



**Department of Veterans Affairs
Jesse Brown VA Medical Center
820 S. Damen Avenue
Chicago, IL. 60612**

R&D 537/151
November 24, 2009
Version 1.0
Revised April 7, 2011

**SOP: Review of Research
Documents for Compliance with
Information Security
Requirements**

PURPOSE

To describe the responsibilities of the Information Security Officer (ISO) regarding the review of research documents for compliance with all applicable local, VA, and Federal requirements regarding information security, and to describe the procedures for conducting and documenting the review of the research documents.

POLICY

In accordance with VHA policy, the ISO serves as an Ex-Officio member of the IRB. In addition, the ISO is also an Ex-Officio member of the R&D Committee.

RESPONSIBILITIES

The ISO is responsible for:

- a) Ensuring the proposed research complies with all applicable local, VA and other Federal requirements for information security, by identifying, addressing, and mitigating potential concerns about proposed research studies, and by serving in an advisory capacity to the IRB and R&D Committee as a nonvoting member.
- b) Reviewing the proposed study protocol and any other relevant materials submitted with the IRB application. [**NOTE:** *It is not sufficient for the ISO to review a checklist completed by the investigator, and not the study protocol and related materials themselves.*]
- c) Completing a review of the proposed research and informing IRB of all their findings related to information security. [**NOTE:** *The ISO is not responsible for approving or disapproving a study, nor does the ISO have the authority to prevent or delay IRB approval of a study.*]
- d) Identifying specific deficiencies in their review of the proposed research, and making recommendations to the options available to correct the deficiencies.
- e) Ensuring the proposed research is in compliance with relevant information security requirements, respectively, before the investigator initiates the study.

- f) Providing summary reports of their review and assessment of each study. The summary report must clearly:
 - (1) Indicate either that all applicable local, VA and other Federal requirements for information security have been met, or
 - (2) Identify specific deficiencies and suggest available options for correcting those deficiencies.
- g) Providing their summary reports on each study to the Collaborative IRB staff within a time frame that does not prolong the study approval process. They must provide their summary reports prior to the convened IRB meeting at which the study is to be reviewed or, in the case of expedited review, prior to the IRB approval determination of the IRB Chair, or designee. For exempt studies, they must submit their summary reports to both ACOS for R&D and the Collaborative IRB, and ensure the study is in compliance before the study is initiated.
- h) Providing their final reports on each study to the R&D Office and the Collaborative IRB staff in a timely manner.

PROCEDURE

1. Research submissions including but not limited to, initial review, continuing review, amendments, and final reports, will be submitted to the R&D Office for review by the ISO prior to submission to the IRB. All research submissions are submitted to the R&D Office prior to the submission to the IRB regardless of whether the submission will be reviewed by the Convened IRB, via Expedited Review, or as a Claim of Exemption.
2. The ISO will conduct a review of the proposed study protocol and any other relevant materials submitted with the IRB application.
3. The ISO will provide an initial summary report of their review. The initial summary report will either a) indicate that all applicable local, VA and other Federal requirements for information security have been met, or b) identify specific deficiencies and suggest available options for correcting those deficiencies.
4. The ISO will provide a copy of their initial summary report for each research submission to the Human Subject Research Specialist or designee. The Human Subject Research Specialist or designee cannot sign and release the JBVAMC IRB Protocol Submission Checklist until both the ISO and the Privacy Officer have completed a review of the submission and have provided copies of their initial summary reports.
5. After the Human Subject Research Specialist or designee signs and releases the JBVAMC IRB Protocol Submission Checklist, including copies of the ISO's and Privacy Officer's initial summary reports, the investigator submits the research submission to the IRB. The IRB considers the ISO's and Privacy Officer's initial summary reports to be a part of the research submission.
6. The ISO attends the Convened IRB meetings as an Ex-Officio member of the IRB, and provides any additional comments regarding the research submissions.
7. Any issues raised by the ISO, whether on the initial summary report or during the Convened IRB meetings, are communicated to the investigators as part of the IRB correspondence. The ISO receives a copy of all communications sent to the investigators by the IRB.

8. The Collaborative IRB staff will contact the ISO to request a review of all changes that affect information security in any manner including, but not limited to responses received from investigators, complaints and serious and/or continuing non-compliance. Whether or not further review is required by the ISO is determined on a case-by-case basis by the Collaborative IRB staff with the assistance of the Collaborative IRB co-chairs as needed. If further review by the ISO is required, the Collaborative IRB staff will coordinate the review process with the ISO including making the protocol files available for review.
9. Once all of the items raised by the IRB and the ISO are satisfactorily addressed, the research receives IRB approval or Exemption determination. The ISO receives a copy of the IRB approval or Exemption determination that is sent to the investigator. Following IRB approval or Exemption determination, the ISO will provide a final summary report to the R&D Office in a timely manner. The R&D Office will ensure that a copy of the final report is sent to the UIC VA Liaison and/or Collaborative IRB staff.
10. After the R&D Office receives a copy of the IRB approval or Exemption determination letter, the ISO final report, and the Privacy Officer final report, the ACOS/R&D Committee performs a review of the research. Only after the ACOS/R&D Committee approval letter is sent to the investigator may the research be initiated at the JBVAMC.
11. The ISO is also an Ex-Officio member of the R&D Committee. Any issues raised to the IRB by the ISO and/or by the IRB to the ISO may be further discussed at the RDC meeting.

REFERENCES

VHA Directive 2007-040

VA Directive 6500

VA Handbook 6500

VHA Handbook 1200.05

VHA Handbook 1200.01

Appendix A

Data Security Checklist

Date	8/31/09 <i>(Checklist Reviewed on 10/5/09) ISO File in R&D on 5/21/08</i>
Name of Protocol	
Name of PI	
PI's Telephone Number and E-mail Address	Not available
Name of Privacy Officer (PO)	Kristina Ellis
PO's Telephone and E-Mail Address	Alternate Thomas Beatty
Name of Information Security Officer (ISO)	Jessica Vanbenthuyssen, Facility ISO Maurice Loggins, Secondary ISO
ISO's Telephone Number and E-mail Address	312-569-6652 ISO 1g - - *Maurice.Loggins@va.gov 312 569-6779

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
1	X			All VA sensitive research information is used and stored within the VA
2	X			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:

#	YES	NO	N/A	Specific Requirement
1	X			Permission to remove the data has been obtained from 1) immediate supervisor, 2) your ACOS/R&D, 3) the VA information Security Officer (ISO), and 4) the VA Privacy Officer.
2	X			A property pass for the equipment (Laptop etc.) has been obtained.
3	X			The laptop or other portable media is encrypted and password protected. NOTE: Contact the VA ISO at your facility for encryption issues.
4	X			Data are not transmitted as an attachment to unprotected e- mail messages.
5	X			Names, addresses, and social security numbers (real and scrambled) have been replaced with a code. NOTE: 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 in the VA.
6	X			Data sent via 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".
7			N/A	For data that will reside on a non-VA server: The server has been certified and accredited as required by the Federal Information and Security Management Act of 2002 (FISMA). NOTE: Your facilities ISO should be consulted.
8	X			Access to the data is only by those who are authorized to access it and the access is related to VA-approved research.
9	X			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.
10			N/A	Do you have a laptop computer? If "YES" please identify the location: Is the laptop encrypted? Y N

11			X	Please describe your procedure for safeguarding data: All sensitive data is locked in locked file cabinet when not in use.
----	--	--	---	---