NNEDV

Data Security Checklist to Increase Victim Safety & Privacy

In this electronic age, we all have heightened data privacy needs. However, victims of domestic violence, sexual violence, and stalking have even greater security and safety concerns. Any data collection initiative within a local program or between several service providers 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.

IMPORTANT NOTE: This checklist is meant to give local programs a starting point in discussing client safety and data security; it is not intended to replace intensive training. Please work with your State Domestic Violence and Sexual Assault Coalition to increase your community's awareness of data security.

Before You Begin Your Data Collection Initiative

❑ **Minimize Data Collected**	Minimize what is collected to lessen the safety risks to victims and your organization's liability. Review the goals of your organization/project 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?
❑ **Develop and Implement Clear Policies**	Develop clear policies and procedures that outline privacy practices for handling sensitive victim data. 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 client identifiable data • Procedures for the secure disposal of computers or other electronic media that contain client identified 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, and information security. The Center for Democracy and Technology offers educational tools for additional information. Please see their website.
❑ **Keep data Separate**	Databases with casenotes and other sensitive information must be carefully protected. It's important to keep a victim advocate's confidential electronic records separate from prosecution databases since defense attorneys may have the right to see prosecutor notes and may attempt to argue that various entities have access to each other's data if the databases are combined or even on the same server. Work with attorneys who specialize in confidentiality and privilege in addition to technology experts. Important Note: If data is shared it should be minimal and should not invade a victim's privacy.

❑ **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 will be shared internally within one organization or across many organizations. It is critical to review the local, state, federal laws that stipulate who can access victim 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. Banks and defense organizations are expected to go to great lengths to protect their data; Victim Service Providers must protect the lives of victims (and their data) to the same levels. An outside Security Audit can provide an in-depth analysis of what is weak or missing.
❑ **Keep victim data away from the Internet**	The safest way to protect sensitive client information is to have separate computers: one for Internet/email and another for all sensitive data. 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, however are not secure enough to adequately protect victim and client-identifiable data.
❑ **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 under the keyboard or taped to the monitor! A password-activated screen-saver for employees with access to sensitive information helps increase data security when they step away from their computers.

❑ **Use Encryption**	Encryption is the conversion of data into a form that cannot be easily understood by unauthorized users. Encryption is not the solution to all security concerns; it is a small piece of a comprehensive security solution. Financial Institutions, the CIA, and the FBI use encryption to protect stored data and data in transit over their networks.

Ongoing Maintenance, Audits, and Training

❑ **Update Operating Systems**	Regularly download all the latest patches and updates for your operating systems.
❑ **Audit for Quality Assurance**	This is a process of evaluating the data collected and removing any incorrect information. At minimum, staff responsible for the day-to-day data entry should not be in charge of the audit. Audits should include random samples of information collected about clients to help assess quality, 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 staff, however, it is imperative that organizations collecting sensitive electronic data have qualified professional technical support. To limit cost, ask organizations that have been used as national models 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 victim safety. With high turnover, it is especially important to offer ongoing training & education to maintain the security of data and the safety of victims.