Privacy First:
Working with IT and Data Vendors

Family Violence Centers (FVC) spend much of their time and resources providing crucial direct services such as survivor advocacy. As technology has advanced many of the forms of communications and support for this advocacy has become virtual necessitating support for Information Technology (IT) and databases that store sensitive and confidential information. As such, there are unique concerns around client confidentiality that must be addressed when FVC's engage with support for IT from external contract partners. This document will give an overview of those concerns and discuss some best practices for working with third party IT and database vendors while complying with law and prioritizing client privacy.

Relevant Laws

Violence Against Women Act (VAWA), Family Violence Prevention Service Act (FVPSA) & Victim of Crimes Act (VOCA)

These three federal laws have consistent language prohibiting sharing of personally identifying information with third parties outside of your family violence program. Specifically, "grantees and subgrantees shall not— (i) disclose, reveal, or release any personally identifying information or individual information collected in connection with services requested, utilized, or denied through grantees' and subgrantees' programs, *regardless of whether the information has been encoded, encrypted, hashed, or otherwise protected..."*

Health and Human Services Commission (HHSC) Texas Administrative Rules

If the program receives HHSC funds, Chapter 379 of the Texas Administrative Code (TAC) outlines extensive requirements regarding privacy and confidentiality, which includes protecting data collected in accordance to HHSC and federal law. Specifically, a center must limit data collection to:

- Information kept in client files to information necessary for funding purposes, advocacy purposes, and documentation for delivery services, and to protect liability.
- Programs may only release information with a written, informed, limited time, specific release of information, unless a state or federal law allows for an exception

TAC Chapter 379 also requires FVC's develop, maintain, and comply with written policies and procedures to promote the safety and security of residents, nonresidents, employees, and volunteers, including policy and procedure to address technology safety and data security.

Chapter 93 Texas Family Code

Under Texas state law, any written or oral communication between an advocate and a victim made in the course of advising, counseling, advocating for, assisting the advocate is confidential and may not be disclosed. This privilege to prohibit disclosure is held by the victim, or on the victim's behalf by the victim's attorney, guardian, advocate, or family violence center.

Important Terms

Personally Identifying Information (PII) Individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, regardless of whether the information is encoded, encrypted, hashed, or otherwise protected, including, a first and last name; a home or other physical address; contact information (including a postal, email or Internet protocol address, or telephone or facsimile number); a social security number, driver license number, passport number, or student identification number; and any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual.

Third Party Think about your program and the survivor receiving services as two parties, and your program has the requirement to keep information the survivor shares confidential within your program. Anyone outside of your program is considered a "third party" and not able to view any confidential information about the survivor.

Zero-Knowledge Encryption Data stored on a server or within a system is coded and unreadable by the third party

Privacy Considerations when Working with Technology, Databases, and Third-Party Vendor Staff

IT SUPPORT

Every program should have access to IT support to track your technology inventory and ensure up to date security measures. Privacy considerations depend on the relationship of IT support staff to your program:

- IT Support as employees of the agency: Having an internal employee is the best option for privacy and confidentiality of information. This staff member should go through the training requirements of your program to qualify as an advocate under Texas privilege law and comply with all federal confidentiality requirements. With this training, IT support staff will not only understand the confidentiality requirements of the PII that they may see while providing support, but also increase their understanding of the mission and goals of your program.
- Contracted IT support: To save on costs and based on need, programs often contract out to receive IT support. In this case, programs can take the same steps discussed below under "Third-Party Vendor Support".

THIRD-PARTY VENDOR SUPPORT

The following information will provide best practices for protecting survivor privacy once you have already identified a database or other third-party vendor for use. For more information on selecting a database, please visit NNEDV's database resources.

THIRD-PARTY VENDOR SUPPORT

Including confidentiality and privilege protections in your contract with the third-party vendor.

Privacy and data safety should be a part of your conversations with database vendors from the very beginning. When negotiating and signing the contract, make sure the following pieces are included:

- Your program is the sole owner of your data, even if your relationship with the vendor is terminated.
- Ensure that the subpoena or court order policy acknowledges your program as the owner of the data and the vendor is not able to provide your data in response to any legal inquiry.
- Utilize the strongest encryption possible for your data. Encryption should be at least 128 bit and, if possible, be zero-knowledge encryption. This means that the vendor and staff of that vendor cannot access your data at any time.
- Make sure the confidentiality language meets the standards of VAWA/FVPSA requirements and Texas privilege law. Have a signed confidentiality agreement that ensures any data shared with the vendor at any time cannot be released. This is incredibly important if the vendor offers database support by remoting into your system.
- A requirement to undergo training in line with HHSC TAC requirements under direct service volunteer requirements as these vendors have access to identifying information.
- A requirement to sign and acknowledge confidentiality agreements.

Protecting personally identifying information when receiving third-party support

Issues arise in the daily use and maintenance of using any technology, including a database. When receiving support, the third-party staff remoting in to fix the issue should be the last resort. This can raise privacy risks and potentially compromise data security. There are many steps that you can take to troubleshoot.

- Work with the third-party staff to solve the issue over the phone or through email.
- Never send individual client data or personally identifying information over email. When discussing an issue, use the client ID, or create a hypothetical situation to avoid sharing PII.
- Utilize a testing site to troubleshoot issues. The third-party staff should have a test system with fake client data available to them. Re-create the issue within the test system to figure out solutions.
- If the issue cannot be fixed over the telephone, email, or within the test system, take steps to protect personally identifying information before the vendor staff remotes into your system.
- If possible, sign into your system in a way that hides all fields that contain personally identifying information.
    - Close all client files within the database, and all other documentation on your computer.
    - Create a new client entry or a fake test client to use for troubleshooting purposes.
    - If you do this, make sure that you always delete any information that may accidently pull into your reporting.
- Ask the third-party staff what steps to clearly communicate what steps they are taking while remoted into your system. Work together to resolve issues without needing to open personally identifying information.

INTERNAL DATA SHARING

Keep in mind that you can practice privacy within your own organization.Make sure that only those who need access to the client level data have a log in. Limit administrative privileges to avoid accidental sharing or changing of data. Sharing information about clients that is needed to provide advocacy only is an easy and meaningful way to respect and practice privacy in all areas of your work.

What Other Technology Do You Use?

FVC's utilize technology in many forms to provide meaningful advocacy to survivors. When using technology, advocates should always ensure strict privacy and confidentiality protections are in place while also respecting survivor choice in how they wish to communicate and access services and the power of connection that can be created when using technology. Technology includes:

- Phones used for hotline calls
- Chat software
- Data collection software
- Email and document sharing software
- Virtual meeting platforms such as Zoom or Facetime... and many more!

No matter what technology you use, remember that survivors always have the right to:

- Refuse to provide any information they would not like to disclose. Services cannot be contingent on disclosure of information.
- View and request copies of their records at any time.
- Use technology as they believe is safe.

Resources and Links

Violence Against Women Act (VAWA)
Family Violence Prevention Service Act (FVPSA)
Victim of Crimes Act (VOCA)
Chapter 93 Texas Family Code
Chapter 51 Texas Human Resources Code
Texas Administration Code, Chapter 379
NNEDV: Vendor Checklist
NNEDV: Tech Safety

tcfv
TEXAS COUNCIL ON FAMILY VIOLENCE

Privacy First:

Third-Party Support Checklist

Use this check list to ensure you are protecting personally identifying information when a program staff (user) is receiving third-party support from IT support or a database support staff (vendor).

□ Work to solve the issue over the telephone or through email. When discussing an issue, use a hypothetical situation, client ID, or data element name instead of actual client information.

□ Troubleshoot problem using a test database owned by the vendor or with the Texas Council on Family Violence (TCFV).

If the vendor has to remote into the system, take the following steps before connecting:

□ If possible, vendor should ask the user to sign in to the system in a way that hides all fields that contain personally identifying information.

□ Have the user open a new client or fake test client to troubleshoot issue. Make sure to delete this client before ending support session.

□ Vendor should clearly communicate to the user steps they are taking within the system, and prioritize solutions that avoid viewing PII.