

SOP# HRP 01.13

Version:	2.0	Origin:	1.0
Author:	Jessica Mendoza		
Changes:	Triennial review and updates w 1200.05	New Version #:	2.0
Approved:	Christopher T. Bever, ACOS/R&D Date: 10/25/2011		
File Name:	Information Security Requirements(HRP01.13)2011v.2.0		

INFORMATION SECURITY REVIEW OF RESEARCH PROTOCOLS

OBJECTIVE:

1. To ensure that information security requirements on the collection, storage, access, transmission and destruction of VAMHCS research information have been met prior to initiation of the research project, according to VHA Handbooks 1200.05 and 1605.1.
2. To ensure prompt reporting of incidents related to research information protection according the VHA Handbook 1058.01.

BACKGROUND:

The VA Central Office (VACO) has established rules for protection of data used in and derived from research projects. These rules apply to already existing data (retrieved for the purposes of the research), data created through the research, data repositories, and other uses of and transfer of VA research data.

In compliance with VA mandates, the VAMHCS has named an Information Security Officer (ISO) who reviews research proposals prior to IRB review to ensure that information security requirements have been satisfied before protocols can be initiated at the VAMHCS. The ISO reviews each research proposal to determine what types of data are involved in the research project, where and how the data will be stored or transferred, the risks of security breaches, and other required elements. The ISO also sits on the R&D Committee (RDC) as a consultant for information security matters (non-voting).

In addition, VHA has instituted reporting procedures for noncompliance and other incidents related to research information protection (VHA Handbook 1058.01 [May 2010]). This handbook delineates the reporting requirements for investigators, information security officers, ACOS/R&D, and facility directors.

POLICIES:

Information Security (HRP 01.13) Prior Versions: 1.0	Version 2.0	Review due: 4/14
---	-------------	------------------

- The VAMHCS Information Security Officer (ISO) reviews each research proposal to determine adherence to information security requirements.
- The RDC seeks the ISO's guidance on information security matters.
- The VAMHCS R&D Service, Investigators and VAMHCS institutional officials shall comply with all VHA reporting requirements for incidents related to research information protection.

DEFINITIONS

Comprehensive Institutional Collaborative Evaluation of Research Online (CICERO) –the electronic protocol management system currently used by the UMB IRB.

Individually-identifiable Information (III) – any information, including health information maintained by VHA, pertaining to an individual that also identifies the individual and, except for individually-identifiable health information, is covered regardless of whether or not the information is retrieved by name. III includes a subset of information called “Individually-identifiable Health Information” (IIHI) further defined in 1605.1 par 4.aa.

Network Security Operations Center (NSOC) – the VA central reporting system for privacy events.

Protected Health Information (PHI) – individually-identifiable health information maintained in any form or medium; includes employment records held by a covered entity in its role as an employer. (1605.1 par 4.ss)

VA Data (or VA Information) – Information owned or in the possession of VA or any entity acting for or on behalf of VA.

VA Research Data – consist of information that has been collected for, or used in or derived from the conduct of VA research.

VA Sensitive Information (VASI) – All Department data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under various confidentiality provisions such as the Privacy Act or HIPAA.

RESPONSIBILITIES:

Information Security Officer (ISO)

1. Reviews the documentation of each human research project prior to IRB review, to ensure that information security requirements have been met or identified.

2. Is a non-voting member of the Research & Development Committee (RDC).
3. Processes information security incidents through the NSOC mechanism and VAMHCS procedures.
4. Includes these incidents in ISO reports to the VAMHCS RDC.

Principal Investigator

1. Designs the research protocol with VA information security requirements in mind, or amends their protocols as recommended by the ISO.
2. Completes the “Checklist for Reviewing Privacy, Confidentiality and Information Security in Research” as a component of the protocol submission to the RDC.
3. Complies with the approved research protocol, including the information security components and reporting any incidents according to R&D SOP 01.08., “Reportable Events”

RDC Coordinator

Notifies the ISO when a human research study is submitted for RDC review.

Research Compliance Officer (RCO)

Conducts routine or for-cause audits of investigator adherence to approved procedures for the use, disclosure, storage, transfer and destruction of research-related PHI and III.

ACOS/R&D

Reports incidents related to information protection to the Medical Center Director and other individuals as required by VHA Handbook 1058.01.

PROCEDURE:

1. Review of Research Protocols

- 1.1. All research projects involving human subjects are reviewed by the VAMHCS Information Security Officer to ensure that the information security requirements have been satisfied and to document the findings of the review using the [“Checklist for Reviewing Privacy, Confidentiality and Information Security in Research”](#)
- 1.2. Prior to IRB review of the protocol, the ISO accesses CICERO to review documents, including but not limited to: the [“Checklist for Reviewing Privacy, Confidentiality and Information Security in Research”](#), the study application, Data Use Agreements, contracts, the Informed Consent Form and the HIPAA Authorization if there is one
- 1.3. The ISO will review the “Checklist for Reviewing Privacy, Confidentiality and Information Security in Research” and the research application to determine what information is being collected, how it will be stored, who has access, whether and how it will be transmitted, use of copyrighted software, use of mobile devices, how/if it will be destroyed, and other elements in the Checklist.
- 1.4. The ISO reviews the documents, completes the right side of the checklist, signs and dates the “Checklist for Reviewing Privacy, Confidentiality and Information Security in Research” upon review of the research project

documents. This signed and noted checklist serves as the ISO summary report to the IRB. The ISO's signature may be electronic or a wet signature.

1.4.1. The ISO report is made available to the IRB prior to its review.

1.5. If Information security issues are discerned, the ISO:

1.5.1. notes the issues on the "[Checklist for Reviewing Privacy, Confidentiality and Information Security in Research](#)";

1.5.2. Notifies the RDC Coordinator;

1.5.3. Reports to the IRB any issues regarding information security requirements (see 1.4.1 above).

2. Reportable Events

2.1. Incidents reportable to NSOC: Members of the VAMHCS research community ensure that the following situations are reported to the ACOS/R&D, ISO, PO and Human & Animal Research Protections Officer (HARPO) within 1 hour of becoming aware of the situations below:

2.1.1. Unauthorized access to VA sensitive information, (including unauthorized use, disclosure, transmission, removal, theft, or loss) related to research, including but not limited to protected health information, individually-identifiable private information, and confidential information protected by HIPAA;

2.1.2. Any research-related incident reportable to the Office of Information and Technology (OI&T) NSOC that impacts, inhibits, or compromises network security;

2.1.3. The ACOS for Research must immediately notify the facility Director, the RDC, and any relevant research review committee upon discovering, receiving, or otherwise becoming aware of a credible report of a research information protection incident described in 6.1.1 and 6.1.2 above, and must ensure that the facility ISO and facility PO have also been notified.

2.1.4. Any oral report or notification of an incident described in 6.1.1 and 6.1.2 above must be followed as quickly as possible by a written report

2.1.5. The PI prepares an Issue Brief of the incident when requested.

2.2. Incidents not reportable to NSOC: Members of the VAMHCS research community ensure that the following situations are reported to the ACOS/R&D, ISO, PO and HARPO within 5 days of becoming aware of the situations below:

2.2.1. Any findings of noncompliance related to research information security or privacy by any VA office (other than ORO) or any other Federal or state entity;

2.2.2. Any other deficiency that substantively compromises the effectiveness of the facility's research information protection program;

2.2.3. Any suspension or termination of research (e.g., by the ACOS for Research or other facility official) related to concerns about research information protection.

2.2.4. Within 5 business days of discovering, receiving a credible report of, or otherwise becoming aware of any situation described in 6.2.1-6.2.3 above, the ACOS/R&D must report the situation directly (without intermediaries) to the Medical Center Director, the RDC, and any relevant research review committees, and must ensure that the facility ISO and facility PO have also been notified.

2.3 Investigators must also report incidents involving human participants to the IRB through CICERO.

2.4 Within 5 business days of being notified of them, the Medical Center Director must report the research information protections incidents listed above to the Southern Regional Office (SRO) of the VHA Office of Research Oversight (ORO) with copies to VISN 5, and must ensure that the facility ISO and facility PO have also been notified.

SEE ALSO:

VAMHCS Policy Memorandum	“Privacy Policy & Procedures” (512-136/MAS-021)
VHA Handbook 1058.01	“Research Compliance Reporting Requirements” (May 2010)
Research Service SOP 01.08	“Reportable Events”

COMPLIANCE:

1. The Information Security Officer, the HARPO and/or the Research Compliance Officer (RCO) may conduct retrospective reviews to ensure information security requirements are currently being met. The results of the review will be discussed with the VAMHCS ACOS for Research and Development and/or RDC Chair.
2. Audits may be announced or unannounced.

REFERENCES:

VHA handbook 1058.01	“Research Compliance Reporting Requirements”
VHA Directive 2007-40	Appointment of Facility Information Security Officer (ISO) and Privacy Officer to the Institutional Review Board (IRB) or the Research and Development (R&D) Committee

APPENDIX A

“Checklist for Reviewing Privacy, Confidentiality and
Information Security in Research”

See Research Service website:

http://www.maryland.research.va.gov/research/human/human_subject_forms.asp