Data Breaches & Victim Service Providers: Considerations for Developing Effective Policies

The Issue

Many victim service providers now maintain electronic records that contain detailed personally identifying information (PII) about people who have received services. Because confidentiality and privacy are essential to the safety and well-being of survivors, and because electronic systems are vulnerable to data breaches, the Office on Violence Against Women (OVW) now requires all grantees to have a data breach response plan in place. Many states and territories also have laws that require entities, which may include domestic violence and sexual assault programs, to follow certain steps in the event of a data breach.

What Programs Can Do

If (or when) electronic records are breached and PII is disclosed outside of the agency, victim service providers must have a data breach response plan in place to adhere to OVW requirements and state laws, while also protecting the privacy and confidentiality of survivors whose PII was disclosed. Programs will need to inform survivors that their information was disclosed so survivors can take steps to protect against any potential fallout of that disclosure. Programs will also need to think through how to safely contact survivors to inform them of the data breach.

The following are considerations for programs to discuss in order to best manage data and create solid data breach policies that prioritize survivor safety and privacy. We recommend addressing the following topics as you work with an attorney to draft a policy that meets the federal, state, territorial, and local requirements that are unique to your program.

Consideration #1: Audit Your Data Intake and Retention Processes

The best way to avoid releasing PII in a data breach is to minimize the amount of PII collected and retained in the first place. The best practice for data collection is to collect as little information as possible, and to keep it for the minimum amount of time necessary, while taking into consideration documentation requirements of funders. Review all of your current data collection and retention practices, do not collect information that is unnecessary, minimize the amount of time you keep the data, and review these policies and practices on a yearly basis. For more information, see our FAQs on Record Retention and Deletion.

Consideration #2: Develop Strong Data Security Measures

Work with IT professionals to ensure your agency's data security measures are up-to-date and that you have the proper mechanisms in place to protect the information you collect. Because the information you collect and keep is sensitive and could have a profound impact on the privacy and safety of the survivors you serve, it is critical that your data be as secure as possible. Review your data security practices every 6 months and update as necessary. For more information on the importance of privacy, confidentiality, and data security see our Data Security Checklist to Increase Victim Safety & Privacy.

Consideration #3: Determine Applicable Laws

The first step to creating internal policies and procedures is to identify the specific requirements and laws that apply to your program. While Federal OVW Special Conditions and state data breach notification laws outline specific requirements that organizations must follow when an individual's personal data is breached, they do not provide template policies. Policies should be drafted in consultation with an attorney to ensure that all applicable legal requirements are considered and incorporated.

- **Federal Laws**

  Pursuant to Special Conditions included in Fiscal Year 2019 grants under the Violence Against Women Act (VAWA), all grant recipients, and any subrecipient at any tier, **must have written procedures in place to respond in the event of an actual or imminent breach** (as defined in OMB M-17-12) if the grant recipient or subrecipient:

  1. Creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of personally identifiable information (PII) (as defined in 2 C.F.R. 200.79) within the scope of an OVW grant-funded program or activity, or
  2. Uses or operates a federal information system (as defined in OMB Circular A-130)

  In a few instances, victim service providers may also be subject to the Health Insurance Portability and Accountability Act (HIPAA). (Read the U.S. Department of Health and Human Services' Covered Entities & Business Associates document to find out if HIPAA rules apply to your organization.) The HIPAA Privacy and Security Rules have specific requirements for protection of protected health information data, along with specific protocols programs must follow in response to data breach events.

- **State & Territorial Laws**

  Every U.S. state and territory has a data breach response law. These laws generally set out specific requirements for how organizations should notify individuals whose sensitive personal information has been breached. The Privacy Rights Clearinghouse has published a summary of all state and territorial data breach statutes.

  In most states and territories, the statute applies to organizations that electronically store names or personally identifying numbers in an

unredacted, unencrypted format. Victim service programs that collect and store personally identifying numbers (such as social security numbers) or maintain personal information in an unencrypted format may be required to comply with these statutes. *Note: It is **not** best practice to store PII in an unencrypted format. Ensuring data is encrypted will significantly decrease the possibility of a breach.*

Consideration #4: Contacting People Affected by the Breach

Since 2005, VAWA has required victim service programs to make reasonable attempts to notify survivors if their information is going to be disclosed when there is a valid mandate. This requirement also applies in the case of an accidental or unauthorized disclosure, such as a data breach. In order to comply with this requirement, programs should already have processes in place for making reasonable attempts to notify and provide follow-up support to survivors.

Such processes must be designed so that programs can contact the survivor without disclosing to others that the person received services, which means carefully considering how a survivor will be notified and how to minimize the risks of accidental or intentional interception. Programs should also be sure to consider how notifications may impact survivors and be prepared to respond. Some survivors may need advocacy related services, some may want emotional support, and others may request referrals as they deal with the fallout of accidental or unauthorized disclosure.

Most state and territorial data breach response statutes are prescriptive in their notification requirements and require direct written notification to every person affected by a data breach, either by mail or email. Although there are potential safety and privacy concerns when a victim service provider contacts a survivor in this way, these statutes generally do not recognize such concerns as an exception to this requirement. (This is another reason that programs should limit the

amount of PII they retain in the first place, and ensure that the personally identifying data they do store is encrypted and secure.) However, some state and territorial data breach notification statutes may be flexible and allow privacy and safety considerations to be included in data breach response policies, as long as the organization develops a policy and procedure that is consistent with the spirit of the statute.

Programs should work with a local attorney and their state & territorial domestic violence and sexual assault coalitions to develop a reasonable and safe mechanism for notifying survivors of a data breach that complies with all applicable laws.

Breach notification policies need to:

- take into account survivors' safety and privacy,
- not breach survivor confidentiality,
- meet the intent of all applicable laws, and
- reasonably inform survivors whose data has been breached so they can take measures to minimize the harm that may have been caused by the breach.

Consideration #5: Notifying Government Agencies

As of Fiscal Year 2019, VAWA grant recipients' data breach response procedures must include a process for reporting the actual or imminent breach of personally identifying information to an OVW Program Manager no later than 24 hours after an occurrence of an actual breach or the detection of an imminent breach. The few programs that are HIPAA-covered entities must also comply with the HIPAA Breach Notification Rule, found at 45 CFR §§ 164.400-414.

Summary

Survivors face significant safety and privacy risks, which can quickly increase if their personal information is shared without their consent. The strict confidentiality obligations outlined in VAWA, FVPSA, and VOCA were drafted to minimize such risks by ensuring that victim service programs are legally bound to protect survivor privacy and autonomy. Organizations should employ best practices related to data collection, retention and deletion, and work with a local attorney and their state or territorial coalition to ensure that in the event of a data breach, they have a response plan in place that carefully balances their legal obligations with the safety, privacy, and emotional well-being of the survivors they serve.

This document was drafted in cooperation with the Danu Center's Confidentiality Institute and the Resource Sharing Project.

Supported by US DOJ-OVW Grant #2016-TA-AX-K064. 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, or contact us with any follow up questions.