Data Security Checklist to Increase Survivor Safety & Privacy

In this electronic age, we all have heightened data privacy needs. However, survivors of domestic violence, sexual violence, and stalking have even greater security and safety concerns. Any data collection initiative within a shelter or transition house must be carefully planned, implemented, and evaluated regularly – the safety and privacy of survivors depend on it.

Data security includes a range of issues – from preventing unauthorized access to minimizing information collected and shared. Given the complex safety risks in this work, such databases may need to be stored on separate servers with tight security within and between different service providers, to maintain privilege and confidentiality.

This checklist is meant to give shelters and transition houses a starting point in discussing client safety and data security; it is not intended to replace intensive confidentiality and privacy training.

Before You Begin Your Data Collection Initiative

Minimize Data Collected	Minimize what is collected to lessen the safety risks to survivors and your organization's liability. Review the goals of your organization and evaluate your data collection process. • Are there less invasive alternatives to measure outcomes and streamline intake? • How could the data you plan to collect be misused if accessed through legitimate or illegitimate means? • What is the minimum amount of information your organization needs to collect to provide services?

Develop and Implement Clear Policies	• Develop clear policies and procedures that outline privacy practices for handling sensitive data. • Review privacy legislation to ensure your policies comply with the law. • Communicate these policies regularly at orientation and meetings.
	Data security policies should address: • The content of the record, how long it will exist, and who may have access to it • Processes for survivors to opt-out, inspect, withdraw, or correct their data/records • Collection, modification, use, and disclosure procedures for identifiable data • Procedures for the secure disposal of computers or other electronic media that contain identifiable data • Screening, training, and background check processes of individuals who have access to sensitive information • Procedures to protect against unauthorized use and unauthorized access
Conduct Privacy Impact Assessments	Government agencies conduct Privacy Impact Assessments (PIA) to address: • Types of information collected • Purposes for collection • The intended uses of information • Information sharing • Client notification • Information security • Check with the database vendor to see if a PIA has been completed for their product and if it is available for you to review.

Keep Data Separate	Databases with case notes and other sensitive information must be carefully protected. Keep case notes separate to ensure that there is no risk of case notes including other survivors if your organization receives a subpoena for records. For example, abusers may subpoena organizations for their children's records. Consider keeping the data of children and mothers separate to avoid inadvertently providing abusers with information about their exes.
Limit Access Levels	Limit the number of users who are authorized to view the most sensitive information. When determining access levels, your organization must consider safety risks if the data is shared internally within one organization or across many organizations. It is critical to review the privacy laws that stipulate who can access data.

Critical Elements to Include when Designing your Data System

Test Your Security	Hire a trusted and skilled consultant or security firm to test the security of your network and data protection procedures. An outside Security Audit can provide an in-depth analysis of what is weak or missing.
Keep Survivor Data Away from the Internet	The safest way to protect sensitive information is to have separate computers: one for Internet/email and another for all sensitive data if you choose an in-house database located on your servers (rather than a cloud-based product). These separate computers should not be networked together. Firewalls and anti-virus programs are helpful (see below) but can be compromised. When lives are on the line, keep data safe.
Utilize Anti-Virus Software & Firewalls	If you have an office network, use anti-virus or firewall programs. Anti-virus software or hardware firewalls are important security steps for any organization with Internet access.
Use Encryption	Encryption is the conversion of data into a form that cannot be easily understood by unauthorized users. Encryption is not the solution to all security concerns; it is a small piece of a comprehensive security solution. Consider a database product that has end-to-end or zero-knowledge encryption.

Ongoing Maintenance, Audits, and Training

Update Operating Systems	Regularly download all the latest patches and updates for your operating systems.
Use Strong Passwords and Change them Frequently	Password management is a critical part of data security. The use of pet names, birthdays, or words in a dictionary should be prohibited. Passwords should be changed frequently and kept safe; do not keep them under the keyboard or taped to the monitor! A password-activated screensaver for employees with access to sensitive information helps increase data security when they step away from their computers.
Audit for Quality Assurance	This is a process of evaluating the data collected and removing any incorrect information. At a minimum, staff responsible for day-to-day data entry should not be in charge of the audit. Audits should include random samples of information collected about survivors to help assess quality and accuracy, and to identify if inappropriate data is being collected or shared.
Use Skilled Technology Professionals	Most non-profit organizations do not have full-time Information Technology (IT) staff; however, it is imperative that organizations collecting sensitive electronic data have qualified professional technical support. To limit cost, ask similar organizations about their databases, their overall design, and the possibility of contracting to use their database as a starting point.
Seek Ongoing Education	Attend issue-specific trainings or bring a consultant to your organization to speak about data security and survivor safety. With high turnover, it is especially important to offer ongoing training and education to maintain the security of data and the safety of survivors.

To support your development of safe tech use policies, WSC has developed a Use of Technology Policy Template Guide for Women's Shelters and Transition Houses (PDF, in English only).

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource Data Security Checklist to Increase Service User Safety & Privacy.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada | Femmes et Égalité des genres Canada