

Appendix C

Data Security Checklist for Principal Investigators

Date:

Name of Protocol:

Name of PI:

PI's Phone Number and e-mail address:

Name of Privacy Officer (PO): *Quin Denton*

PO's Phone & e-mail address: 205-554-3725; Quin.Denton@va.gov

Name of ISO: *Alicia Marshall*

ISO's Phone Number and e-mail address: 205-554-3652; Alicia.Marshall@va.gov

Instructions: *If you answer NO to any one of the statements, you may not remove or transmit the data outside the VA and you must consult with your supervisor, ISO and Privacy Officer. If the research will not obtain any VA sensitive information/data the statements below should be marked as not applicable (N/A).*

Yes	No	N/A	Specific Requirement
			All VA sensitive research information is used and stored within the VA
			All copies of VA sensitive research information are used and remain within the VA

If you have answered yes or N/A to both statements above, stop here.

If the original or copies of VA research information are removed from the VA the following apply: *See Appendix A for definition of terms used in this document.*

Yes	No	N/A	Specific Requirements
			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.
			A property pass for the equipment (Laptop etc.) has been obtained.
			The laptop or other portable media is encrypted and password protected. Note: <i>Contact the VA ISO at your facility for encryption issues.</i>
			Data are not transmitted as an attachment to unprotected e-mail messages.
			Names, addresses, and Social Security Numbers (real and scrambled) have been replaced with a code. Note: <i>Names, addresses, and 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 within the VA</i>
			Data sent via mail or delivery service have been encrypted. Note: <i>It is preferable to send data on CDs or other media by a delivery service where there is a "chain of custody".</i>
			For data that will reside on a non-VA server: The server has be certified and accredited as required by Federal Information and Security Management Act of 2002 (FISMA). Note: <i>your facilities ISO should be consulted.</i>
			Access to the data is only by those who are authorized to access it and the access is related to VA-approved research.
			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.

Appendix D

Principal Investigator's Certification: Storage & Security of VA Research Information

Instructions:

- 1. This certification must be completed by all Principal Investigators (PI) and submitted to their facility's ACOS/R&D no later than April 15, 2007. It must also be completed and submitted to the ACOS/R&D by April 15th annually thereafter. If you are PI on more than one research protocol, you may a) complete a form for each protocol, b) list additional protocols and date of R&D approval on the bottom of this form, or c) attach a separate list.*
- 2. This form must be completed for each new protocol and a copy of this form must remain with the research protocol file.*
- 3. This form must be submitted to ORD during the Just-In-Time process if you will be funded by ORD for a research project.*

I certify to the best of my knowledge that all VA sensitive information associated with the research study entitled _____ and approved by the Research and Development Committee on _____ is being used, stored and security in accordance with the applicable VA and VHA policies and guidance.

Name: _____
(Print Name and signature required)

Title: _____

Date: _____

Phone: _____

E-mail: _____