Other concerns mentioned here included ***gathering data that does not always feel relevant/lack of flexibility around data collection***:

Our system doesn't allow us to lock workers out of certain files and we would prefer that it did. Our system doesn't allow us to collect all of the data we want to.

Too much information can be shared that is not relevant to the services provided.

HIFIS: some fields (e.g. rent subsidies) must be entered into multiple locations, can be confusing; all clients must be entered into system, even if they want to remain anonymous; concern over client privacy and confidentiality with greater sharing to ESDC. BC Housing Connections: not user-friendly; seems redundant alongside existing intake procedures; seems more useful to BC Housing than to organization. Overall, funder requirements to use specific databases limits organization control over protection of privacy and confidentiality of clients, as well as client autonomy over who they want to give their information to.

Not all forms are in the database.

Inconsistency and errors in data entry were also mentioned:

Entry errors. Inconsistent data entry.

Dat[a] entry not always consistent between shelters, different levels of usage.

Unable to edit mistakes such as misspellings or incorrect information in the case notes.

Nine people reported that they were not aware of any negative outcomes resulting form using an electronic database or case management system.

Final Comments from Respondents

Respondents were asked to leave any final thoughts or comments before completing the survey. Fourteen people left the following comments, which illustrate the need for further development of the process of implementing and maintaining electronic databases and client case management systems in this sector:

1. *I think this is important information to discuss and continue to develop processes around, i.e. policy around confidentiality breaches, etc.*
2. *The issue of data or information management is a huge one for our organization. We struggle to find the balance of protecting and honoring the stories and information women and children put in our care with providing funders and the community with data that is useful and necessary to improve and protect our program. Decisions were not made quickly or lightly for us to move to using HIFIS, we continue to debate at our staff, and board tables how we can best use the system in our workplace.*
3. *Using the system makes it difficult to correct information. We also don't like that the vendor has access, but recognize that he must in order to make back-end changes when MCSS requests a different statistic to be collected, and they make frequent changes to the information they are seeking!*
4. *Since we are still in the process of developing our electronic database process, I will be very interested in the outcomes of this survey.*
5. *Non-profits need additional funding in order to implement highly secure e-databases.*
6. *I feel like doing this survey means I've added several things to my to do list!*
7. *Generally speaking, the move to an electronic database has been a positive experience.*
8. *In 40 years, our Centre has had records subpoenaed less than a handful of times, so not a risk that required a lot of weight in our decision to go digital; however, file notes are careful and kept on paper copy, which mitigates some risk.*
9. *Some of the questions were difficult to answer because we collect only the basics in the HIFIS database. We do not enter any case notes etc. and collect information under broad categories.*
10. *Our office has recently gone back to all paper files.*
11. *Thanks for researching this. It is a needed area to address.*
12. *As a woman's transition house we should not be accredited and we are not because those standards increase the safety [risks] for women as they collect too much personal information and storing is dangerous if it is subpoenaed by the court*
13. *A consistent, mandated database/case management system that contains all our provincial programs would be amazing and well used.*

14. *Hard to answer if we have several databases. From question 12 I answered based on our database of houses and not the system of the Federation of Transition Houses*

DISCUSSION

There is no argument that electronic databases can help streamline the record keeping process and help to ensure the consistency of data collection when databases are customized from a privacy by design perspective. However, using a database that is designed with the objective of maintaining the privacy of women, children and youth, to the best of the vendor's ability, means that anti-violence organizations must work collaboratively with their chosen database vendor to ensure compliance with provincial, territorial, and/or federal privacy laws. Privacy laws such as PIPA and PIPEDA can provide anti-violence programs with a database customization framework.

Before implementing a database or making changes to an organization's current one (as most vendors allow), it is recommended that organizations:

- develop policies and training for their Board, staff, work placement students and volunteers about the collection of and storage of personal information of service recipients;
- work collaboratively with vendors to customize and delete data fields to those only necessary to provide the service that the recipient has consented to;
- have a permanent deletion of records plan in place, and;
- have a system for workers to enter service recipient's data anonymously.

Based on the findings from the survey, the following discussion will highlight important considerations of organizations related to database use and safety and security of data. For a comprehensive review of the important privacy and security considerations and recommendations of electronic database use see BCSTH's "Privacy, Security and Confidentiality: Database Considerations for Canadian Anti-Violence Organizations" https://bcsth.ca/projects/technology-safety/

Considerations for the Collection and Electronic Storage of Personal Information

As shared in the survey findings, just over half (51%) of the respondent's report using an electronic database. Respondents report that the risks to service recipient's privacy via the collection and electronic storing of personal information goes beyond electronic databases (e.g. the use of an Excel spreadsheet as their database). Some respondents report that though their organization does not have

an electronic database - case notes, names and contact information of service recipients are written in software applications, like Word or Excel, and saved to a cloud based storage system. While cloud storage is an affordable storage solution for underfunded anti-violence programs, there are many privacy implications agencies must consider prior to use. The Office of the Information and Privacy Commissioner of BC says:

> *"Organizations must ensure they fully understand their obligations under Canada's private sector privacy legislation, including those under certain provincial privacy legislation, and they need to carefully assess the risks against the benefits. Organizations considering a cloud computing service should carefully consider what information will be stored in the cloud and why. Organizations must consider the sensitivity of the personal information and carefully assess all the risks and implications involved in outsourcing personal data to the cloud. This assessment should also take into account whether the cloud is a public cloud, community cloud, private cloud or hybrid cloud, as defined in the OPC's Introduction to Cloud Computing."*[4]

The above statement holds true whether an organization is storing their documents in a cloud storage facility, their database is stored on the organization's cloud based server, or the electronic database is accessible through the cloud hosted by the database vendor.

In addition to the considerations above, organizations must also know what country the cloud storage facility is located. Just over half of respondents (51%) said that they did not know what country their cloud storage facility is located in. Though Canadian privacy laws do not prohibit what country an organization's cloud based storage facility is in, privacy commissioners warn that the privacy laws of the country that the cloud storage is located is the one that applies to the Canadian organization.[5] For example, if your organization's data is stored in a cloud storage facility in Mexico, any legal action for a data breach would most likely take place in Mexico. In addition, Mexico's privacy laws pertaining to data collection storage and destruction would likely apply and your organization may have to travel to Mexico for all legal proceedings. Most vendors standby the safety of the cloud storage facility they use. However, it is important to ask where your data is being stored before licencing a database product and consider the implications if the data is stored outside of Canada.

---

[4] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia. Cloud Computing For Small- And Medium-Sized Enterprises. Retrieved from: https://www.oipc.bc.ca/guidance-documents/1437

[5] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia. Cloud Computing For Small- And Medium-Sized Enterprises. Retrieved from: https://www.oipc.bc.ca/guidance-documents/1437

Another privacy implication of storing personal information in a cloud storage facility is not knowing who has access and control of your agency's data. The Office of the Privacy Commissioner warns, "while cloud computing may not increase the risk that personal information will be misused or improperly exposed, it could increase the *scale* of exposure. The aggregation of data in a cloud provider can make that data very attractive to cybercriminals, for example. Moreover, given how inexpensive it is to keep data in the cloud, there may be a tendency to retain it indefinitely, thereby increasing the risk of breaches.[6]

Barriers to Implementing an Electronic Database

While just under half of the respondents report that they do not currently use databases in their programs, many programs are interested in learning more about them. Twenty-six percent of respondents report that their organization is considering purchasing an electronic database and 23.4% are not sure if their organizations are going to use an electronic database in the future. Respondents reported the same primary reasons for their organization not purchasing a database. Having adequate funds to implement all aspects of an electronic database is the top reason anti-violence programs do not have databases. These reasons all appear to be reflect how underfunded anti-violence programs across Canada are. Respondents report the following reasons for not being able to purchase a database:

- Not having the funds for the initial purchase of the database
- Not having the funds for hiring Information Technology (IT) companies, and
- Not having time to train staff.

When developing a plan to purchase a database, BCSTH encourages organizations to consider the following in their implementation plan:

- Time to write policies about database use
- Funding for a professional external IT audit to ensure the IT infrastructure is secure
- Funds to implement recommendations of the IT audit
- Training of new employees about record keeping, privacy legislation and the database system
- Plan and funds for annual licensing fees and upgrades
- Plan for renewal of IT infrastructure software.

[6] Office of the Privacy Commissioner of Canada. (2011). Frequently asked questions about cloud computing. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/02_05_d_51_cc_faq/

Risks of Free Databases

Given the funding and resource issues faced by anti-violence programs across the country, having access to a free database is understandably appealing. However, there are increased concerns about the privacy of women, children and youth's personal information when databases are low cost or free that need to be considered. Nine survey respondents report using the Government of Canada's free electronic database: the Homeless Individuals and Families Information System (HIFIS). This database is free for shelters and transition houses to use. However, respondent's report being concerned about its privacy implications because people's personal information is collected by the Government of Canada in exchange for the free database software.

Upon further analysis, it appears that the privacy concerns with HIFIS stem from two different sources:

- HIFIS capabilities, and;
- Organization/funder policies and practices.

HIFIS software has the capability to be used by one shelter or by many shelters in a community/region. This allows data to be shared with other databases in a shared cluster. From a safety and privacy perspective, there are a number of risks when funders and anti-violence organizations have their organization's data comingled with other organizations through these networks of databases. The personal information of women, children and youth experiencing violence should not be able to be accessed by staff of external agencies. This increases the ability for personal information to be accessed by multiple people and puts the safety and privacy of women, children and youth at risk.

In addition to not sharing personal information through a network of databases, it is recommended that funders and organizations also develop a policy and practice to allow for service recipients to be entered into HIFIS and all databases anonymously. HIFIS and most commercial databases allow for service recipients to be entered anonymously, and it is the funder or organization's policy and practice that dictate for mandatory personal information to be entered and collected which puts women, children and youth's privacy at risk.

The HIFIS database itself can be customizable; however, there are 38 mandatory data fields. The Government of Canada states that only aggregated data is collected from the data entries and that each person entered is assigned an anonymous ID. However, the sophistication of the HIFIS allows the ID of a person to be tracked across the country even if their name is anonymized. Another interesting privacy issue is that the data of service recipients are encrypted in transit but there is no clear answer about who holds the data encryption key. It is imperative that anti-violence programs using HIFIS receive informed consent from women, children and youth when storing their personal information in HIFIS, as

well as provide service recipients with a choice about whether their information (aggregated or not) is shared with the Government of Canada. In compliance with privacy laws, anti-violence programs must ensure that the personal information of service recipients can be redacted and permanently deleted from HIFIS.

It is recommended that anti-violence programs carefully determine what data fields should be included on their program's database by considering what fields are necessary to provide service. It is important that anti-violence programs take the time to customize their database in order to protect the privacy of service recipients.

"HIFIS…all clients must be entered into system, even if they want to remain anonymous; concern over client privacy and confidentiality with greater sharing to ESDC. Overall, funder requirements to use specific databases limits organization control over protection of privacy and confidentiality of clients, as well as client autonomy over who they want to give their information to."- Survey respondent

"Decisions were not made quickly or lightly for us to move to using HIFIS and we continue to debate at our staff and board tables how we can best use the system in our workplace." – Survey respondent

*Note: The HIFIS team were invited to complete the BCSTH's Database Questionnaire but did not respond to the invitation. Information about HIFIS in this report is based on information found on the HIFIS website, participation in a HIFIS demonstration through BC Housing and survey respondents' feedback about HIFIS. We were unfortunately unable to speak with anyone at the HIFIS team directly to get answers to our questions.

Policy Development and Training

Respondents report being concerned about two things: theft of data and the unauthorized use of data by those who have authorized access to an organization's electronic database. Based on the survey results, respondents are more concerned about staff accessing information about service recipients than theft of personal information. Working collaboratively with database vendors to customize a database, assigning appropriate access levels to each user, and developing policy and training for staff and

volunteers about their privacy and confidentiality obligations and database use can help mitigate an internal privacy breach.

Before implementing a database, it is recommended that organizations develop policies about the use of databases that reflect privacy legislation and the safety needs of service recipients.[7] Suggested policies include:

- User agreements
- Confidentiality
- Informed consent
- Revocation of consent
- Unauthorized use of data
- Storage of personal information
- Destruction of personal information
- Data breach plan
- Updates and renewal
- Subpoena of records
- Training
- What devices the database can be accessed on

As previously mentioned, respondents reported that a barrier to having a database is not having enough resources to train staff and volunteers about how to use the database. They also reported that they were not aware of the capabilities of their electronic database. In addition to training about how to use the database, it is essential that anti-violence organizations considering implementing a database train staff and volunteers about the applicable privacy laws; specifically how to comply with legislation about the collection, storage and destruction of women, children and youth's personal information. It is recommended that training also include information about the organization's database use policies as well as recording personal information and case management notes into the database that maintains confidentiality and nonjudgement.

[7] BCSTH published "PEACE Program Use of Technology Template Guide" in 2019. For sample database policies see BCSTH website https://bcsth.ca/projects/technology-safety/

Information Technology Infrastructure

Respondents report they are concerned about the potential of a data breach and the lack of control over personal information once entered into a database. Whether an organization considers a server or web hosted database, it is important that organization's plan for the time and costs associated with ensuring their IT infrastructure is up to date with the best security protections available. Having an external IT company perform an IT audit of your organization's infrastructure is best practice before storing personal information into an electronic database. It is recommended that organizations consider:

- server protection
- firewalls
- equipment capacity
- anti-virus and anti-malware programs
- network database access
- wireless access and connectivity
- other requirements the database product may need

Budgets must include funds to purchase the initial software and equipment needed and organizations must also plan for funds to be allocated for license renewal and upgrades.

Informed Consent

The OPC states, "under privacy laws, organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information.[8]"

However, forty percent of respondents reported that their organizations ask for informed consent from women, children and youth before collecting personal information and storing it in an electronic database. Fifty-one percent report that service recipients cannot opt out of the database once consent is given. Thirty-six percent of respondents say that service recipients can change their mind and be deleted from the database once their data has been inputted into the database.

[8] Office of the Privacy Commissioner of Canada. (2018). Guidelines for Obtaining Meaningful Consent. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

Informed consent is "an ongoing process that changes as circumstances change; organizations should not rely on a static moment in time but rather treat consent as a dynamic and interactive process.[9]" Organizations using an electronic database must comply with provincial/territorial or federal privacy laws and have policies and practices for informed consent and the revocation of consent. It is recommended that organizations include the following in their informed consent policy and practice:

- inform service recipients about the transfer from paper files to storing personal information in an electronic database;
- inform service recipients about the risks to their personal information;
- inform service recipients about where their personal information is stored and who has access to it;
- provide service recipients with the option to consent to having their information inputted into a database;
- develop a policy about the ability for service recipients to revoke their consent at any time;
- inform service recipients that they can revoke having their personal information inputted into a database at anytime;
- inform service recipients when their personal information will be permanently deleted from the database and any (cloud) servers hosting their personal information; and
- work with the database vendor to ensure personal information can be permanently deleted with no ability to be restored when record keeping obligations are met or when a service recipient revokes their consent.

** While some programs attached to the RCMP may not be able to delete personal information once it is entered, this does not account for all respondents. The majority of commercial database vendors report that records can be permanently deleted.

[9] Office of the Privacy Commissioner of Canada. (2018). Guidelines for Obtaining Meaningful Consent. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

RECOMMENDATIONS

Anti-violence programs across Canada are faced with ongoing funding and resource issues. While programs express interest in utilizing an electronic database to streamline their record keeping process, not having access to adequate, annual funding prevents anti-violence organizations from being able to choose a database with the best privacy and security features to collect and store the personal information of women, children and youth experiencing violence. In order for organizations to have a privacy informed database, adequate funding must extend beyond the actual database product itself.

We believe that in order for anti-violence organizations to successfully implement and maintain a privacy centred informed electronic database, funders and accreditors that require their use must provide financial support for:

- training staff about privacy legislation, informed consent and database use;
- human resources to develop privacy centred and legal compliance policies;
- consulting fees for an external IT audit, and;
- funds to upgrade IT infrastructure to make it as secure as possible.

It is also recommended that funders and accreditors provide guidelines for a minimum level of IT security infrastructure with concrete requirements for IT security and software before approving or requiring the use of databases for anti-violence programs.

Anti-violence programs, database vendors, funders and private companies would benefit from wider distribution of the helpful privacy resources that are currently available. The OPCC, OIPC BC and OIPC AB have many accessible resources that can guide non-profit and for profit anti-violence programs to comply with provincial privacy legislation, the Privacy Act or PIPEDA. Resources about data breaches and cloud computing are also available and would be helpful resources for anti-violence programs exploring the implementation of databases. The development of database policy guidelines for anti-violence programs would be a worthwhile knowledge transfer resource that would be useful for programs across Canada.

For more information about choosing the right database, please see BCSTH's "Privacy, Security and Confidentiality: Database Considerations for Canadian Anti-Violence Organizations" here https://bcsth.ca/projects/technology-safety/

RESOURCES FOR ANTI-VIOLENCE PROGRAMS

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

Privacy Act:

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/

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 programs:

Selecting a Database:

https://nnedv.org/mdocs-posts/selecting-a-database/ or https://www.techsafety.org/selecting-a-database/

APPENDICES

Appendix 1: What type of anti-violence organization are you responding to this survey on behalf of?

181 people responded to this multiple-choice question, of whom 12 selected 'other' and provided the following comments:

1. *Multi-service agency provided shelter, outreach, children exposed to violence programming, prevention education, child care, foster care*
2. *Our organization has nearly all of the above except police based*
3. *Women's Shelter/Transition House Program, Second Stage Housing Program, Children and Youth Exposed to Violence Program, Sexual Assault/Violence Program and Court/Legal Advocate Program*
4. *and second stage, crisis line*
5. *CBVS, STV, MCS, PEACE*
6. *VAW/anti-violence coalition, coordinating committee*
7. *Family violence protection program*
8. *Children's Access Agency*
9. *STV Counselling*
10. *Shelter for abused and troubled young women*
11. *VAW Counsellor*
12. *Outreach Worker*

Appendix 2: How does your organization currently practice record keeping?

183 respondents answered this question, of whom 28 did not select any of the multiple choice options (The names and other personally identifiable information are kept in an electronic database but case notes or notes are kept as paper files; The names and other personally identifiable information and case notes are kept in an electronic database or case management system; The organization keeps only paper files and does not have an electronic database or case management system) and instead selected other and left the following comments:

1. *Primarily, we use software like Microsoft Excel and case notes are often saved in Word files. Save on a cloud service.*
2. *We do not have an electronic database or case management system. We keep electronic case notes or notes electronically in Word, and paper files.*
3. *We use basic Excel spreadsheets with very minimal contact information only. Other details are kept on paper.*
4. *Names/personally identifiable information and case notes are kept in electronic database; paper file contains printed notes, all client's consents and sometimes artwork for children.*
5. *We keep paper and electronic records, but do not take notes.*
6. *Names and personally identifiable information are kept only as paper files; basic non-identifying information is kept electronically.*
7. *We use a combination of electronic and paper forms. We do most case notes electronically, but often print off notes to ensure we have a paper copy as well.*
8. *Combination- we are only using our WISH database at a minimum but will be using it more [for] case notes. We have a client-running log that is not a counselling record plus paper files for each counselling session/contact. We also have the original inventory log of names, sins, date of admission in an Outlook file, not shared on any network.*
9. *The names and other personally identifiable information and case notes are kept digitally but separately. Case notes refer to a client number stored in a separate spreadsheet. Paper files have notes and limited personally identifiable information.*
10. *Paper file (contact information, birthdate, children's names, health information, name of the abuser, medical needs, questionnaire about what brought them to the shelter, consent forms, copies of ID, goals, appointment log, referral forms, copy of safety plan, injuries, valuables and medication). We also use WSIS, an electronic web-based program, provided by the Ministry of Justice.*

11. *We have paper client files....at times we write letters of support for clients for things like housing, these letters are stored on our computer, the letters have client names in them and may identify names of children at times.*
12. *Combination of paper files and files on secured computers.*
13. *Full paper file, some data electronic version also.*
14. *Notes and personal data are stored electronically, but are also printed in a paper file.*
15. *All files are entered into our electronic database, however only certain staff have access, other staff/volunteers record notes on a paper file that is then eventually destroyed once the info is logged electronically.*
16. *The case notes are kept as papers during the accommodation; they are destroyed upon their departure. However, statistical data are kept electronically.*
17. *Paper files and electronic database without mention of names.*
18. *We keep paper files, but do notes on the computer and print them out.*
19. *The case notes and the personal data are written on the computer and then printed out and put in a paper file.*
20. *We keep the paper files. Little information is included in our paper files. No electronic data.*
21. *We keep only non-nominal data.*
22. *We keep only the name of the service date and the phone number. In some cases, we have some words that detail a particular problem.*
23. *Only information for R.P statistics.*
24. *Personal data is stored in an electronic database for statistical purposes but without names and without case notes*.
25. *We are in the process of moving to a fully electronic system but still have some paper files.*
26. *Working on setup of an electronic database this year.*
27. *Counselling program is separate from shelter and has moved to electronic files only.*
28. *Last option, we don't take notes for individual files though.*

Appendix 3: Is a client's record and data purged immediately from the electronic database or case management system as a routine practice as soon as the organization determines the record can be destroyed?

81 respondents answered this question, of whom 25 said yes, 27 were unsure and 29 said No. Those who answered no, were asked to describe their organization's approach to the destruction of records. Comments were as follows:

1. *Paper records are destroyed every 5 years.*
2. *Shredding every 5 years.*
3. *Keeping the paper file for 5 years under lock and key.*
4. *Paper files are required to be kept for 6 years as per Government of Alberta's funding agreement*
5. *Records can be destroyed after five years. The organization is not yet 5 years' old.*
6. *After 7 years, I think?*
7. *7 years.*
8. *Every 7 years*
9. *We have not used this long enough. All files are less than 7 years old.*
10. *Currently we retain paper files for 10 years, so we pull those and shred them annually. We have not reached the 10-year mark yet with our current record management database. Management is planning on putting a process in place.*
11. *We have yet to deal with this systemically as we have not used the system long enough to reach any time limits.*
12. *We don't have a records destruction policy or protocol... it's on my list of things to look at*
13. *We must maintain records for a minimum of 1 year but haven't developed an electronic records policy in this regard. At the moment we are maintaining all records.*
14. *We shred them in house, if necessary but many clients are long-term.*
15. *We keep minimal information indefinitely, but destroy paper files after 10 years or once the oldest child reaches age of majority.*
16. *Paper copies are destroyed at 6 years - database information is not destroyed.*
17. *The HIFIS database only allows us to deactivate a client not delete the record. Paper files are not destroyed.*
18. *Paper records are eliminated once per year - database remains with names only.*
19. *Only paper files are destroyed. Manitoba has a very high rate of re-utilization and multi-generational women accessing the shelters. We are obviously missing something in our process to help the client leave abusive relationships and recognize potentially abusive relationships in the*

future we needed to understand the client better. Providing safe temporary shelter with minimal counselling isn't working. The database's purpose is to track the clients progress (or not) to provide better service to the client. Since we have only used a database within the last few years we haven't gotten to the point of needing to purge records and at this point it would defeat the purpose of a database. Clients who do not wish to be identified are entered into the database as anonymous and those records will be purged eventually but our funder would like to have 3 and 5-year progress reports we are still working on a policy. Our thoughts are that the client files are very much like the medical records and that data needs to be retained.

20. *We haven't destroyed any of our records.*
21. *We maintain all client records.*
22. *We do not destroy client records.*
23. *We do not destroy records.*
24. *Paper files are purged, all legal documents and signed documents are kept on file and stored in closed files.*
25. *For the paper files - records are to be kept under double lock for at least 7 years after services cease. I am unsure on the Ministry of Justice (SK) regulations on the electronic records.*
26. *Shredding.*
27. *We implement specified practices as per our policies.*

Appendix 4: Positive outcomes that result from using an electronic database or case management system

1. *All participants are tracked at an agency level.*
2. *Quick, efficient, easily legible, can store a lot of information without using a lot of physical space, ease of access*
3. *Efficient record keeping, allowing for accurate reporting*
4. *Keep tracks, statistics, updates on client's journey*
5. *Ease of access, history of client kept, connected to police system easy access to historical information accessible by all of unit for team approach to service delivery*
6. *Quick access to information; remote access to information; stored safely; less paperwork*
7. *Ease of reference*
8. *Lessens the amount of information we are keeping about clients. Lessens the amount of paper records on hand and the need to find safe storage. Allows us to print reports to help shape our program to meet the needs of the women and children we serve.*
9. *More clear case notes and easier access to information. More accurate stats collection.*
10. *HIFIS: easier for information sharing among workers and case management; multiple people assisting one client can access same information.*
11. *Ease of communication and consistent client support.*
12. *Ability to create accurate reporting and data submissions, quick access and destruction of information, shared information between staff of organization*
13. *Data compilation is simple and available immediately, if paper files are damaged or lost (i.e. in a fire) we still have the data stored electronically*
14. *Allows workers in other programs to assist the client without having to make the client go through duplicated paperwork. It also completes the whole picture of services needed through our organization to help give the client better assistance.*
15. *Statistics are easier to gather for reporting purposes. It does not benefit clients in any way.*
16. *All staff can access the files from their desk, write notes and read notes.*
17. *What we have noticed so far it that clients who are attempting to use the shelters for free accommodation during a shopping trip (for example) have decreased considerably. On a more positive note we are now able to pick up with a client where they left off in their counselling process. Previously we would start each client from the beginning of the DV counselling process, now we can easily track what counselling topics have been provided and after the crisis management stage the shelter can pick up where they left off (after a review of course). This is producing positive comments from clients and staff are feeling more productive. Another benefit has been the follow*

up process, we know clients have better outcomes if they retained contact with the shelter upon being discharged after the 30 days but we didn't have a reliable mechanism to maintain contact and service provided. Staff are finding it quicker to use the computer then having to write everything out, at least those who can type. Additionally, what paper files are kept are now small so some shelters have been able to reduce storage space which is a huge bonus and staff mentioned that it's a relief not to always be searching for a file or a lost document. Staff also mentioned that it was much easier and less time consuming when preparing for court as all the data was available and easy to find using the database. Managers and staff can review what work they have done with a client or throughout a specific time frame. Some staff don't like that but it has helped to weed out staff who were not doing the work. Management often didn't have time to find and review all the paper files to monitor.

18. *No data is lost. Easily searchable for employer and employees. Safely secured on a cloud server. Information can be mobile (on laptop) and easily accessible. Mandatory information is not missed as unable to proceed until filled in. Time savvy, errors easily fixed.*
19. *Files are able to be secured so that only workers who need to access the file are able to. This guarantees confidentiality of the client*
20. *Access to related files can provide a background history especially in domestic violence situations. Court information and history is easily accessed and provided to the Client. Provides accountability for the caseworker to ensure service provided is client centered and steps are not missed. Files are QA on a regular basis to ensure Client is receiving all the support they may need. As we are connected to a secure database there are extra measures in place to ensure that client's information is safe.*
21. *Ease of record keeping, environmentally friendly (paperless), accessing info is quicker and less prone to error*
22. *Case notes are in order and easier to read than hand written notes. With HIFIS we can share information between departments - so for individuals beginning work in outreach, their file can be accessed by the new support worker and provide more continuity of service. Our community is in the process of building a shared database to better serve folks in the community facing all kinds of homelessness.*
23. *Accuracy, time saving for month end stats for funder, less paper, smaller files easier for limited storage space.*
24. *Stats are easier to get and manage*
25. *Statistics are calculated by the system, making manual stats no longer necessary. All notes are legible and organized. Saves staff time.*

26. *Less time spent documenting, easier to locate specific information quickly, easier to document specific information in a standard way, easier to look back at past stays to provide documentation that enables women to access services and benefits*
27. *Records are in a highly guarded RCMP program and no paper copies of any records are kept - so unless you have given permissions to see other files they are not accessible to anyone.*
28. *Statistical data Consistent record keeping Improved staff communication and accountability*
29. *More secure control over personal information (as opposed to paper records) and ability to share files with different VS programs if the client moves to another town.*
30. *Professionalization of record keeping and standardization of record keeping practices. Timesavings. Ease of finding client file, whether current or historical.*
31. *Faster data entry control and record keeping -Can create import diary dates and flags*
32. *efficient, better stat keeping*
33. *Makes record keeping more efficient. Are able to transfer clients to another region if needed. All documents kept together.*
34. *Streamlined data entry. Statistics collection and reporting made easier. More legible. Storing attachments on the file is made easier.*
35. *Consistency in record keeping*
36. *I prefer paper*
37. *The client files are accessible to both staff and supervisors when needed. Documentation is legible and easy to read by anyone who needs to access the file information. Data and statistical information is easily accessible when required applying and reporting to funders etc.*
38. *Easily searchable, particularly for emergency contacts (which would normally only be available in the paper file). Assists in keeping track of file closure/archive dates.*
39. *Quick access to client records. Ability to generate reports. Easy to update.*
40. *It should be better than paper files, but we are not using our electronic system the way it should be.*
41. *Easy access to prior recent records - allowing workers to tailor the program/services to the woman's need - and an opportunity to deal with possible difficulties in communal living that may occur*
42. *Helpful for quarterly stats/ ministry requirements*
43. *Coordinated stat collection (not information sharing)*
44. *It provides us with an easy consistent way to provide stats to funders and access information on goods and services provided. It also allows us to see the work in a provincial context.*
45. *Consistent information & record keeping - ensures all vital information is present when a client goes missing and a missing person's report is filed. All women's shelters in Saskatchewan must use it so we are consistent throughout the province. It keeps all staff members accountable because only the*

individual staff member can make log notes under their name. Less chance of records being forged or edited

46. *More secure/easier to read/better organized and reliable as we do file audits more easily. Transporting is replaced with remote access this protects against loss or misplaced information.*
47. *We are able to give women money from the Homelessness Prevention Program and they can avoid eviction or secure housing.*
48. *Quick access*
49. *Not sure*
50. *Ease of use. Ease of gathering statistical information.*
51. *Everything about my client can be seen by me and admin.*
52. *Access to information across all programs - minimizing trauma to clients by asking questions only once - legible notes - time stamped notes - inability of staff to edit or change notes after a week - consistency*
53. *Could more effectively continue service in the event of a fire or flood. speed at which you can find information*
54. *Able to access client info quickly through SV, helpful for safety reasons.*
55. *Consistency of information gathered and stored, peace of mind that if there were a fire or other such incident, we have backup e-files and not just paper, ability to quickly and efficiently match up clients to past program use, and include their children and the children's program use. Ease of record keeping for staff and ability to report better to funders.*
56. *Efficient reports collect data that is specific*
57. *Primary goal: collect statistical data*
58. *Facilitates writing, reading No waste of paper (greener) Facilitates data collection, cross-tabulation, multi-year comparison etc.*
59. *Faster when requesting accommodation; when consulting a file (we do not call a file since it is a rather medical term)*
60. *Speed and fewer papers to keep*
61. *Avoids repetition of information - ensures better follow-up by workers working on various shifts - facilitates the collection of statistics to submit to our funders - more accurate information*
62. *Justification of our grants -Statistics taken from the databases of the houses allowing a better awareness / activism of our group -More understanding the profile of the women using our services to improve them and to adapt them to the specific needs of the latter*

Appendix 5: Negative outcomes that result from using an electronic database or case management system

1. *None of note.*
2. *Obviously I don't know much about the security of the database, and many other staff probably don't either. We don't understand the implications of an online system. If we don't, the clients probably don't either.*
3. *Lack of control, employee can access the system off site*
4. *Not applicable*
5. *Worries about breaches of privacy; controlling access to records,*
6. *Risk of data loss (deletion)*
7. *Always the concern of a privacy breach. We currently use a laptop that is password protected, does not leave the office and is locked in a cabinet when not in use. We are exploring further the idea of using the system for case management but want to be sure we understand and can mitigate the risks.*
8. *Time and cost to train staff members*
9. *HIFIS: some fields (e.g. rent subsidies) must be entered into multiple locations, can be confusing; all clients must be entered into system, even if they want to remain anonymous; concern over client privacy and confidentiality with greater sharing to ESDC. BC Housing Connections: not user-friendly; seems redundant alongside existing intake procedures; seems more useful to BC Housing than to organization. Overall, funder requirements to use specific databases limits organization control over protection of privacy and confidentiality of clients, as well as client autonomy over who they want to give their information to.*
10. *Too much information can be shared that is not relevant to the services provided*
11. *If system or internet is down, handwritten notes are required - more time consuming*
12. *We've not noted any at this time*
13. *If the internet is down or a power outage happens, we don't have access to files and have to complete paper forms until services are restored. This is a very infrequent issue.*

14. *All clients are treated the same. We can block one client's information when there are conflicts of interest between a worker and a client; however, privacy for clients is a concern.*
15. *Older staff found it difficult to switch and to trust the system. It was also hard for staff who have never used a computer and for those who didn't know how to type. So the negative part is that shelters have had a turnover of staff, but that's actually been a benefit in the long run. So far we are not aware of any negative outcomes regarding clients.*
16. *Huge learning curve for some users who are not computer orientated. If internet down, unable to access system. Glitches causing the program to not work properly, i.e. book appointments for outreach.*
17. *Not really sure that when a file is deleted that it is truly deleted*
18. *When the system is down or being worked on, we lose our access to Client information for follow up during that period.*
19. *If not secured or encrypted can be hacked or corrupted, ensuring confidentiality*
20. *Power outages and system fails.*
21. *Harder to review a full file, power outage leaves you stranded*
22. *We still have paper as we don't trust some documents on the computer.*
23. *There really weren't any negative outcomes. Getting all staff proficient with the system took some time, but that was to be expected.*
24. *Difficult to maintain as we have no IT person. Difficulties getting staff into the habit of locking the computer screen when they leave their desk. Still need to maintain some hard copies of things. Challenging adjustment for staff who struggle with change. Some information isn't being recorded accurately, so house manager has to go back manually for quarterly stats reports. Although staff aren't supposed to, some access information about clients at our adult-only shelter. We also aren't using WISH to its full capacity.*
25. *If we can not access the electronic files for some reason - we have no way of updating or referring to reports*
26. *Awkward to find a secure computer in the RCMP detachment in order to input information.*
27. *It takes time to build a database that meets all of the users needs, glitches that take time to sort out. System needs to be upgraded regularly.*

28. *None*
29. *None*
30. *If repairs or upgrades are being done it interferes with your work day.*
31. *Our system doesn't allow us to lock workers out of certain files and we would prefer that it did. Our system doesn't allow us to collect all of the data we want to.*
32. *Time consuming over non electronic*
33. *Far too time consuming*
34. *Our organization has a policy that client information is only accessed on a need to know basis. There for, it is more difficult for management to monitor when staff who should not be accessing this information do so. Working "bugs" in the gathering and reporting of statically information for funders continues to be a challenge.*
35. *Names accessible to anyone working here; however, client case notes and pertinent info are only available to the counsellor in a paper file.*
36. *Entry errors. Inconsistent data entry*
37. *My worry would be that it's cloud based...*
38. *Don't know*
39. *Date entry not always consistent between shelters, different levels of usage.*
40. *Constant retraining required to insure consistency in the way data is entered; Concern that information is inappropriately accessed.*
41. *Unable to edit mistakes such as misspellings or incorrect information in the case notes*
42. *Invasion of privacy*
43. *System crash stops our record keeping/potential for loss if system fails and or if security is broken*
44. *Women's information is entered into a database that we have no control over.*
45. *Data entry*
46. *Files are never deleted or could be hacked into*
47. *Possible privacy breaches. Some staff are not versed in using electronic databases.*

48. *Not all forms are in the data base*
49. *Reliance on a server - training staff on how to use -*
50. *If computer system were down temporarily we would not be able to access files. This has happened but only for 2 hours*
51. *Not aware of any*
52. *Occasionally technology issues and breakdowns, and uncertainty of ability to protect women and their information. Also training for staff and lack of consistency across the sector.*
53. *None known*
54. *Danger of violation*
55. *Loss of data per bug or human error*
56. *None*
57. *Piracy of personal data (residential address, date of birth, health insurance number)"*
58. *Piracy*
59. *Access by unauthorized persons - Employees who do not master the electronics adapts very hard - several training and reminders needed.*

61. *None*

60. *That someone finds them and uses them*