

Privacy and Data Security Plan

The following template should be used to elaborate the Privacy and Data Security Plan.

VA Sensitive Information (SI) includes data, in any format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration or destruction. SI includes, but not limited to, individually identifiable medical or health data. Properly de-identified data records are not considered to be SI. The data security plan should address the following elements.

1. The particular SI that will be used in this study [i.e., Describe SI data elements].
2. How the SI in this study will be used [i.e., Describe purpose of using SI].
3. SI will be used by approved study personnel.
4. In the event of a real or suspected breach of security, the VA Police, the VA Information Security Officer, and the VA Privacy Officer will be notified.
5. SI will be accessed, stored, and destroyed according to a data security plan that will promote security and privacy. [i.e., Describe the data security plan].

Suggested elements of data security plan:

Hardcopy stored in the VA: Hardcopy SI will be stored in the investigator's laboratory in a locked cabinet and destroyed by [state who is responsible] at [state date or "the end of the study"]. Only approved study personnel [and add study monitor identification here if appropriate] will have access to this information.

Electronic SI in the VA secure network: SI will be stored electronically within the VA secure network and accessed only by approved study personnel [and add study monitor identification here if appropriate] using VA secured workstations.

Electronic de-identified data storage in any computer: Study records entered into a computer system [or on electronic media] will be assigned code numbers and will not be individually identifiable. The key that relates the code numbers to the individuals will be kept in a locked cabinet in the research team's office and destroyed at [state date or "the end of the study"].

Electronic SI in a stand-alone computer in the VA: SI will be stored in a stand-alone (non-networked) computer system that is maintained in a locked office within the VA, protected by strong passwords, and accessible only by approved study personnel. This system will not leave the protected VA environment unless the data storage components are removed or destroyed.

SI removed from VA [e.g., sent to sponsor or collaborator]: SI will be sent to [List recipients] for the purposes of [describe use of the data]. The data will be sent by [describe secure method of transmission including encryption method if digital]. The information that is sent will be destroyed [describe method of destruction, date, and responsible party].

If there is a HIPAA waiver and SI is removed from the VA: An approved Authorization to transport and utilized VA sensitive information outside protected environments will be utilized for any SI that is removed from the VA protected environment in any format. A Data Use Agreement (DUA) between the VA and [recipient institution] will be utilized and approved by the VA. The DUA indicates [describe data elements to be removed, how the data will be used and disclosed, and the safeguards in place to prevent other uses or disclosures]. The DUA prevents the recipient from identifying or contacting the individual subjects and holds the recipient to conditions of the DUA.

If there is a HIPAA waiver and SI is stored in a computer not on the VA secured network: The sensitive information will reside in a non-VA server at [recipient institution] that has been certified and accredited as required by the 2002 FISMA act.