

# SSVF Domestic Violence Guidance for HMIS Reporting

## **What is the policy on entering information about SSVF participants who are victims of domestic violence into HMIS?**

Only programs whose primary mission is to serve victims of domestic violence are prohibited by VAWA from entering client data into HMIS. All other SSVF grantees are required to collect and enter data for 100% of SSVF participants into HMIS. Grantees who perceive this SSVF requirement to be in conflict with state law, local law, or local HMIS policy must contact regional coordinators with documentation of the specific law and/or policy. VA will review and, when possible, take additional action to facilitate the entry of this data into HMIS. If there is any doubt about a conflict, grantees should contact regional coordinators immediately rather than waiting until a participant with a history of domestic violence requests SSVF assistance.

## **Why does VA require grantees to enter information about victims of domestic violence into HMIS?**

National-level counts of SSVF participants and tracking of outcomes are based on HMIS data. Only clients for whom data is entered into HMIS and successfully uploaded to the Repository can be counted by VA as having been served by your program.

## **What steps can grantees take to ensure the security of HMIS data?**

It is the responsibility of the grantee to take precautions to protect the client information of all of those served. Information in HMIS tends to be more secure than information in paper files. There are basic information security practices that you should follow to keep all personally identifying information secure:

1. Protect any computer that stores or accesses identifying information about any client – which includes accessing HMIS or data exported from HMIS for upload to the Repository – with a username and password.
2. Do not share the username and password for your computer or your HMIS account with anyone, and don't keep them written down in a place where anyone else could find them.
3. Log out or lock your computer when you are not at your desk.
4. The only VA-approved method of transmitting exported HMIS data for SSVF clients is by upload to the Repository; exported files may not be emailed.

## **Are there special safeguards grantees can implement for data related to victims of domestic violence?**

If there is reason to believe that an abuser has or could gain access to HMIS data, contact your regional coordinator, who will work with you to develop a plan to enter data without compromising your participant's safety; it may be appropriate to delay data entry until after the participant has been discharged. In addition, although data required by VA for SSVF participants does not include an address or other contact information, some HMIS applications have the capacity to track such data, as well as information about employers, etc. In instances where there is reason to believe that an abuser may have access to HMIS data, none of that additional information should be entered into HMIS.