



Stratton VA Medical Center

R&D Standard Operating Procedure: Data Security and Information Technology (IT) in Research

PURPOSE

This policy describes the Stratton VA Medical Center (VAMC) Information Security (IS) and Privacy measures that are to be taken by all staff associated with research 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 cell data.

DEFINITIONS

- ◆ **VA Sensitive Data** is defined in VA Directive 6500 as “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, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation, such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law, harm, or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.” In regard to Research: Human studies, in general, are viewed as generating or dealing with sensitive data. In most

instances, animal research does not generate sensitive data; however, a risk assessment of the animal study must be done to determine if there is a potential for harm to the VA from unauthorized use or release of the data, in which case the research would become sensitive. For the purpose of this form, DNA and/or genetic information is considered sensitive if it can be used to specifically identify an individual; otherwise, portions of DNA and/or genetic information that would not be enough to specifically identify an individual is not sensitive data.

- ◆ **De-Identified Data** – When information is de-identified in accordance with VHA Handbook 1605.1 Appendix B it would not be considered sensitive information. If data is not de-identified, names, addresses, and Social Security Numbers (real and scrambled) must be replaced with a code if the data is to be shared or transported offsite. Code must remain within the VA. Note: De-identified information is not considered to be individually identifiable; therefore the Privacy Act HIPPA and VA Confidentiality statutes 38 U.S.C. 5701 and 7332 do not apply. It is not possible to de-identify an *entire* DNA sequence; de-identification of DNA and/or genetic information may only be considered accomplished if the isolated section could not be used to identify any single individual.

The following identifiers of the individual or of relatives, employees, or household members of the individual are considered PHI identifiers under HIPAA. Identifiable information includes the following 18 items:

- Names
- Postal addresses
- Dates (directly related to individuals)
- Telephone numbers
- Fax numbers
- Electronic addresses
- Social security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certification/license numbers
- Vehicle identifiers, including license plates
- Name of relatives
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifiers, including fingers and voice prints
- Full face photographic images and any comparable images
- Or any other unique identifying number, characteristic or code.

ACTION

Practices

Research staff shall protect human research subjects, their PHI, and other VA sensitive research data and 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 research data and information, including PHI, is not stored on local hard drives but 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 computer equipment that has 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). Information Resource Management (IRM) 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, the ISO and a waiver has been submitted in accordance with VA Handbook 6500. This includes storage on non-VA computer systems/servers, desk top computers located outside the VA, laptops, or other portable media.

Wireless Access

At this time we do not allow wireless access for researchers. Any future request will require approval from the ISO.

Data Storage

All Research data, to include sensitive data as described on page one (1) titled "Policy," is only authorized to be stored within the VA and on VA servers. If the data is 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.

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

If sensitive VA data is 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.

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

Removable Storage Media

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 140-2 compliant in accordance with VA Handbook 6500. In addition, the equipment must be up to date on the latest anti-viral and software/security.

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.

VA researchers may only use OI&T issued thumb drives to access or store VA information. A thumb drive can be obtained through the ISO office when there is an established need and approval has been granted.

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 is 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 research information including subject identifiers and PHI that are submitted to an 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. These trainings include: *Information Security Awareness (annual)*, *VHA Privacy Awareness Training (annual)*, and *Information Security 201 for Researchers (one-time)*. *Completion of these trainings is required prior to the start of any research project, or within 30-days of employment of any research staff.*

Routine Review of Protocols

Investigators who have an approved research study are required to submit an annual *Data Security Checklist for Principal Investigators* (See Appendix B) on each of their protocols in research. All new protocols and associated checklists are reviewed by the ISO and Privacy Officer to determine that appropriate security safeguards are in place or if additional ones are required to protect research data and/or patient information. New studies will not be approved by the IRB or the R&D Committee without a completed *Data Security Checklist for Principal Investigators*, completed training certificates and a review by the ISO and PO. All reviews by the ISO and PO are documented via e-mail to the HRPP coordinator, who files the correspondence in the investigator's file.

The ISO and PO are appointed ex-officio members of the IRB and attend meetings on a regular basis. Committee request for changes to the original protocol or consent may require a second review by the ISO and PO.

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 at the Stratton VAMC and possible other actions as required by the Department of Veterans Affairs.

Preparatory To Research

Prior to protocol approval, if you are 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.
- Investigators are required to follow guidelines specified in Appendix A.

VA Incident Reporting 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 research office will be able to assist you in locating these documents. At a

minimum the following should occur as soon as it is discovered that there has been a loss:

- Report the loss to your immediate supervisor, ACOS R&D Research and Development, Information Security Officer and Privacy Officer immediately. They will assist you to report the loss or theft to all necessary parties including security/police officers immediately (see Appendix C for specific contact information).
- If loss occurred within a VA health care facility, the VA police must be notified.
- In addition to item (1) above, if you are on travel or at another institution, the security/police officers at the institution such as hotel security, university security etc. must be notified 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.

Destruction of Data

When destruction of data is required, all VA sensitive data in research must be retained or stored for the period of time stated in the applicable Privacy Act System of Records notice, Records Control Schedule (RCS) 10-1, and VA Handbook 6500, and the Guidelines for Media Sanitization, outlined by the National Institute Standard and Technology (NIST) 800-88.

- All paper data which is to be destroyed is done so by being placed in the VA shredder containers (NexCut) 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.

Exiting Research Personnel

Exiting personnel must meet with the ISO and PO for a departing interview. The ISO and PO will ensure that all research paper documents are secure and properly stored in the research archive room. All information system-related property such as keys, ID cards, building passes, thumb drives etc. will be collected. All system accounts of exiting personnel will be revoked. All research records, data, and data repositories will remain at the VA, under VA control. The VA will retain access to all official documents and reports created on VA information systems by exiting personnel. Removal of any data must have approval from institutional officials prior to removal.

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.
- VA Handbook 6500, Information Security Program, 2007.
- VA Handbook 1200.12 Use of Data and Data Repositories in VHA Research
- 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 MCM.

Implementation: July, 2009

RESCISSION: None - new

RECERTIFICATION: June, 2012

Appendix A

To: Stratton VA Investigators:

1) When an individual is interested in writing a protocol and needs to view Protected Health Information (PHI) for the purposes of writing a research protocol they will need to submit the following document to research and the Privacy Officer.



C:\Documents and Settings\vhhaalnrodri\

2. When pre-research PHI data is requested, investigators will need to submit the following form. The only PHI the OIA will release prior to study initiation will be aggregated data.



C:\Documents and Settings\vhhaalnrodri\

3) Investigators who have an IRB approved study that includes a HIPAA Waiver must send a copy of the IRB letter granting permission to seek PHI to the OIA either by fax or as a scanned document.

4). In the future, to request PHI, investigators must use the Data Request Form. It can be found at <http://vaww.visn2.med.va.gov/sp/ia> when completed e-mail it to:

"VISN 2 Data Request"

Mail or fax IRB approval letters to:
VISN 2 Office of Information and Analysis
VA Healthcare Network Upstate NY (VISN 2)
113 Holland Avenue, Building 7
Albany, NY 12208
Fax (518) 626-7333

If you have any questions please contact:
Jessica Capeci , HRPP Coordinator, Research Service at: 518-626-5626
and/or
Toni Smith, Privacy Officer at: 518-626-5603

Appendix B

Data Security Checklist for Principal Investigators

<http://vaww.visn2.portal.va.gov/sites/albresearch/Research%20Forms/Forms/AllItems.aspx?RootFolder=%2fsites%2falbresearch%2fResearch%20Forms%2fData%5fSecurity&FolderCTID=&View=%7b100C8152%2dF532%2d4E5A%2d8967%2d171BF6AF219B%7d>

Network 2 Privacy Policy
Network Memorandum 10N2-103-09
September 4, 2009



Network Privacy
Policy.docx

Appendix C

What to do if a computer, disk, or files with sensitive VA research data is lost or stolen

1) Report the loss or theft to security/police officers immediately

VA Police (518) 626-6750 Detective Ralph Pitcherelle (or any officer on duty)
Ralph.Pitcherelle@va.gov

If at another institution, contact security for that institution as well as police in the jurisdiction where 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.

2) Within one hour, call or email (preferably both)

✓ **Your supervisor**

✓ **Research Office:**

Dr. Kaminsky Laurence.Kaminsky@va.gov
ACOS R&D
(518) 626-5622

or

John Carroll-Barbuto John.Carroll-Barbuto@va.gov
AO R&D
(518) 626-5621

✓ **Privacy officer** Antoinette Smith Antoinette.Smith@va.gov
(518) 626-5603

✓ **ISO** Rosemary Turton Rosemary.Turton@va.gov
(518) 626-6224

✓ **RCO** Linda Rodriguez LindaA.Rodriguez@va.gov
(518) 626-5787