

ISO Data Security Checklist for Research Protocols

DATE	Name and Number of Protocol		
Name of PI	PI Telephone number and Email address		
VA Storage Checklist <input type="checkbox"/>	Resources ISO Name, Email address and phone: Lucy M. Fleming, lucy.fleming@va.gov , 410-605-7141		
NON VA Storage Checklist <input type="checkbox"/>	Privacy Officer Name, Email Address and phone: Janice H. Crosby, Janice.crosby@va.gov , 410-605-7328		

Instructions: If the research does NOT include any VA sensitive information/data, Specific Requirements 1 and 2 should be marked as not applicable (N/A).

To check boxes electronically, please double click the boxes below. This will open up a dialogue box, allowing you to change the default value to Checked.

#	YES	NO	N/A	Specific Requirement
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Only paper documents will be maintained in conjunction with this protocol.
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All electronic VA sensitive research information is used and stored behind the VA firewall.
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All copies of electronic VA sensitive research information are used and remain within the VA.

VA Storage Checklist

#	YES	NO	N/A	Specific Requirement
Administrative				
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Permission to remove the data has been obtained from 1) Your immediate supervisor, 2) your ACOS/R&D, 3) the VA Information Security Officer (ISO), and 4) the VA Privacy Officer (PO).
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Access to the data is only by those who are authorized to access it and the access is related to the VA-approved research.
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Procedures for reporting theft or loss of sensitive data or the media such as a laptop, containing sensitive data are in place and familiar to the researcher and all others who have access to use, store, or transport the data.
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Are provisions to protect the confidentiality of data, including derived data from research subjects, adequate?
Equipment				
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A VA property pass for the equipment (Laptop, other portable media device, etc.) has been obtained.
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The VA laptop or other portable media device is VA encrypted and VA password protected. NOTE: Contact the VA ISO at your facility for encryption issues.
Transmission and Storage				
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	VA sensitive data are transmitted only as attachments to protected e-mail messages (PKI).
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Names, addresses, and social security numbers (real & scrambled) have been replaced with a code. NOTE: Names, addresses, & social security numbers (real or scrambled) may only be maintained on a VA server and documentation of the procedure by which the data were coded must remain in the VA.
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Data sent via regular mail or delivery service have been encrypted. NOTE: It is preferable to send data on CD's or other media by a delivery service where there is a "chain of custody."
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	For VA data that will reside on a non-VA server: The server has been certified and accredited as required by Federal Information and Security Management Act (FISMA) of 2002 or a signed/approved MOU with the organization is in place. Your facility ISO may be consulted.
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Will release of data be performed in accordance with VHA regulations and policies?
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	How long will the data be kept? How will it be destroyed?

DATE	Name of Protocol
	Comments:
ACCEPTANCE / REQUEST FOR MORE INFORMATION	
<input type="checkbox"/> I have reviewed the research protocol and certify that data security protections are adequate and the research is in compliance with VHA data security requirements.	
<input type="checkbox"/> I have reviewed the research protocol and find that data security protections are not adequate and recommend the following actions in order for the research to be in compliance with VHA data security requirements.	
ISO Name and Signature:	Date:
Privacy Officer Name and Signature	Date:

Information About VA Cyber Security and Privacy Policies

Information about VA's cyber security and privacy policies as they pertain to the conduct of human research can be found in the documents listed below:

- [VHA Handbook 1200.5 - Requirements for the Protection of Human Subjects in Research](#)
- [VHA Directive 2007-040 - Appointment of Facility Information Security Officer \(ISO\) and Privacy Officer \(PO\) to the Institutional Review Board \(IRB\) or the Research & Development \(R&D\) Committee](#)
- [VHA Handbook 1605.1 – Privacy and Release of Information](#)
- [VA Handbook 6500 – Information Security Program](#)
- [VA Directive 6502 – Privacy Program](#)
- [VA Handbook 6502.1 – Privacy Violation Tracking System \(PVTs\)](#)
- [VA Handbook 6502.2 – Privacy Impact Assessment](#)
- [VA Directive 6502.3 – Web Page Privacy Policy](#)
- [VA Directive 6102 – Internet/Intranet Services](#)
- [VA Handbook 6102 – Internet/Intranet Services](#)
- [VA IT Directive 06-2, Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations](#)
- [VA Handbook 5011/5 – Hours of Duty and Leave \(Telework\)](#)
- [VA Directive 6212 – Security of External Electronic Connections](#)
- [VHA Directive 2004-002 – The Use of Commercial or External Web Hosting Services for VHA Websites](#)

Definitions

Data Use Agreement (DUA): *Primarily needed if using data from another source.*

The VA is the data owner and the investigator needs to use the VA data. The investigator will then be the custodian of the data while the study is open. It describes the responsibilities of the data custodian. Some conditions include (1) Disclosure of data in a "limited data set", (2) Disclosure is for research purposes, (3) Individual authorization is not obtained as part of an IRB-approved protocol.

Data Transfer Agreement (DTA): *Put in place for any non-routine transfer of data*

Data agreements should be completed for all transfers that your facility or department makes to other VHA organizations. For example, the VISN data mart gets automated feeds from a data warehouse. In this example the data warehouse would effect the agreement since they are sending the data to the VISN.

Memorandum of Understanding (MOU): *Document outlining responsibilities between parties*

A written agreement between data owner and data custodian detailing what is expected between each party. This can include support, interconnectivity, data handling, and data access.

Certified and Accredited System in accordance with FISMA:

VA Data needs to be protected in compliance with federal standards. VA Directive 6500 includes the standards that data must be protected to ensure confidentiality, integrity, and availability. These standards include the managerial, technical and operational controls necessary to control access to VA data.

VA Sensitive Information:

In accordance with VA Directive 6504 VA sensitive (research) information is defined as: data that require protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration or destruction of the information. The term includes

- (1) information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission,
- (2) propriety information,
- (3) records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and
- (4) information that can be withheld under the Freedom of Information Act (FOIA). Health information de-identified in accordance with VHA Handbook 1605.1 Appendix B would not be considered sensitive information.