

Version Number: 1	Research & Development Policy 151-21	Supersedes Document Dated: N/A
Effective Date: 11/08/2010	Research Information Protection Program (RIPP)	Expiration Date: 11/07/2014

PURPOSE

This policy describes the VA Research Information Protection Program (RIPP) measures that are to be taken by all staff associated with research at the Syracuse, Canandaigua, and Bath VA Medical Centers for the protection of VA research data and/or information (sensitive and non-sensitive) and personal health information (PHI) obtained for research purposes under approved research protocols.

POLICY

It is the responsibility of all VA employees associated with VA research to uphold the standards of information security and privacy as established by the VA for the protection of all research data, including but not limited to, personal health information (PHI). It is the responsibility of all VA researchers, coordinators, and research staff (including Without Compensation (WOC) employees, Interagency Personnel Act (IPA) appointees and individuals with dual appointments) to be familiar with and to comply with existing policies, procedures and directives concerning the protection of human subjects in research and the use and disclosure of individually identifiable information as well as animal and laboratory research data.

DEFINITIONS

Please refer to SOP151-01, Appendix B for Definitions.

ACTION

Practices

All staff associated with research shall protect VA sensitive research data, human research subjects and their PHI, and other VA research information by instituting the following practices:

Anyone involved with research (human, animal and/or cell) shall protect all research information, and associated PHI from human studies, that involve research at this facility. This protection includes the assurance by all investigators and staff that sensitive research data and information, including PHI, are stored in a secure folder on an appropriate VA network server, unless otherwise stipulated in this SOP.

Physical Security

All rooms containing computers with sensitive data must be secured properly and monitored by VA police. Employees must use approved VA computer equipment, and laptops must have encryption that is FIPS 140 compliant. Employees must secure

approval to obtain, use, transfer and store sensitive data as required by VA directives. This may or may not include the use of a Data Use Agreement.

Use and Storage on Non-VA-owned Government Furnished Equipment

All VA sensitive information (including PHI) must be properly sanitized from non-VA-owned Government Furnished Equipment (VAGFE) with methods approved by the Information Security Officer (ISO). VA Information Technology (IT) employees assure that all servers containing VA sensitive data are secure within the VA's control; behind a VA Firewall with access properly controlled; with locked server rack cabinets. Sensitive research data may NOT be stored outside the VA unless applicable permissions have been obtained from the person's supervisor, the ACOS/R&D, the Privacy Officer (PO), the Information Security Officer (ISO) and a waiver has been submitted in accordance with VA Handbook 6500. This includes the storage of VA sensitive research data on non-VA computer systems/servers, desk top computers located outside the VA, laptops, or other portable media.

Data Storage

All sensitive research data, as described in SOP 151-02, Appendix B, are authorized to be stored within the VA and on VA servers. It is critical to note that as of the date of this SOP, there is no identified sensitive animal data at the Syracuse VAMC, as defined in the March 20, 2007 Subcommittee for Animal Studies meeting minutes. This determination is based upon these criteria: Only data that can be linked directly to an individual, or data/results that directly impact and/or link to an individual or population group would be considered sensitive animal data. It is noted that this determination is subject to future changes, and each new VA Animal Component Of Research Protocol (ACORP) undergoes this determination during initial review and subsequent continuing reviews.

If the data are coded, the key to linking the code with the identifiers must also be stored within the VA unless specifically waived in accordance with VA Handbook 6500 and appropriate language exists within the informed consent and HIPAA authorization form.

Sensitive data transferred to a non-VA computer system/server or site must only occur after the required permissions are obtained and the transfer must be in compliance with requirements found in VA Handbook 6500.

If sensitive VA data are authorized to be stored on non-VA systems, the system must meet all requirements set forth in VA regulations and be approved by the VA ISO and Privacy Officer.

Data Encryption

All laptops and portable media used to store Research data and information must be encrypted and only accessible to authorized individuals. Password protection is not adequate. Any offsite equipment must have prior approval with encryption that is FIPS 140 compliant in accordance with VA Handbook 6500.

Storage of all VA sensitive research Information on laptops, other portable media, or personal computers not within a VA health care facility must have prior approval in accordance with the requirements of VA Handbook 6500. Note: The original sensitive data

may not be stored on the hard drives of laptops or portable media regardless of their location within or outside the VA; it must be on a secure drive or server.

Patient and/or Subject Data

Research subjects or veterans names, addresses, and Social Security Numbers (real or scrambled) may only be stored within the VA and on VA servers. If the data are coded, the key to linking the code with these identifiers must also be stored within the VA, unless specifically waived in accordance with VA Handbook 6500 and appropriate language exists within the Informed Consent and HIPAA authorization form.

IRB Oversight

All research protocols that will include the collection, use and/or storage of human subject research information including subject identifiers and PHI that are submitted to the Syracuse VAMC Institutional Review Board (IRB) and to the Research and Development Committee (R&D Committee) for approval must contain specific information on all sites where the data will be used or stored, how it will be transmitted or transported, specifically who will have access to it, and how it will be secured and the length of data storage throughout its life cycle until termination. If copies of the data will be placed on laptops or portable media a discussion of the security measures for these media must be included and approved.

Training Requirements

All research staff (including WOC employees, IPA employees, research coordinators, investigators, laboratory assistants and students) must complete required training for the protection of all research data including sensitive data/information. This training includes completion of *VA Information Security 201 for Researchers* (one-time) prior to the start of a research project.

There are additional VA mandatory trainings [*Information Security Awareness* (annual), *VHA Privacy Awareness Training* (annual)] which must be completed by all VA employees (paid, WOC, IPA, students) as part of their VA appointment and to maintain access to VA IT resources. These trainings are tracked by the individual and their immediate supervisor.

Routine Review of Protocols

Principal Investigators (PIs) are required to submit the *Data Security Checklist for Principal Investigators* for each of their new protocols in research. New studies will not be approved by the R&D Committee and related subcommittee (Institutional Review Board-IRB, Subcommittee for Animal Studies-SAS, Subcommittee on Research Safety-SRS) without a completed *Data Security Checklist for Principal Investigators* and training verification of *VA Information Security 201 for Researchers* completed by all protocol staff. If offsite storage is needed, the PI will need to follow all VA regulations regarding the approval of such offsite storage and/or transfer of data.

All new protocols containing sensitive VA data and their associated checklists are reviewed by the ISO and PO to determine that appropriate security safeguards are in place or if additional ones are required to protect research data and/or patient information. The PO and the ISO must ensure the proposed research complies with all requirements for privacy and confidentiality, and for information security, respectively, by identifying, addressing, and mitigating potential concerns about proposed research studies.

The PO and ISO identify deficiencies and make recommendations to the investigator of options available to correct the deficiencies. They follow up with the investigator to ensure the proposed research is in compliance before the investigator initiates the study. The PO and ISO must provide their summary reports on each study to the 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 will be reviewed or, in the case of expedited review, prior to or at the IRB approval determination of the IRB Chair or designee's action. For exempt studies, the PO and ISO must submit their summary reports to the ACOS for R&D or the Chair of the R&D Committee, and ensure the study is in compliance before the study can be initiated.

At continuing review for all research protocols (human, animal, or laboratory), the PI will certify whether any data security issues have changed or been identified and subsequently will revise and re-submit to the appropriate subcommittee (IRB, SRS, SAS) the *Data Security Checklist for Principal Investigators* with the necessary updates.

Information Security audits will be performed regularly and as needed for cause by the Information Security Officer (ISO). Failure to comply with these policies, procedures and medical center memoranda may result in suspension of research by the Syracuse VAMC R&D Committee and its related subcommittees (IRB, SAS, SRS) and possible other actions as required by the Department of Veterans Affairs.

Prior to Protocol Approval

For investigators preparing a research protocol, access to sensitive data for research purposes shall be restricted to those:

- Individuals named within the research protocol, (or added as staff during the life of the study).
- Individuals who are responsible for oversight of the research program.
- VA investigators who require access to data, which is "preparatory to research" (per VA handbook 1200.12 10(a)) if their activities meet the requirements set forth in VA policies.

Loss and/or Theft Response

The loss or theft of sensitive VA research data/information or portable media such as laptops or personal computers (PCs) is covered in VA Handbook 6500. The VA Research Office will assist you in locating these documents, if necessary. At a minimum the following should occur as soon as it is discovered that there has been a loss:

- Report the loss or theft to security/police officers immediately. If you are in a VA facility, notify the VA Police. If you are on travel or at another institution, notify the security/police officers at the institution such as hotel security, university security, etc. as well as the police in the jurisdiction where the event occurred. Obtain the case number and the name and badge number of the investigating officer(s). If possible obtain a copy of the case report.
- Immediately call or email the following regarding the incident:
 - Your supervisor
 - Your VA Facility's Information Security Officer
 - Your VA Facility's Privacy Officer

- Your VA Facility's Security Officer/VA Police Chief
- You VA Facility's ACOS/R&D, Medical Center Director, or Chief of Staff

Destruction of Data

When destruction of data is required, all VA sensitive data in research must be destroyed according to VA Handbook 6500, and the Guidelines for Media Sanitization, outlined by the National Institute Standard and Technology (NIST) 800-88.

- All paper data which are to be destroyed are placed in the VA shredder containers (locked grey bins) specially marked for disposal.
- Electronic data to be destroyed must be done by a method rendering it unreadable, undecipherable, and irretrievable as outlined in VA's current electronic sanitization procedures. VA IT staff will assist with this process, as necessary.

Information Inquiries

All requests received for research information from outside entities (private citizens, special interest groups, non-VA institutions, etc.) should be discussed with and handled through our local Freedom Of Information Act (FOIA) Officer and the PO. The VHA FOIA Officer has been very involved in providing guidance to local FOIA Officers to interact with him as needed. Involvement of the FOIA Officer and PO will allow development of a coordinated response, particularly in light of HIPAA regulations as well as violent acts against animal researchers in the past few years. The VA considers these requests extremely sensitive, and FOIA Officers and POs will ensure an adequate response that does not place any VA research staff at risk.

Securing VA Research Information when VA Appointment Terminates

It is the responsibility of all VA employees to protect sensitive VA data when the employee resigns or transfers from the Syracuse/Canandaigua/Bath VAMC. Individual investigators or VA employees (compensated by VA or persons appointed under a without compensation (WOC) or Interagency Personnel Agreement (IPA) do not own the data used or obtained by VA investigators for R&D Committee approved research, preparatory to research activities, or data placed in VA Research Data Repositories. These data are VA information and owned by the Administration, Staff Office, or other Agency component that generates or gathers the information to perform statutory responsibilities. For clinical trials the original, completed case report forms are the property of the research sponsor, but VA must retain copies of the case report forms. Patient medical records, III, original notes, documents, and records produced by VA in the course of the protocol are the property of VA.

Research staff will protect all research data including human research data, their PHI, and other VA sensitive information by instituting the following practices when terminating their VA appointment:

- a. Prior to termination the Investigator must submit a page 19 form to R&D staff for the e-PROMISE system.

- b. Investigators needing to store, transfer, or transmit sensitive research data outside the VA should contact the ISO and the Privacy Officer for assistance meeting all required VA regulations including waivers and offsite permission to do so in accordance with VA Handbook 6500, and Medical Center Memorandums (MCMs). If research data are to remain at the Syracuse/Canandaigua/Bath VAMC, the study must be transferred to another VA investigator (with appropriate permissions in place) or closed and stored according to VA regulations.
- c. If data (paper or electronic) (sensitive or non-sensitive) are to be transferred to another VA computer system/server or site this may occur after approval has been obtained from both the Institutional Review Board (IRB) (if applicable) and R&D Committee at the current site and the future VA site by the Investigator. This transfer must have concurrent approval by the ISO, Privacy Officer, (if applicable), ACOS R&D and the Institutional Official (IO) and the transfer must be in compliance with all VA requirements including those found in VA Handbook 6500.
- d. If tissue samples are to be transferred to another VA the PI must obtain approval from the IO, ACOS R&D, and from the VA Central Office of Research and Development and must follow all VA requirements.
- e. All research protocols that include the collection, use and/or storage of research information including subject identifiers and PHI that are submitted to an Institutional Review Board (IRB) and to the R&D Committee for transfer approval must contain specific information on all sites where the data will be used or stored, how it will be transmitted or transported, specifically who will have access to it, and how it will be secured and the length of data storage throughout its life cycle until termination. If copies of the data will be placed on laptops or portable media a discussion of the security measures for these media must be included.
- f. For the loss or theft of sensitive VA research data/information or portable media such as laptops or personal computers (PCs) during a transfer, please refer to the **Loss and/or Theft Response** section noted previously in this SOP.

REFERENCES:

- National Institute Standard and Technology, (NIST) Guidelines for Media Sanitization, 800-88.
- VA IT Directive 06-2, Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations, 2006.
- VA IT Directive 06-5, Use of Personal Computing Equipment, 2006.
- VA IT Directive 06-6, Safeguarding Removable Data, 2006.
- VA Directive 6500, Information Security Program, 2006.
- VA Directive 6502, Privacy Program, 2003.
- MCM 00-ISO-03, Procedures for Virtual Private Network, 2007.
- MCM 00-ISO-05, Removable Storage Media, 2007.
- VA Handbook 6502.1, Privacy Violation Tracking System (PVTs), 2004.
- VA Handbook 6502.2, Privacy Impact Assessment, 2004.

November 2010

VA Handbook 6500, Information Security Program, 2007.

VA Handbook 1200.5, Requirements for the Protection of Human Subjects in Research, 2003.

VHA Handbook 1605.1, Privacy and Release of Information, 2002.

VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information, 2003.

VA Memorandum DUSHOM/CRADO, Certification by Principal Investigators: Security Requirements for VA Research Information, February 6, 2007.

VA Memorandum DUSHOM/CRADO, Research Responsibilities for Protecting Sensitive Information, June 12, 2006.

VA Memorandum PDUSH/CRADO, Cyber Security and Privacy, June 27, 2006.

RESPONSIBILITY: Research and Development Service will be responsible for the content, update, and recertification of this SOP.

IMPLEMENTATION: November 2010

RESCISSION: None - new

RECERTIFICATION: November 2014



BERNADETTE KALMAN, M.D., Ph.D.
ACOS/R&D Service