NNEDV
NATIONAL NETWORK TO END DOMESTIC VIOLENCE

1325 Massachusetts Ave NW
7th Floor
Washington, DC 20005-4188

NNEDV.org
phone: 202.543.5566
fax: 202.543.5626

HUD Continuum of Care and Emergency Solutions Grants Grantee Monitoring for Victim Service Providers

Domestic violence providers that receive HUD Continuum of Care (CoC) and Emergency Solution Grant (ESG) funds face pressure from grant funding auditors and monitors to reveal clients' personally identifying information. This resource provides statutory references to help domestic violence programs and other Victim Service Providers navigate their responsibilities to protect victim confidentiality and participate in auditing and monitoring in connection with their HUD funds.

This resource answers the following two questions:

> **May VAWA, FVPSA and VOCA-funded victim service providers grantees disclose personally identifying victim information to HUD auditors conducting routine audits? No.**
>
> **Can victim service providers participate in HUD audits and other program evaluations without disclosing personally identifying victim information? Yes.**

In brief, pursuant to the universal grant conditions imposed by Congress on VAWA, FVPSA, and applied to VOCA Victim Assistance programs by regulation:

- Personally identifying victim information (PII) is confidential, and may not be disclosed in the course of reporting to funders, participating in program evaluation, or complying with routine audits.
- Grant administrators and auditors may be provided with non-personally identifying, aggregate data (totals) in order to comply with federal, state, tribal, or territorial reporting, evaluation, or data collection requirements.
- If a Victim Service Provider shares personally identifying client information (without informed, written, time-limited consent of the victim), then the program could be in violation of federal and/or state law, and risk losing access to federal VAWA, FVPSA, and/or VOCA funds. These confidentiality grant conditions also prohibit programs from making the signing of a release a condition of service.
- Within the confidentiality requirements of VAWA, FVPSA and VOCA, there are:
  - no exceptions for disclosure pursuant to administrative regulations, and
  - no allowances for disclosure of encrypted data if the recipient auditor has a key to unlock the encryption.
- VAWA, FVPSA and VOCA do contain an exception for disclosure pursuant to statutory or court mandate. If disclosure of PII pursuant to statutory or court mandate is made, the program is required to:
  - make reasonable attempts to provide notice to victims affected by the disclosure, and
  - take the steps necessary to protect the privacy and safety of persons affected by the disclosure.

Author: Alicia L. Aiken, J.D. - Confidentiality Institute © 2018
(adapted from previous work with permission from Julie Kunce Field, Esq.)

- The regulations granting federal access to the records of non-profit organizations do not allow access to names or other personally identifying information about crime victims in routine audits.
- Victim Service Providers can and should cooperate with HUD audits by assigning managerial staff to:
    - assist auditors in reviewing agency records,
    - complete **redaction** of personally identifying information from records, and
    - answer specific questions about services provided without disclosing confidential information.

Relevant Statutes Prohibiting Disclosure of Victim Identifying Information

Violence Against Women Act (VAWA)

Since 2005, VAWA has explicitly protected personally identifying victim information (PII) from disclosure, even to federal grant administrators and auditors.

VAWA 2005 was passed by Congress in December 2005 and became effective on January 6, 2006. The VAWA confidentiality provisions were continued in the 2013 Reauthorization of VAWA. VAWA 2013 includes a universal grant condition that requires VAWA grantees to maintain the confidentiality of personally identifying victim information.

VAWA has two provisions that are relevant to understanding the congressionally mandated confidentiality protections for Victim Service Providers receiving both VAWA and HUD funding:

1. **VAWA 2005 Section 605,[1] Amendment to the McKinney-Vento Homeless Assistance Act Prohibiting Disclosure of PII in the Homeless Management Information System (HMIS).**

   VAWA 2005 Section 605 addresses the confidentiality of a victim's personally identifying information for purposes of a data collection project – the Homeless Management Information System (HMIS). In this provision, Congress amended the McKinney-Vento Homeless Assistance Act to prohibit victim service providers from entering PII into an HMIS system. The prohibition on entering PII into an HMIS (42 USC §11363) and the definition of a "victim service provider" and of "personally identifying information or personal information" are drawn directly from VAWA 2005 (42 USC §11360(16), (32)). The provision protects victims' information from being disclosed or entered into HMIS which (alone or in conjunction with other information) specifically identifies a particular victim or their location.

2. **VAWA 2013 Section 3 Universal Grant Conditions: Nondisclosure of Confidential or Private Information[2]**

   VAWA 2013 Section 3, applies to all recipients and subrecipients. It prohibits disclosure of personally identifying information or individual information collected in connection with services requested, utilized, or denied through recipients' and subrecipients' programs.

   "Personally identifying information" is specifically defined in VAWA (34 USC §12291(a)(20) as:

   (a)(20) PERSONALLY IDENTIFYING INFORMATION OR PERSONAL INFORMATION.—The term 'personally identifying information' or 'personal information' means 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 any individual.

This memo does not address what information, e.g., geographic or demographic information, might be or might become personally identifying. What is personally identifying is contextual – the smaller the community is geographically or the more demographically unique the person, the more easily information that would not otherwise be personally identifying alone could become so. Programs must exercise judgment about an individual's record to protect the victim's personal identifying information.

VAWA 2013 explicitly prohibits sharing personally identifying information for federal, state or tribal grant reporting, evaluation or data collection purposes, and prohibits requiring victims to consent to share information as a condition of receiving services.

Victim Service Providers can share aggregate information that does not identify individuals. Section 3 of VAWA 2013 specifically allows the sharing of "nonpersonally identifying data in the aggregate regarding services to their clients and nonpersonally identifying demographic information in order to comply with federal, state, tribal, or territorial reporting, evaluation, or data collection requirements."
Programs can and should report on their services to the community and be accountable for how they spend federal funds; *however,* they are not allowed to share an individual trauma survivor's identifying information as part of their reporting and accountability activities.

Family Violence Prevention and Services Act (FVPSA)

In 2010, the Family Violence Prevention and Services Act (FVPSA) adopted the VAWA Standard for Non-Disclosure of Victim PII. [3]

As of December 20, 2010, the Family Violence Prevention and Services Act (FVPSA) was amended to include a confidentiality requirement that closely mirrors the language in VAWA as a universal condition of funding. While FVPSA has always recognized the importance of confidentiality, it is now completely clear that the contours of the personally identifying information protections under FVPSA are the same as the protections under VAWA.

In addition to meeting the specific criteria set forth in FVPSA, grantees must also agree to comply with requirements that the U.S. Secretary of Health and Human Services deems necessary to carry out the purposes and provisions of the FVPSA. One such requirement, reflected in previous program announcements, specifies: "when providing statistical data on program activities and program services, individual identifiers of client records will not be used." Under FVPSA, programs may not release personally identifying information, and may only share nonpersonally identifying, aggregate information when complying with federal, state and tribal grant reporting and evaluation requirements.

Victims of Crime Act (VOCA)

In 2016, the Office for Victims of Crime (OVC) adopted the VAWA Standard for Non-Disclosure of Victim PII by victim assistance grantees.[4]

As of July 2016, Victim Assistance Program grantees under the Victim Compensation and Assistance Program (part of the Victims of Crime Act of 1984) (42 USC §10601 *et. seq.)* are prohibited from disclosing personally identifying and individual information collected in connection with services. The Office for Victims of Crime explicitly adopted the VAWA standard for non-disclosure of information. As with the VAWA statutory prohibitions it specifically prohibits sharing PII to comply with reporting, evaluation or data-collection requirements of "any program".

Personally Identifying Information & Auditors

There is no federal statutory mandate requiring VAWA, FVPSA, and VOCA grantees to disclose personally identifying information about people receiving services for the purposes of audits of grantee financial records and their use of federal funds.

While there are regulations indicating that HUD program recipients and subrecipients should share all records with federal auditors and regulators, those regulations do not rise to the level of a *statutory* mandate as is required by VAWA, FVPSA and VOCA before recipients and subrecipients of HUD program funds are allowed to lawfully disclose PII. Significantly, even the regulations which are often relied on to justify access to PII prohibit routine access by auditors to the "true names" of crime victims.

Much of the confusion as to whether auditors can access the PII of victims of crime (including victims of domestic violence, sexual assault, stalking, dating violence and family violence) stems from the language in Emergency Solutions Grant (ESG) regulations. 24 CFR 576.500 requires ESG recipients and subrecipients to have a policy to protect the confidentiality of all records of any families receiving ESG assistance, *but also* articulates an exception for federal government access to records pursuant to the regulation at 2 CFR 200.336. 24 CFR 576.500(x),(z). Some have incorrectly assumed that this ESG regulation creates a requirement that VAWA, FVPSA and VOCA funded recipients of ESG funds disregard their specialized confidentiality requirements and grant HUD auditors and administrators routine access to the personally identifying and individual information of domestic violence, sexual assault, stalking, dating violence, family violence, and other violent crime victims. As discussed above, VAWA, FVPSA and VOCA funded grantees may only disclose PII collected in connection with services provided in response to a *statutory* or *court* mandate. The regulations for administration of the ESG program are neither statutory nor court mandated, and thus don not carve out an exception for disclosure of VAWA, FVPSA, VOCA protected information.

Even if the ESG regulations could create an exception for routine access to crime victim information, the current regulation does not actually do so. ESG recipients and subrecipients are required to provide a federal right of access to records in accordance with 2 CFR 200.336. Section(b) specifies that "[o]nly under extraordinary and rare circumstances would access include the review of true names of victims of crime." To make the intent exceedingly clear, Section 200.336(b) also specifies that routine monitoring does not rise to the level of an extraordinary or rare circumstance, and that where access to crime victim names is actually necessary, it must be accompanied by protective measures, and (absent a court order or subpoena) be approved by the head of the federal awarding agency or delegate. The VAWA, FVPSA, and VOCA requirement of extraordinary protections for victim identifying information is completely consistent with the Section

200.336(b) requirement of heightened protection for crime victim identifying information.

How to Achieve Appropriate Oversight

Appropriate oversight of programs can be achieved through disclosure of aggregate, non-personally identifying information about clients.

VAWA, FVPSA, and VOCA regulations explicitly allow programs to disclose "nonpersonally identifying information, in the aggregate, regarding services to their clients and demographic nonpersonally identifying information in order to comply with federal, state, or tribal reporting, evaluation, or data collection requirements." There are many ways in which a program can accurately report on its activities and participate in routine audits without violating confidentiality and non-disclosure requirements.

The following are specific procedures which address the requirements of confidentiality and the need to report on activities to third parties:

- The program can create a client identifier code or number that can be used on a file and maintained internally to the agency, in such a way that the number itself does not inadvertently identify the client, (i.e. because of initials, date of birth, or other pieces of information that might suggest who the client is). The "key" to the client identifier code would itself be confidential and would not leave the agency. In the circumstance of HUD programs, the Unique Personal Identification Number which is generated within the comparable database could be used with auditors to identify records of services to distinct individuals.
- The oversight organizations can limit the information required to be disclosed by the agency to non-personally identifying aggregate data that describes demographics and services provided, such as age (rather than date of birth) or number of days in shelter.
- Auditors or evaluators might be given access to representative files without any sharing of individual client identifying information by following procedures such as:

    - ✓ Records may be randomly selected by, or with the oversight of, the auditor/evaluator as long as the process does not compromise confidential victim information. For example, an auditor could ask a service provider to review every fourth file on the numeric list of Unique PIN's, and supervise the program's manager while doing so (but not in such a way that the auditor/evaluator could see any client identifying information), and then ask the manager a series of questions about the file which are designed to determine compliance or provision of services and do not seek any client identifying information.

    - ✓ If requested by the auditor/evaluator, the program may provide the auditor/evaluator with a summary sheet of services provided and other relevant information that completely redacts any identifying information. Ideally, redaction should be done by use of electronic pdf redaction programs which remove all metadata and eliminate the risk of insufficient blacking out that can occur with manually using a black marker and a photocopy.

    - ✓ The agency could provide the auditor/evaluator with a file or a portion of a file which has had all client identifying information effectively blacked out (as confirmed by a manager's review of the document). Ideally, redaction should be done by use of electronic pdf

redaction programs which remove all metadata and eliminate the risk of insufficient blacking out that can occur with manually using a black marker and a photocopy.

- ✓ The auditor/evaluator may request access to a checklist or other form that demonstrates that the agency did verify and determine that the client was eligible for program services and that the program performed the services for the client, if the checklist does not include any identifying information.

- ✓ Where there is a suspicion of actual fraud (separate from routine oversight activities), federal oversight authorities can seek a court mandate for disclosure of identifying information as they are able to show it is necessary to determine whether federal funds were misappropriated.

The core goal of any program audit is to assure proper expenditure of the program's funds without impeding the program's delivery of services. The disclosure of personally identifying information is not necessary to meet the goals of an audit, and such disclosure will actually impede the willingness of victims to seek services or to share accurate information while receiving services. Just as importantly, the routine disclosure of victim PII, even for federal grant programs, could jeopardize the continuation of vital federal funding to meet the specific needs of domestic violence, sexual assault, stalking, dating violence, family violence and other violent crime victims. Government and private funders currently conduct successful and appropriate audits of a range of funded entities with strong confidentiality rules (e.g. legal services programs) without resorting to the disclosure of personally identifying information. Victim Service Providers are similarly bound by strong confidentiality rules, and oversight must be conducted without demanding the disclosure of personally identifying information.

Conclusion

The Violence Against Women Act and the Family Violence Prevention and Services Act are designed to protect the safety of adult, youth and child victims of domestic violence, dating violence, sexual assault or stalking and their families; one critical means for doing so is to protect the confidentiality of victim information, in part by restricting the entry of such information into a third-party database that tracks and links personally identifying victim information. If Victim Service Providers participate in such a database, they could be in violation of federal and state laws, and be at risk of losing their federal grant funds.

For further information or technical assistance, please reach out to Monica McLaughlin at mmclaughlin@nnedv.org or Alicia Aiken at aaiken@confidentialityinstitute.org.

The National Network to End Domestic Violence (NNEDV), a social change organization, is dedicated to creating a social, political and economic environment in which violence against women no longer exists.

www.nnedv.org

NNEDV
NATIONAL NETWORK TO END DOMESTIC VIOLENCE

This project was supported by Grant #2015-AX-K009 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.

Domestic Violence and Housing Technical Assistance Consortium

The Consortium, launched in 2015, provides training, technical assistance, and resource development at the critical intersection between domestic violence/sexual assault services and homeless services/housing. Funded by a partnership between the U.S. Department of Justice, the Department of Health and Human Services, and the Department of Housing and Urban Development. This multi-year Consortium supports a collaborative TA Team that includes the National Alliance for Safe Housing (a project of the District Alliance for Safe Housing), the National Network to End Domestic Violence, the National Resource Center on Domestic Violence, and Collaborative Solutions, Inc., to build and strengthen technical assistance to both housing/homelessness providers and domestic violence/sexual assault service providers. The Consortium aims to improve policies, identify promising practices, and strengthen collaborations necessary to enhance safe and supportive housing options for sexual and domestic violence survivors and their children.

More Questions? The Consortium TA Team is available to provide individualized TA and training to communities interested in expanding the array of safe housing options for domestic and sexual violence survivors. We can also provide support to domestic violence and sexual assault advocates, homelessness and housing providers, and other allied partners interested in building stronger community collaborations.

SAFE HOUSING PARTNERSHIPS

Visit **SafeHousingPartnerships.org** to access a comprehensive collection of online resources and to request technical assistance and support.

---

[1] VAWA Section 605: Amendment to the McKinney-Vento Homeless Assistance Act Prohibiting Disclosure of PII in HMIS

42 USC §11363 – Protection of personally identifying information by victim service providers.
In the course of awarding grants or implementing programs under this subsection, the Secretary shall instruct any victim service provider that is a recipient or subgrantee not to disclose for purposes of a Homeless Management Information System personally identifying information about any client. The Secretary may, after public notice and comment, require or ask such recipients and subgrantees to disclose for purposes of a Homeless Management Information System non-personally identifying information that has been de-identified, encrypted, or otherwise encoded. Nothing in this section shall be construed to supersede any provision of any Federal, State, or local law that provides greater protection than this paragraph for victims of domestic violence, dating violence, sexual assault, or stalking.

42 USC §11360 – Definitions.
(16) PERSONALLY IDENTIFYING INFORMATION OR PERSONAL INFORMATION.—The term 'personally identifying information' or 'personal information' means 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—
(I) a first and last name;
(II) a home or other physical address;

(III) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number);
(IV) a social security number; and
(V) any other information, including date of birth, racial or ethnic background, or religious affiliation, that, in combination with any other non-personally identifying information would serve to identify any individual.

(32) VICTIM SERVICE PROVIDER.— The term 'victim service provider' means a private, nonprofit, nongovernmental organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. Such term includes rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.

[2] Section 3 of VAWA 2013 (34 USC §12291) provides, in relevant part:

(A) IN GENERAL. In order to ensure the safety of adult, youth, and child victims of domestic violence, dating violence, sexual assault, or stalking, and their families, grantees and subgrantees under this title shall protect the confidentiality and privacy of persons receiving services.
(B) NONDISCLOSURE.—Subject to subparagraphs (C) and (D), grantees and subgrantees shall not —
(i) disclose 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; or
(ii) disclose, reveal or release individual client information without the informed, written, reasonably time-limited consent of the person (or in the case of an unemancipated minor, the minor and the parent or guardian or in the case of persons with disabilities, the guardian) about whom information is sought, whether for this program or any other Federal, State, tribal, or territorial grant program, except that consent for release may not be given by the abuser of the minor, person with disabilities, or the abuser of the other parent of the minor.
(C) RELEASE.—If release of information described in subparagraph (B) is compelled by statutory or court mandate—
(i) grantees and subgrantees shall make reasonable attempts to provide notice to victims affected by the disclosure of information; &
(ii) grantees and subgrantees shall take steps necessary to protect the privacy and safety of the persons affected by the release of the information.
(D) INFORMATION SHARING.—Grantees and subgrantees may share—
(i) nonpersonally identifying data in the aggregate regarding services to their clients and nonpersonally identifying demographic information in order to comply with Federal, State, tribal, or territorial reporting, evaluation, or data collection requirements;
(ii) court-generated information and law-enforcement generated information contained in secure, governmental registries for protection order enforcement purposes; and
(iii) law enforcement- and prosecution-generated information necessary for law enforcement and prosecution purposes.
(ii) In no circumstances may –
(I) an adult, youth, or child victim of domestic violence, dating violence, sexual assault, or stalking be required to provide a consent to release his or her personally identifying information as a condition of eligibility for the services provided by the grantee or subgrantee;
(II) any personally identifying information be shared in order to comply with Federal, tribal, or State reporting, evaluation, or data collection requirements, whether for this program or any other Federal, tribal, or State grant program.

[3] Family Violence Prevention and Services Act, Confidentiality section 42 USC 10406(c)(5)
42 USC 10406(c)(5) provides:
(c) Grant conditions…
(5) Nondisclosure of confidential or private information.
(A) In general. In order to ensure the safety of adult, youth, and child victims of family violence, domestic violence, or dating violence, and their families, grantees and subgrantees under this title [42 USCS §§ 10401 et seq.] shall protect the confidentiality and privacy of such victims and their families.
(B) Nondisclosure. Subject to subparagraphs (C), (D), and (E), grantees and subgrantees shall not--

(i) disclose any personally identifying information collected in connection with services requested (including services utilized or denied), through grantees' and subgrantees' programs; or

(ii) reveal personally identifying information without informed, written, reasonably time-limited consent by the person about whom information is sought, whether for this program or any other Federal or State grant program, which consent--

(I) shall be given by--

(aa) the person, except as provided in item (bb) or (cc);

(bb) in the case of an unemancipated minor, the minor and the minor's parent or guardian; or

(cc) in the case of an individual with a guardian, the individual's guardian; and

(II) may not be given by the abuser or suspected abuser of the minor or individual with a guardian, or the abuser or suspected abuser of the other parent of the minor.

(C) Release. If release of information described in subparagraph (B) is compelled by statutory or court mandate--

(i) grantees and subgrantees shall make reasonable attempts to provide notice to victims affected by the release of the information; and

(ii) grantees and subgrantees shall take steps necessary to protect the privacy and safety of the persons affected by the release of the information.

(D) Information sharing. Grantees and subgrantees may share--

(i) nonpersonally identifying information, in the aggregate, regarding services to their clients and demographic nonpersonally identifying information in order to comply with Federal, State, or tribal reporting, evaluation, or data collection requirements;

(ii) court-generated information and law enforcement-generated information contained in secure, governmental registries for protective order enforcement purposes; and

(iii) law enforcement- and prosecution-generated information necessary for law enforcement and prosecution purposes.

[4] Victims of Crime Act (VOCA) (42 USC §10601 *et. seq*) regulations at 28 CFR 94.11

Non-Disclosure of Confidential or Private Information

(a) Confidentiality. SAAs and sub-recipients of VOCA funds shall, to the extent permitted by law, reasonably protect the privacy and confidentiality of persons receiving services of persons receiving services under this program and shall not disclose, reveal, or release, except pursuant to paragraphs (b) and (c) of this section

(1) Any personally identifying information or individual information collected in connection with VOCA-funded services requested, utilized, or denied, regardless of whether such information has been encoded, encrypted, hashed, or otherwise protected; or

(2) Individual client information, without the informed, written, reasonably time-limited consent of the person about whom information is sought, except that consent for release may not be given by the abuser of a minor, incapacitated person, or the abuser of the other parent of the minor. If a minor or a person with a legally appointed guardian is permitted by law to receive services without a parent's (or the guardian's) consent, the minor or person with a guardian may consent to release of information without additional consent from the parent or guardian.

(b) Release. If release of information described in paragraph (a)(2) of this section is compelled by statutory or court mandate, SAAs or sub-recipients of VOCA funds shall make reasonable attempts to provide notice to victims affected by the disclosure of the information, and take reasonable steps necessary to protect the privacy and safety of the persons affected by the release of the information.

(c) Information sharing. SAAs and sub-recipients may share—

(1) Non-personally identifying data in the aggregate regarding services to their clients and non-personally identifying demographic information in order to comply with reporting, evaluation, or data collection requirements;

(2) Court-generated information and law-enforcement-generated information contained in secure governmental registries for protection order enforcement purposes; and

(3) Law enforcement- and prosecution-generated information necessary for law enforcement and prosecution purposes.

(d) Personally identifying information. In no circumstances may—

(1) A crime victim be required to provide a consent to release personally identifying information as a condition of eligibility for VOCA-funded services;
(2) Any personally identifying information be shared in order to comply with reporting, evaluation, or data-collection requirements of any program;