Client Information Databases & Confidentiality:
A Comprehensive Guide for Service Providers

This document is both an overview of key data and confidentiality concepts, and a guide to the many considerations that must be weighed when selecting a database, which include: purpose, confidentiality, data security, and program capacity (including costs, technology and staffing). This document is intended primarily for community-based victim service programs that are legally obligated under VAWA, FVPSA, and VOCA to maintain confidentiality.

Companions tools, including checklists, comparison forms, and an audio guide are also available to assist with this process. Please see page 11.

Table of Contents *(click to jump to any section)*

Purpose

When preparing to choose a database vendor it is important to be clear on why your program needs a database and how you plan to use it. The purpose of the database will drive most of the design and other decisions. If your program has been using only paper files, why move to an electronic system at this time? If your program has been using an in-house system and is considering a vendor-maintained database on the cloud, why the switch?

Clearly define the specific types of data your funders request or require. Also include the types of data you use for internal planning, programmatic work, and outreach. At each point, step back to consider what information is truly needed in order to provide quality, non-invasive, survivor-centered services. Narrow this list as much as you can, so that you are employing the best practice of collecting as little information as possible. Once you have a clear perspective on what information you need to collect and what reports you will need to complete, it will be easier to see which vendor offers a tool that meets your needs.

If you find that funders or partners are asking for information that's personally identifying, open a dialogue with them about how such data can compromise survivor safety, privacy, and your legal obligations to maintain confidentiality.

Privacy, Confidentiality, & Privilege

Privacy refers to an individual survivor's right to choose who they want to share their information with. This information includes any abuse they've experienced, and any help they've sought. Supporting a survivor's right to privacy is an essential part of survivor-centered advocacy – it impacts their safety, their trust of your organization, their ability to control their own life, and their dignity.

Confidentiality encompasses the measures we as service providers are obligated to take to protect a survivor's ability to choose who accesses their information. The confidentiality of domestic violence and sexual assault survivor information collected by government-funded victim service providers is governed by U.S.

federal law (VAWA 34 USC §12291(b)(2); FVPSA 42 USC § 10402; VOCA 28 CFR 94.115, among others) and by the law(s) of most states.

Privilege refers to a legal rule that prohibits certain professionals from disclosing someone's information against their will. Generally speaking, when an advocate has privilege, a court cannot force a survivor or their advocate to disclose information shared between the advocate and survivor, and neither the advocate nor the survivor can be punished for a refusal to disclose the information**.**

You can out check these three tools in our our Confidentiality Toolkit for more in-depth information: Confidentiality Obligations Under VAWA, FVPSA and VOCA, Summary of State Laws Related to Advocate Confidentiality, and A Primer on Privilege & Confidentaility for Victim Service Providers.

Client Files: Content & Retention

A first step in ensuring that a database is truly confidential is to consider what information your program collects from survivors. **Best practice is to only collect the minimum amount of identifying information needed to provide services, and to keep it for the shortest amount of time necessary.** Not everything needs to be written down, shared with coworkers, reported, or retained. Only keep information deemed absolutely necessary to provide services and meet survivor-defined needs, or required to be kept by applicable laws or regulations. Purge anything else regularly and completely. Read our FAQ's on Record Retention & Deletion for more information.

Data collected during intake and service provision should be grounded in a survivor-centered approach. The heart of advocacy work involves talking with a survivor and hearing their story. From there, we work with the survivor to assess their immediate safety concerns, needs, and goals. Databases can make it too easy to add "just one more question" to the intake, which can lead to staff focusing more on filling out the fields on the form rather than listening to the survivor's needs. Intakes shouldn't feel burdensome to either the survivor or the program staff and should focus solely on gathering basic information needed to provide services.

Regularly discuss the data you collect with survivors, and let them review their own client file. Survivors can tell you what is outdated, what information they want removed, what they want kept, and what information may or may not be shared in the case of death (and possible fatality review). Survivors' lives and circumstances change, so the data an agency collects one day may become outdated - and potentially harmful - the next.

Our data obsessed culture has conditioned people to overlook daily invasions of privacy. We share our personal information in return for discounts, to get the latest popular app, and sometimes just to avoid being seen as difficult. For survivors, a breach in privacy can quickly become a life and death situation. By putting strong confidentiality protections in place, and by proactively offering opportunities to opt out of data collection through truly informed consent, we reinforce to survivors that we understand the impact of privacy on their safety, and they have a right to control their information.

Survivor Data

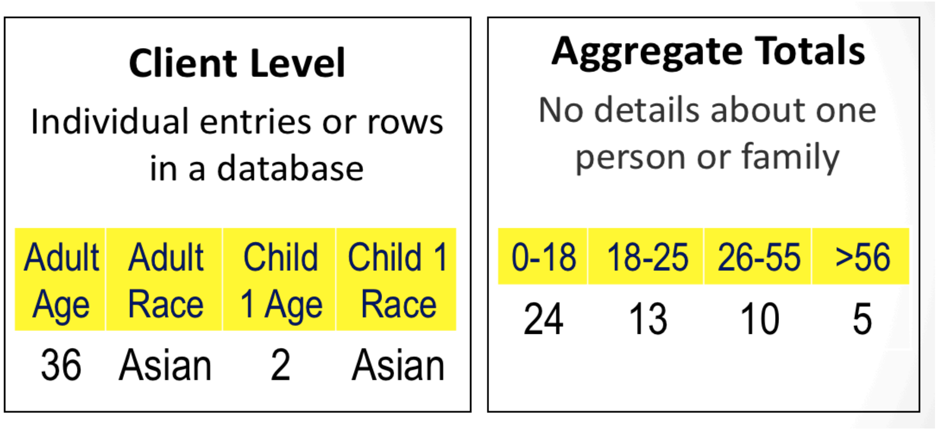
There are a few key terms that are helpful to understand related to survivor data and confidentiality.

Personally Identifying Information (PII) is information that alone, or in combination, could be used to identify a survivor. Obvious examples include name or contact information. However, individual demographic categories like race, ethnicity, gender, faith, and others can also be personally identifying when used in combination. For instance, in a rural area, the demographic categories: "South Asian," "gay," and "male," may be used to easily identify someone in the community.

Informed Consent requires that survivors should always be given meaningful opportunities to decide if and how they use use their information. It means they must be given the power to determine exactly what details will be collected, stored, and shared; be told exactly who will have access to that information; and that they will be able to determine how long that access is granted. They should be given information that helps them determine the risks and benefits of having their information collected, stored, and shared. And they should know they are able to withdraw consent and to opt-out of data collection at any time.

Survivors must never be forced to consent to share their information as a condition of services. Some funders have required certain questions to be asked in the hopes of gathering more information, but claim to “allow” survivors to give consent and to opt-out. In these situations it can be helpful to ask what will happen if a majority of people opt out of sharing that information when given a chance for truly informed consent. Will your organization be pressured or punished for how survivors exercise their privacy choices? If yes, then it is not a truly consent-based process.

Client Level Data vs. Aggregate Data Client level data refers to information about one specific person or family. Aggregate data refers to the totals of all the people or families served.



Client Level

Individual entries or rows in a database

Adult Age	Adult Race	Child 1 Age	Child 1 Race
36	Asian	2	Asian

Aggregate Totals

No details about one person or family

0-18	18-25	26-55	>56
24	13	10	5

Agencies are permitted to share ***non-personally identifying*** aggregate data about the services they've provided. Federal grant conditions also allow the sharing of ***non-personally identifying*** demographic information in order to comply with federal, state, tribal, or territorial reporting, evaluation, and data collection requirements. It is often for this purpose that programs consider using a database.

Data Security

In addition to making decisions about authorized access to the database, you must take strong precautions against accidental or malicious security breaches. Programs should abide by the phrase, "Don't collect what you can't protect," and may be required by grant conditions to have data breach policies in place (OVW awards now include this requirement). Read more about developing data breach policies.

While there is a risk even for paper files, storing sensitive survivor information electronically, and transmitting it through the Internet, poses additional risks. Any data kept on a computer that has Internet access is vulnerable to interception or breaches. Weigh these risks along with potential benefits including ease of tasks like reporting or hand-offs, and continuity of services and data recovery in the event of a disaster.

Paper Files

- Risks: unauthorized access to the physical files; destruction of the files in a natural disaster; data could remain on hard drive of copier or fax machine.
- Benefits: no risk of "hacking" or unauthorized access from a distance.

"Card Catalog" Database

In this method, the database references paper files and both are used. The data is entered with a non–identifying client code instead of a name. Paper files are labeled with the same code and this helps staff know which filing cabinet to go to in order to find the paper file.

- Risks: same as with paper files, plus non-identifying code might actually be identifying if based on PII.
- Benefits: no risk of "hacking" or unauthorized access from a distance.

In-House Database

The equipment and software for the database reside on a computer or server in your main office. The most secure option is for the database be kept on a computer that is not connected to the Internet, or to other devices that are connected to the Internet. Access to the equipment should be restricted to trusted staff and a board officer, and the protocol and practices should be audited annually to help ensure security and confidentiality standards are being maintained.

It's important to note that any information entered into a database might still be recovered even after it is deleted, as it's usually only truly purged once it is over-written with new information. Best practice is to secure backup copies of the data from an in-house database at the same level of security as the original source. With disaster preparedness in mind, backups should be stored securely either on-site in a fire- and water-proof safe, or off-site in a safe deposit box. Policies should clearly outline how long data should be retained, and identify a regular timeline and procedures for purging from both the working copy of a database and all backups.

- Risks: unauthorized access through an Internet-connected computer; responsibility for the security of the equipment and software rest with staff or a contractor; personnel could purposely or accidentally share confidential information or take advantage of their access to the database to perform searches for personal use; data might be recovered from a hard drive; all records might be accessed if hard drive is legally obtained in a warrant; destruction or limited access to data in a natural disaster; back-up of the data off-site or to the Cloud could lead to unauthorized access; untrained users may accidentally delete or alter data.

- Benefits: equipment is owned and/ or physically controlled by the program; number of people with access to the equipment is more limited.

Off-Site or Cloud-Based Database

The data is stored in the "Cloud," which really just means on someone else's server (often several servers or rented space in a "server farm"). These databases require an Internet connection every time information is transmitted back and forth. The vendors may actually use subcontractors to house and maintain the equipment that runs or stores backups of the database (meaning they may not own or have access to the servers where your data is). Read more about In-House Services vs. Cloud-Based Services.

- Risks: may give vendor and subcontractors routine access to PII without survivor consent; unauthorized access to data by vendor or subcontractors; increased opportunities for theft/hacking of vendor or subcontractor; vendors may routinely comply with subpoenas, warrants, informal law enforcement requests, etc.; internet access by staff and volunteers on personal machines may make information vulnerable to unauthorized disclosure.
- Benefits: protection against data loss during a natural disaster; less need for staffing, equipment to securely maintain database; internet access by staff and volunteers on mobile devices increases flexibility in delivering services.

External/Shared Databases

If programs are using databases that are accessible by other agencies, such as a collaborative partnership or a funder-provided database, no survivor personally identifying information should be included in the database. If the funder intends to offer an individual instance of the database to each program and claims no other programs can access your data, then you should ask the same questions about security of this database as you would of the off-site or cloud-based databases addressed above. Pay particular attention to whether the funder offering the database is also giving access to a "systems administrator" employed by the funder.

A “systems administrator” typically has access to everything in every corner of a database as part of the job, but that level of access would count as disclosing PII outside of your program.

Encryption

No matter where the database is located, an important security measure to be familiar with is encryption. *Encryption* is the method for protecting data by scrambling it, or making it unreadable to unauthorized people. Think of it as a lock with a key. Only people with the right key can unlock it. Encryption should be in place to protect data “at rest” when it is being stored on a server, and “in transit” when it is being sent to and from the database, usually over the Internet.

Zero-knowledge encryption (also called *no-knowledge encryption*) is the strongest option currently available to protect data held by third-parties. With zero-knowledge encryption, only the program holds the keys to unlock, or read, encrypted data; neither the third-party database provider nor any of their subcontractors holds a copy of the key to the encrypted data. This means that even if they did get access to the data, turned it over under subpoena, or had it stolen off of their machines, only an encrypted, scrambled, unreadable version would be seen.

Best practice requires that victim service programs choose databases that maintain confidentiality and protect the privacy and safety of survivors. No one outside of your stand-alone program or victim services unit should have access to the personally identifying information of survivors at any time. This includes database and IT vendors, their employees, and their subcontractors, as well as community partners your agency collaborates with.

The importance of encryption increases when the data or a back-up of the data will be held off-site or in the Cloud, as no one outside of your program should have access to the PII of survivors unless a survivor instructs you to share by providing written, informed, and time-limited consent.

If you are using a database that is off-site or in the Cloud, you should be able to change, download, or delete that data at any time. You should have clear information from the vendor about what would happen to the data if: you end your contract with them, they go out of business, they sell their company, they experience a data breach, they receive a request for survivor data, or the community experiences a natural disaster. The vendor should absolutely not own the data. Remember, information about a survivor belongs to that survivor, and your program is just holding on to it.

Access to Data

Any database should have specific access levels and security provisions. Policies and procedures should outline who will have access to which individual, personally identifying information. Authorized access to PII in the database should be determined based on need to know, role in the agency, type of data, event, and location.

***Role*.** Types of roles that indicate different levels of access include advocate, attorney, social worker, supervisor, program manager, administrative staff, IT staff, and vendor. When different professions are working together, they may have different legal requirements for information protection and mandatory disclosure. Be sure that information which a survivor voluntarily shared with one kind of professional remains within a circle of people who follow the same rules about information protection and sharing. If the database will be maintained by someone outside of your program, such as a vendor, security checks of personnel, confidentiality agreements, and technical security measures must be in place to protect the data in transit and at rest.

***Data*.** The type of data or part of the database to be accessed may include individual, identifying information about a survivor, demographic data that might or might not be identifying (learn more about PII above), aggregate data about services provided or communities served, or the structure of the database itself.

Event. Events that might warrant access to the database include during immediate or ongoing service provision; the review of files in the event of a mandatory report, an emergency, or a fatality; during supervision or case staffing; in response to a subpoena, warrant, court order or other similar external request; in order to report to funders; or when a survivor requests that information be shared with another external service provider. *Note: federal obligations prohibit sharing PII unless mandated by court order or state statute or with written, time-limited, and informed consent. Please refer to those obligations before extending access or pulling data to share due to a request.*

Location. Access to the database might be from a main office, a satellite office, a co-located service, courthouses, medical facilities, or other community locations. In addition, a variety of types of devices might be used to access a database, including desktops, laptops, tablets, or other devices. Read more about privacy and security with mobile advocacy.

If access will be possible outside of the main office, procedures must be in place to require that access to the devices/computers is secured with passwords; that passwords to the database are never saved on the device or web browser, that devices can be reclaimed or wiped when employee/volunteer leaves the program, and that the program is immediately notified if a device/computer is lost or stolen. There should be a clear and specific policy about accessing the database on personal devices, and the agency should provide staff and volunteers with the necessary secure equipment if off-side database access will be allowed.

Decisions about access based on role, type of data, event, and location will have implications for the structure and contents of the database, in order to support strong confidentiality and data security practices. Having a clear picture of these needs before reviewing databases or contacting vendors will help to clearly identify a product that meets your needs and protects survivor privacy.

Selecting a Database Vendor

Given that programs must maintain the confidentiality of survivor information, and that many will choose to use client information databases in order to hold sensitive information about survivors, it is crucial to select a database vendor that can offer the strongest possible protections for survivor data.

As a companion to this document, we offer three tools specifically designed for use by community-based victim service providers.

1. Client Information Database Needs Assessment. This can be used if you would like technical assistance from us as you gather information and make several key decisions before you begin evaluating vendors.
2. Vendor/Database Comparison. This form will help you compare the features, functionality, costs, and security of two or more vendors, in light of your needs, and survivor safety and privacy.
3. Vendor Negotiation Checklist. This will help you ensure that key considerations are discussed and resolved during the negotiation or contracting process with a selected vendor.

In addition to these tools, we offer an audio guide to selecting a database. Key considerations when selecting a vendor are included in the Vendor/Database Comparison chart, and are briefly explained below.

Ownership

The program must ensure that it retains control, oversight, and ownership of data. Ultimately, information about a survivor belongs to the survivor. The program is just holding on to it. The vendor, and any subcontractors, are simply providing the place in which a program stores it. The vendor should understand the program’s confidentiality obligations. Since they are different from other professions you cannot assume that a vendor working with hospitals or other social services already understands and will likely have to provide that education.

All agreements with the vendor should reflect these confidentiality obligations. The program should be able to download the data at any time, and take it with when the service agreement ends. The vendor should not keep copies of the data after that point. The vendor should clearly explain what will happen if they change ownership or go out of business.

Access

The vendor and its subcontractors should not have access to un-encrypted confidential client information. The program should understand and be comfortable with the vendor's policy for responding to a subpoena, court order, or warrant for the data. The vendor should notify the program of any request for data, so you can take steps to protect it.

Security

Sensitive survivor data, PII, should be encrypted in such a way that only the program can read the data. The vendor should not hold the key to decrypt the data. With these measures in place, inadvertent or malicious access to the data should be less of a risk, in that any data accessed would be "scrambled" and un-readable.

However, the vendor's security measures should still be robust, and they should do a regular internal security audit. The vendor should clearly explain what would happen when security flaws are discovered and if there is a security breach, including how flaws would be addressed, what records would exist of any breach, and how quickly the program would be notified.

Program Capacity

Pre-packaged, commercial databases are often less expensive up front, but may not be adaptable or may require additional costs to modify the database or create a new type of report, for example. If you choose to contract with someone to have a database developed especially for your program, modifications might increase the cost, or may be limited. The costs to develop, implement, and maintain a database can range widely from $5,000 to over $50,000.

Consider whether customizations and changes must be made by the vendor or can be done in-house. The ability to hide or remove certain fields, allow a field to be optional rather than required, or change the format from a text box to a drop-down menu can all be helpful over time, and, in some cases, may be required in order to meet confidentiality obligations. If changes can be done in-house, be sure to take into account needed training and support to the staff responsible for that work. Account both for any vendor fees for user training, as well as the time it will take advocates, managers, and IT staff to learn the new system.

The Vendor Comparison form is designed to help you compare Total Cost of Ownership, which includes:

- Initial fees (the database product itself, import of existing records)
- Customization (form fields, reports, access levels)
- Added capacity (storage, records, users, features)
- Technical support from the vendor
- Technology (hardware, software, Internet access, storage)
- Staff time (for managers, IT administrators, and user training)

Soliciting two or more bids is good practice for a large investment, in addition to meeting any requirements from funders or your own policies. Has the agency designated appropriate funds for the project? While modest expenses for outcomes measurements are part of any grant, a direct services grant should primarily fund services and not outcomes measurement.

Communicating with Survivors

If your database is linked in any way to your communication with survivors (e.g. websites, online chat, text, hotline call management, etc.) be aware of data incidentally collected through that communication technology that may include PII. Examples include survivors' phone numbers in records of calls, accounts, or billing information; survivors' IP addresses used in chat or when visiting your website; or survivors' user names or other information collected when beginning online chat sessions.

When communicating with survivors using technology, empower them to have greater choice, control, and knowledge about their own information and devices. Provide notice about how PII might be collected, and discuss risks and other options for receiving services. Help survivors increase privacy and security by navigating device and account settings. But also keep in mind that the survivor gets to choose what level of access is best and what risks to accept. The goal is not to pre-decide what technology is safe, but to help survivors decide for themselves what technology they feel is safe.

Remember that as survivors' experiences, needs and, risks are unique, complex, and constantly changing in "real life," there will also be implications for their digital life. Check in often about potential risks and make it clear that they can request a higher level of security at any time. More information about securely communicating with survivors can be found in our Digital Services Toolkit.

Supported by US DOJ-OVW Grant # 2019-TA-AX-K003. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.