Supportive Services for Veteran Families (SSVF)

The SSVF Program Guide describes requirements and expectations of confidentiality with regard to client information, which is critical. The security and the safety of client information is important and can help establish trusting relationships between service providers and their clients. Protecting such information can be seen in the care provided in the storage of client information recorded in a physical means. Paper files are typically stored in a locked filing cabinet or archived in a secure location. They are then destroyed when the information they provide is no longer necessary through an established procedure. However, as more programs move to electronic documents, it is important to avoid any gaps between the storage, maintenance, and other oversight procedures that must be put into place to secure personal information. While the baselines established in the Homeless Management Information System (HMIS) Data and Technical Standards are a starting point, they do not reflect a mobile office and outreach role where client information might be obtained on-site and not be immediately available to enter into the HMIS.

To better understand the possible gaps that may exist in the protection of electronic client information, the SSVF Program Office would like for grantees to assess their programs with the following questions. If the answer to any of these questions is "No", please revisit existing Policies and Procedures regarding information security to ensure the protection of client information.

Item	Description	Yes	No
1	Does the Grantee have records of their systems that may be used in the storage and/or transmittance of client data? (Serial #, Model, Manufacturer)	◯	◯
2	Does the Grantee have an accurate method to track who is maintaining possession of each asset used in the storage and/or transmittance of client data?	◯	◯
3	Is there a policy in place to certify the destruction of client information stored on a Grantee's asset once it has been inputted into an HMIS?	◯	◯
4	When an asset that may be used in the storage and/or transmittance of client data is not currently in use, is it protected through a locking mechanism such as by logging out or a password protected screensaver? [HMIS Data and Technical Standards 2004 3.4.1]	◯	◯
5	When client information is accessed or inputted on a Grantee's electronic asset is it done in such an area so that no passer-by may be able to glean information and are measures in place to help limit this possibility?	◯	◯
6	Are systems that store and/or transmit client information and that may also be easily removed from the premises secured in a manner when not in use to prevent theft?	◯	◯
7	Do systems that are taken off-site and used in the storage and/or transmittance of client information have some form of volume encryption to protect client information if lost, misplaced, or stolen?	◯	◯
8	Is there policy in place by the Grantee to deal with managing access rights when dealing with the hiring/firing process of staff and the associated outcomes?	◯	◯