In this practice tool, Part I covers the rules for protection of victim information and privacy. Part II offers strategies for conducting audits within those rules. Part III offers strategies for collaboration and key resources for assistance when there is conflict or uncertainty.

Part I
The Rules

VAWA Statutory Grant Condition:
“[VAWA] [G]rantees and subgrantees shall not disclose, reveal, or release any personally identifying information [PII] 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[.] 34 USC §12291(b)(2)

To a large extent, that’s the end of the story. The VAWA grant conditions require that grantees “shall protect the confidentiality and privacy” of people receiving services from providers receiving that funding. Difficulties with fully protecting personally identifying information (“PII”) tend to arise in three circumstances:

(1) When grantees believe they have to share despite the rule;

(2) When funding administrators believe they are entitled to information notwithstanding the rule; and

(3) When allies believe they can be trusted with the information, and seek to go around the rule.
To ensure appropriate victim privacy, grantees, funding administrators, and allies all need to learn the rules of best practice and be prepared to abide by them.

Privacy means respecting a person’s right to have control over their personal information. Whenever a program is considering sharing, distributing, manipulating, or otherwise disclosing PII, the program must consider the privacy impact. Does this disclosure infringe upon the personal control of victims and their families over information about themselves? To protect their “confidentiality and privacy,” victims of violence should decide for themselves whether PII may be disclosed by a grantee.

To properly protect victims’ PII, programs must determine what counts as a “disclosure of PII”. VAWA defines PII as:

“...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... including –

(A) a first and last name;
(B) a home or other physical address;
(C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number);
(D) a social security number, driver license number, passport number, or student identification number, and
(E) any other information, including date of birth, racial or ethnic background, or religious affiliation that would serve to identify an individual.”

- VAWA 2013, 34 USC §12291(a)(20)

Given the data manipulation available in modern technology, almost any set of data points in combination, linked to an individual (even an unnamed one), becomes potentially identifiable.
Because abusers/assailants can be highly motivated to find information about victims, programs should constantly reexamine practices to ensure they are protecting against this. Abusers can \textit{and do} enlist others to help them locate victims in hiding, so any information that could link a victim to a particular program might be dug up as a tool to stalk or track. Family members who work for state agencies can be asked to access databases; law enforcement officers can be co-opted as investigators of missing persons’ reports; and private investigators can be hired on false pretenses.

Even when programs submit reports from their database with aggregate information about victims (with the intention that aggregate data will de-identify individuals), programs should first consider if that information could be cross referenced with other databases of information with identifiable information (such as an HMIS database or web-based news sites.)

\textbf{Here are some useful questions to ask when considering whether or not victim privacy is at risk:}

1. \textit{“How might this information be used to identify, locate, or harm the person who trusted me with it?”}  
   Emotional and reputational harm are just as damaging as physical harm in this analysis.

2. \textit{“Does this count as a disclosure?”}  
   If grantees or sub-grantees put PII in the hands (literal or electronic) of anyone outside of their victim services program, or put information at substantial risk of leaking outside of their program, they have a disclosure problem. In the past, some local and even government funders believed they could receive confidential PII as long as it was encrypted to protect against a hack or other data breach. However, giving PII to funders in an encrypted form is \textit{still} a disclosure of PII to a third party; the funder is the third party. Encryption merely prevents \textit{additional} third parties from accessing the PII.
Passing on sensitive information about survivors to funders violates individual privacy by putting the information outside of the control of the victim. The disclosure increases the risk that it will leak out to the broader world because most funders do not have the same legal protections against forced disclosure as do the service providers. For some government-based funders, any information they receive could become a “public record,” subject to disclosure upon a demand by any person or media outlet. Other funders could be forced to disclose information pursuant to subpoena or other legal action, even though the original domestic violence shelter would have had a privilege to prevent disclosure.

To protect victim safety, agencies should develop a policy stating that disclosures (absent informed consent or legal mandate) are prohibited, and should clearly articulate that sharing outside of the victim services program (even with allies and funders) counts as a disclosure.

3. “Is this information identifying even though it is presented in an aggregate report?”

Programs can routinely share aggregate, non-personally identifying information with funders and the public. When sharing aggregate data, programs have to watch out that it doesn’t become identifying. If a particular person or family is demographically rare in the community (because of national origin, race, size of family, gender identity, etc.), then the person’s information cannot be safely aggregated.

Imagine if a program served 100 white survivors, 100 African-American survivors, and one Asian survivor. Disclosing those numbers outside of the program poses a fairly substantial risk that the one Asian survivor can be identified. Similarly, identifying a program’s unnamed Asian client as pregnant, transgender, or a parent to six children increases the risk of re-identification. Any demographic category that combines a specific characteristic and a small number of individuals can become identifying.
To preserve survivor privacy, programs should use broad report categories such as “other” to capture services offered to demographic outliers. Programs still can analyze that information internally to examine whether this person is demographically unique or the program needs to increase outreach to survivors in that demographic. But, they would want to avoid sharing it outside of the victim services program.

**Exceptions When PII May Be Disclosed**

While keeping privacy in mind, grantees are allowed – sometimes even commanded – to disclose PII in narrow circumstances. These are summarized below.

1) **Information generated by law enforcement, prosecutors, and courts** can be disclosed by those entities. This exception does not apply to community-based victim service provider grantees, because they are not part of law enforcement agencies, prosecutors’ offices, or courts. However, grantees should be aware of this exception, and all systems partners should help survivors connect with victim service providers that are able to fully protect PII whenever it is appropriate to do so.

2) When a program is subject to a **valid court mandate** (e.g., a properly issued search warrant), it can disclose the information specifically identified by the court. If a court decision has set a state-wide precedent requiring disclosure of specific information (e.g., a common law duty to warn), then VAWA-funded programs can comply with that common law. Note that a subpoena is not necessarily the same as a final court order in most jurisdictions and may not create an exception to the confidentiality obligations. In the situation where a valid court mandate is issued, programs may disclose the information required, and shall also:

   a) make reasonable attempts to give notice to victims affected by disclosure,
   b) and take the steps necessary to protect the privacy and safety of persons affected by the release of information.
• One key step to protect privacy is retaining counsel for the program or the employee to resist court orders or subpoenas that violate state law or public policy. Programs that are confronted with a subpoena can access the following resources for technical assistance:

  o American Bar Association & Confidentiality Institute’s “Protecting Privacy to Enhance Safety” Subpoena Defense Project training materials for attorneys

  o Technology & Confidentiality Toolkits at techsafety.org/resources

  o Safety Net Project in partnership with Confidentiality Institute at safetynet@nnedv.org

3) When a program is subject to a valid statutory mandate, it is allowed to disclose the narrow amount of PII required by the statute. As discussed above, the program is also required to take protective measures and make reasonable attempts to notify the victim.

• The disclosure must be actually required, not just allowed, and it must be commanded by a statute, not just a government policy, procedure or regulation. If a state-funding contract instructs recipients to share identifying information with state agencies, even though no state statute requires it, that is not a statutory mandate and would not create an exception under VAWA. If a state agency issues a rule requiring rape crisis centers to disclose PII, that is not a statutory mandate. Wherever a program experiences overreaching in demands for disclosure of PII, the program has a duty to put on the brakes, assert the VAWA non-disclosure rule, and determine whether an exception applies. Programs can reach out to the same resources listed above for assistance in complying with VAWA mandates.
Releases: Keep your W.I.T.S. About You!
Survivors can instruct programs to share PII by completing a written, informed, reasonably time-limited specific release. It is easy to remember the rules of releases if you remember to keep your W.I.T.S. about you:

- Written
- Informed
- Time-limited
- Survivor-centered & specific

W.I.T.S. releases will protect victim privacy interests. Conceptually, releases are an extension of the privacy and non-disclosure rules, not an exception to them.

When a survivor wants PII released by the program in an identifiable way, the survivor is exercising their right to control their own information. The program is merely acting as the survivor’s agent in the disclosure and is not acting on its own behalf or for its own purposes. Releases should never be demanded or even routinely expected. Under VAWA, a grantee cannot make a release of information a condition of receiving services.

Survivor-centered practice means that each survivor will decide how PII disclosure fits in with their individual goals and safety planning. A sample release form is available in NNEDV’s Confidentiality Toolkit located at techsafety.org/confidentiality-templates.
In this practice tool, Part I covers the rules for protection of victim information and privacy. Part II offers strategies for conducting audits within those rules. Part III offers strategies for collaboration and key resources for assistance when there is conflict or uncertainty.

Part II
Playing by the Rules

Programs, grant administrators, and allies can all work together to play by the rules of privacy. Let’s consider the most frequently asked question that arises, and ways to solve it while protecting victim privacy:

Conducting Performance and Compliance Audits
Grantors and auditors should not read a victim service program’s raw files (paper or electronic) as part of grant management, monitoring, or audit processes. There are alternative ways that grantors and auditors can assess performance and compliance, without reviewing raw files that contain PII of survivors. The federal government has long funded confidential professionals such as legal services lawyers, and has conducted appropriate routine audits without needing to violate attorney-client privilege. The same protocols should be followed for victim service program files

Both the auditor and the program must start by understanding the program’s confidentiality rules (whether stemming from VAWA, FVPSA, VOCA, other funding conditions, state law, or mission-based best practice). Then the auditors should identify what information is actually needed to effectively assess performance
and compliance. Next, discuss how to sufficiently confirm completion of the work without disclosing PII. Here are some practical strategies that often work:

- A program can give aggregate numbers of people served and services delivered, *and* offer a detailed explanation of its board-approved process for counting clients and services provided.

- Together, the program and auditor could agree on a checklist that is associated with each client, that doesn’t include PII, but reflects the program’s confirmation of which services were provided to each client.

- An auditor can sit across from an Executive Director (or designee) who has access to files and ask yes/no compliance questions. The Executive Director can be instructed to pull every fifth file from a drawer or every fifth name from an electronically-generated list.

- A program can give all clients a client identifier code (that is completely unconnected to any PII) to facilitate creation of anonymous lists of people served. The key to that code will not leave the program or be shared with the auditor.

- An auditor can request access to randomly-pulled files with all identifying information redacted. The auditor then reviews those redacted copied files on-site at the program, and the redacted versions are shredded when the audit is completed.

  - Redaction is the most resource-intensive option with the highest likelihood of violating federal confidentiality requirements through inadvertent disclosure of PII.

  - Programs must have advance notice of which files are being sought so that they can assign staff to spend time redacting the files.

  - All of the demographic and narrative information must be read and assessed for its potential to identify, either directly or through context.
A staff person must copy the records and permanently remove the PII.

- Black marker is often insufficient to actually remove the PII because the typeface shows through, especially when copies are made.

- Programs using redaction should seriously consider purchasing a product, such as Adobe Acrobat Pro, that will electronically & permanently remove selected data from the document, allowing the program to print out that redacted copy with no risk of disclosing the information that was removed.

- Temporarily covering information with a post-it note is not an effective redaction technique.

Another staff person should read the redacted documents to see whether the remaining information, after redaction, can be used to identify the survivor and/or their family members.

- For example, the author of this document once received a “redacted” file from child welfare that removed the name of a collateral witness, but left in a narrative description of that witness as the minor child’s paternal uncle – thus identifying the witness.

These documents are reviewed at the provider’s site and shredded after audit/administrator review is completed.

**Key Considerations for Site Visits at Locations Where Survivors Receive Services**

On-site visits by auditors to locations where survivors are receiving services (especially shelters) should always be planned and never be surprise visits.

- Survivor autonomy and control over information is central to providing effective services for domestic and family violence.
• To avoid re-traumatization, programs must prepare survivors for visits by outside government auditors and state administrative staff.

• Survivors can then choose if they prefer to be in the building at the time of the visit or not.

• While inside of the program, it is not appropriate for administrators to try to contact survivors or ask them about their experience.
  
  o Programs can prominently display the grant administrator’s contact information for any survivor who chooses to reach out and share the experience they have had with the victim services provider.

• Despite best efforts, a visiting auditor may be exposed to PII about survivors receiving services, therefore all visitors should sign a confidentiality agreement in advance confirming that they will not further disclose any information about individual survivors that they happen to learn during the visit.

Further Exploration
To further explore other methods for oversight without violating privacy, programs should ask colleagues who participate in auditing processes of other confidential professions to find out how they do it. One caution: depending on your state, VAWA-funded programs may have a higher level of privacy protection than even lawyers and doctors, so you can never skip the step of understanding the rules that apply to the specific program that will be audited.

• HIPAA allows for a fairly broad swath of protected health information to be shared with “business associates,” so long as the medical provider feels it is helpful to share the information and the business associate contractually agrees to follow the healthcare provider’s rules. Neither FVPSA, VAWA, nor VOCA contain any business associate exception.
In this practice tool, Part I covers the rules for protection of victim information and privacy. Part II offers strategies for conducting audits within those rules. Part III offers strategies for collaboration and key resources for assistance when there is conflict or uncertainty.

Part III
Collaboration, Communications, & Technical Assistance

How Programs Can Collaborate with Partners to Serve Survivors

Federal and non-governmental funders are placing increasing emphasis on collaboration and coordination between organizations and agencies. These are valuable goals, and programs should always be looking for ways to collaborate that are consistent with their mission and guidelines.

“Consistent with the mission and guidelines” is the key concept. Victim privacy and control over their information is fundamental to the work of victim service providers; therefore, victim services programs cannot make disclosure exceptions for collaborations with outside entities.

Here are some touchstone considerations for any victim services provider looking to participate in a community collaboration:

• Have a memorandum of understanding that sets forth:
  o The goals of the collaboration with a fair amount of measurable specificity;
  o The identity of each participant / entity in the collaboration; and,
- The information-sharing norms (around both disclosure and non-disclosure) applicable to each professional/entity in the group (such as prosecutors, police officers, victim service providers, medical providers, and educators).

A sample memorandum of understanding for collaborative partners can be found in NNEDV’s Confidentiality Toolkit at [www.techsafety.org/confidentiality-templates](http://www.techsafety.org/confidentiality-templates).

- Consider sending a representative to the collaboration who does not provide direct services and does not know any PII, to decrease the likelihood that any PII would be disclosed.

- Create opportunities for victim service providers to teach other participants in the collaboration about their work, their mission, and their rules. The confidentiality obligations of community-based victim service providers may be the least well-known within the multidisciplinary group, and education about confidentiality can vastly reduce pressure on individual advocates to disclose. It can also help other professions understand the parameters of the information that victim service providers can offer to the collaborative effort.

- Prepare for the meetings and talk to individual clients about how they might want to participate in the collaboration. A client can direct an advocate to act as an agent and disclose specific information. Clients don’t often ask to do that because they don’t realize it is possible; advocates may want to raise survivor awareness about this strategy for participating in collaborations. If a client wants to rely on an advocate as an agent to disclose information, then a written, informed reasonably time-limited release must be completed and strictly followed.

- Use questions about an individual survivor as an opportunity to do systems level advocacy about the needs of survivors as a group. If a prosecutor asks, “Did she ever have sex with him before the alleged rape?” then an
advocate could answer: “Experience tells us that victims feel ashamed and blamed for their rape when their personal sexual histories are investigated. Just asking a question like that could cause a survivor to stop cooperating with the prosecution. Can you help me understand why you want to know that information? What impact does a yes or no have on whether you will prosecute or get a conviction?” This discussion furthers the collaboration, may uncover information needed by the survivor, and protects survivor’s private information held by the advocate.

**Demonstrating Outcomes**

In this increasingly data-driven, competitive funding environment, programs and communities ask, “How do we tell the stories of success and explain our outcomes?”

When a survivor names a rape crisis center as having been key to her recovery, she makes a huge impact on the public understanding of the value of victim services. But when a rape crisis center decides to use a survivor’s story to advance program-defined goals of publicity and fundraising, it runs a huge risk of violating privacy and objectifying the survivor. Programs need to think carefully about when and how to even seek permission to use a person’s story, because programs hold so much power in the relationship with the survivor. Here are some thoughts on how to go about celebrating success consistent with protection of victim privacy and the mission of victim services work:

- Participation in long-term outcomes measurement should always be completely voluntary. Never suggest to clients that participation is routine or expected from them. Don’t ask the survivor to make the decision while talking to you – offer them time and space to consider it more thoroughly. Be prepared to tell the client what benefit they will get from participating. Clients are entitled to time and privacy to decide whether to opt into measuring outcomes.
• Report your outcomes as non-personally identifying, aggregate information, not individual information.

• Ask for clients’ opinions for a variety of reasons – not just when you want to brag publicly or track them. Create an atmosphere where former clients are welcomed to participate in systems advocacy, program quality improvement, and volunteering opportunities. If a client decides that the path from victim to survivor is served by publicly sharing benefits received, then facilitate this and let the client take the lead in telling his or her own story.

Compliance with Federal Confidentiality Requirements
Privacy is extraordinarily important in this work, and 21st century pressures to disclose information can be intense, so programs should access help to ensure they stay within the boundaries of federal confidentiality requirements.

Programs and grant administrators should discuss confidentiality policies and procedures in order to help grantees document compliance with privacy and confidentiality provisions. This process of “assessment and assurances” may uncover a need for procedural change or new policies. And while the rules for privacy are straight-forward enough, the best way to play by them is not always obvious. Sometimes, we are saddled with past practices that violate victim privacy, but changing them feels difficult, and maybe even impossible. When funders and allies are accustomed to a certain access to information, a program will need to directly address why the change is being made, and reassure that this is not a judgment about the trustworthiness of a particular community partner.

Regardless of pushback, protecting survivor privacy is not optional. Failure to be protective of confidentiality could result in loss of funding sources, distrust by the survivor community, and even legal liability if harm flows from an unauthorized disclosure of PII.
Grant administrators, coalitions, and individual programs can all get help to implement confidentiality correctly:

- Confidentiality Institute (www.confidentialityinstitute.org) provides national privacy training, as well as individualized technical assistance for resolving thorny confidentiality problems.

- The National Network to End Domestic Violence is a national technical assistance provider on survivor confidentiality and works closely with Confidentiality Institute. Together, they have created an online toolkit of templates, FAQs, tip sheets, and excerpts of the law. You can find the Confidentiality Toolkit at www.techsafety.org/confidentiality, and you can submit technical assistance questions to safetynet@nnedv.org.

© 2019 National Network to End Domestic Violence, Safety Net Project. Supported by Grant No. 2016-TA-AX-K064 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

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