Databases, Confidentiality and Third Parties

A. What Domestic Violence and Sexual Assault Programs Should Know

Programs Are Required by Law To Keep Survivors' Personally Identifying Information Confidential

- Confidentiality of domestic violence and sexual assault survivor information is governed by U.S. federal law (VAWA 42 USC §13925/FVPSA 42 USC § 10402, among others) and by the law(s) of most states.
- The only exceptions to a program's confidentiality obligations are as follows:
  - When compelled by **state law(s)** that specifically overrides confidentiality protections (*e.g.*, mandated reporting of suspected child abuse or neglect).
  - When compelled by an official **court mandate**.
  - In the above circumstances, a program should still notify the victim of the disclosure and take steps to safeguard the privacy and safety of the victim and others impacted.
- Unless compelled by law, before a program may share personally identifying information about a survivor, it must first obtain a release that is *informed, written, and reasonably time-limited*. The release should be specific to meet the client's needs.

Confidentiality, Survivor Information, and Databases

- **Internal databases,** in which the information is *not* shared with outside parties, do not necessarily require client consent; however, programs must be vigilant and honor confidentiality. It is best practice for programs to create access levels that limit access to personally identifying information to only staff within the organization who need to see such information in order to do their jobs.
- **External/shared databases:** If programs are using databases that are accessible by third parties, such as a collaborative partner, no personally identifying information regarding survivors can be included into the database. Databases, by their nature, are not time-limited, and therefore do not meet the informed, written, and time-limited consent requirement in VAWA. Programs and agencies should not enter personally identifying information into databases shared within their partnerships.
- **Off-site data storage** is possible for domestic violence or sexual assault programs but only under certain limited circumstances that ensure that confidentiality of victim information will be maintained.
- Personally identifying information may only be shared outside of the domestic violence or sexual assault program if the program has an informed, written, and time-limited release from the victim or there are statutory or court mandates (see above). Releases can be used to share survivor information when doing so meets the needs of the survivor and should never be a condition of service.

Non-personally identifying aggregate data (totals) regarding services to program clients and **non-personally identifying demographic information** may be shared in order to comply with U.S. federal, state, tribal, or territorial reporting, evaluation, or data collection requirements.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

Databases, Confidentiality and Third Parties

B. What Domestic Violence and Sexual Assault Programs Should Do

- **Understand** all confidentiality laws regarding your programs.
- **Know** how to discuss confidentiality obligations with partnering agencies and why personally identifying information of survivors cannot be disclosed by you in shared databases.
- **Understand** that if your program chooses to use an off-site storage service, your program must sill honor confidentiality obligation.
- **Recognize** that the off-site storage guidelines apply to both electronic and paper records.
- **Evaluate** data collection and retention process and policies. Ask:
  - **Why?**
    - Why do we need to create and maintain a database?
    - What are the specific purposes and limits of data collection and data retention in light of confidentiality provisions?
  - **What?**
    - What information about survivors will be collected and maintained in the database?
    - Will the database include personally identifying information about survivors?
    - Will this information meet the goals of why you're collecting this data? Is all the information you're collecting necessary?
    - Note: It is best practice to only collect and maintain minimal amount of identifying information that is necessary to provide services.
  - **Who?**
    - Who will maintain the database? Is that person an employee, a contractor of our program, or an external third party?
    - What confidentiality agreements might be necessary?
    - Who will have access to the database? Will access levels exist so access to the data is limited?
  - **Where?**
    - Where will the database physically reside? On a computer or server within your program or on a third party server?
  - **When?**
    - How long will records be kept? How often will the database be purged?

C. Internally Maintained Databases vs. Off-Site/Remotely Maintained Databases

- **Internally maintained databases:**
  - Will the database be kept on a computer that is not connected to the internet and have specific access levels and security provisions?
  - Who will have access to individual, personally identifying information, and how will such access by limited (e.g., password protected computer or database; computer in separate, locked space; etc.)?

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

NNEDV

Databases, Confidentiality and Third Parties

- **Off-site/remotely maintained databases:**
  - Ensure that the offsite database is for storage only. There is a distinction between data that is stored offsite and data that is sent offsite for a third party to analyze, use, or manipulate. If the data is stored offsite and the program maintains proper oversight and control over the information, a survivor's consent to having their information stored in offsite databases is not required. If, however, the data is sent offsite for a third party to analyze, manipulate, or otherwise use, then each individual survivor must consent to that third party having access to her personally identifying information. Fully informed consent would include upfront notification to the survivor about who might get access to her/his data and for what purposes.
  - With offsite storage, the program must ensure that it retains control, oversight, and ownership of the data. Specifically, the program must have an agreement or understanding of the following with the offsite or third party service provider:
    - Philosophically, the client continues to own her own data.
    - The third-party storage provider understands the confidentiality obligations of the program.
    - What is the data storage provider's policy if they receive a subpoena, court order, or warrant for your data?
    - The off-site storage provider will not have unauthorized access to confidential client information.
    - Can you take your data with you when you leave the provider? Will they keep copies of your data even after you've left them?
    - The program understands the security measures in place by the off-site storage provider and that those measures are strict enough to avoid the inadvertent, unauthorized disclosure or use of individual, confidential client information. (For instance, such security measures could include the program having sole access to the stored data).
    - A specific confidentiality and non-disclosure agreement between the off-site storage provider and the program must be signed and followed.
    - Find out which third parties the company deals with and whether they are able to access your data.
    - Will the data storage provider have access to your information? If so, who?
    - Where is the data kept, and what data protection laws exist in the relevant jurisdictions?
    - Does the provider back up the data they store? If so, what are the security policies around that data?
    - Does the provider periodically do an internal security audit to ensure that staff doesn't suddenly or accidentally gain access privileges they're not supposed to.

The VAWA funded domestic violence or sexual assault program is required to ensure that client confidentiality is maintained, even when a third-party or offsite storage service is used.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.