

**Department of Veterans Affairs
Tuscaloosa VA Medical Center**

Human Research Protection Program SOP #10

October 26, 2009

RESEARCH DATA SECURITY AND PRIVACY

1. POLICY

The Tuscaloosa VA Medical Center (TVAMC) Human Research Protection Program (HRPP) is committed to protecting information about our veterans and employees. When individuals who have served our country volunteer to participate in VA research, they entrust us to keep their personal and health information safe.

It is the policy of the TVAMC to ensure the integrity and security of patient health and personally identifiable information and data compiled during the course of doing research within this facility.

This policy establishes procedures that ensure the security of VA research data and the protection of the privacy of VA research participants. The policies and procedures described within this document do not take the place of information contained in other related Tuscaloosa VA Medical Center (TVAMC) policies, such as IRB Policies and Procedures or Automated Information System (AIS) Security Policies. Rather, they work in conjunction with these other policies and procedures in providing guidance for TVAMC employees.

2. RESPONSIBILITIES

Every VHA employee must comply with all applicable Federal privacy and confidentiality statutes and regulations when collecting, using, sharing or disclosing individually identifiable information, which includes sensitive VA research data from the TVAMC administrative records or VA databases (national, regional, or subject specific).

The applicable Federal statutes and regulations are:

- The Freedom of Information Act (FOIA), 5 U.S.C. 552
- The Privacy Act (PA) of 1974, 5 U.S.C 552a
- The VA Claims Confidentiality Statute, 38 U.S.C. 5701
- Confidentiality of Drug Abuse, Alcoholism & Alcohol Abuse, Infection With the Human Immunodeficiency Virus (HIV) and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332
- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 Code of Federal Regulations Parts 160 and 164
- Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705

These six statutes and regulations with the privacy requirements are set forth in VHA Handbook 1605.1, “Privacy and Release of Information,” which establishes guidance on privacy practice and provides VHA policy for the use and disclosure of individually identifiable information, and for individuals’ rights in regard to VHA data. In addition, all TVAMC employees must remain in compliance with applicable confidentiality statutes and regulations when obtaining or disclosing individually-identifiable patient records (VHA Handbook 1200.5) and handle such information as instructed by VA policies. Employees authorized to remove confidential and Privacy Act-protected data from the VA take all relevant precautions to safeguard that data until it is returned or destroyed.

All VA employees must take annual training for VA Information Security Awareness and Rules of Behavior and VHA Privacy Policy.

Anyone involved in VA research must receive annual training in data security. All individuals must be in compliance with all applicable Federal laws, regulations, policies and guidance related to privacy of research subjects, the use and disclosure of individually-identifiable information, and confidentiality, storage and security of research data. Specific requirements are found in:

- VA Directive 6500, “Information Security Program”
- VA Directive 6502, “VA Enterprise Privacy Program”
- VA IT Directive 06-02, “Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations”
- VA IT Directive 06-06, “Safeguarding Removable Media”
- VHA Handbook 1200.12, “Use of Data and Data Repositories in VHA Research”
- VHA Handbook 1605.1, “Privacy and Release of Information”
- VHA Handbook 6500, “Information Security Program”

The TVAMC Medical Center Directors has ultimate responsibility for ensuring the security and confidentiality of sensitive VA research data in their facilities. On an annual basis (May 15 yearly), the medical center Director must certify to his/her VISN Directors that all principal investigators have met the certification requirements related to storage and security of sensitive VA research data.

TVAMC HRPP and Research and Development (R&D) Committee must assure the security and confidentiality of sensitive VA research data, and the privacy of VA research subjects, by verifying the principal investigator’s (PI) certification checklists (Appendix C and D of VA Memo February 6, 2007). The R&D Committee also has responsibility for ensuring that all investigators and everyone else involved in research at the TVAMC are appropriately trained, credentialed and has research privileges and/or scopes of practice consistent with education, training and expertise. The R&D Committee is responsible for reviewing and evaluating all its subcommittees’ decisions, including IRB approval or exemption, before approving a research protocol.

TVAMC Institutional Review Board (IRB) is responsible for protecting the rights and welfare of subjects. The TVAMC IRB will not approve a protocol unless its data management plan includes certification from the investigator that the use, storage and security of all research information collected for, derived from, or used during the conduct of the research is in compliance with all relevant requirements.

Principal Investigators are responsible for submitting a plan to the IRB and R&D Committee for maintaining privacy of research subjects and confidentiality of sensitive VA research data that includes all applicable information (i.e. storage provisions, security measures, transportation or transmission methods, provisions for controlling access to the data, encryption methods, plans for how long identifiable information or linkages will be kept, provisions for disposition of the data at the end of the study, in accordance with the current record control schedule). For all new research protocols, the principal investigator must certify that the use, storage and security of all information collected for, derived from, or used during the conduct of the research will be in compliance with all VA and VHA requirements. This will require that the PI complete two forms, the “*Data Security Checklist*” and the “*Principal Investigator’s Certification: Storage & Security of VA Research*” for each new protocol, submit them to the IRB and R&D Committee and retain a copy of each of these forms with the study’s regulatory documents. For Just-In-Time review, the PI must submit the “*Principal Investigator’s Certification: Storage & Security of VA Research*” form to the Office of Research and Development (ORD) during the Just-In-Time process for the proposal to be considered for VA research funding. *Note: If, at any point in a study, the PI determines that the security or confidentiality of data being maintained on non-VA systems or otherwise outside the VA on portable equipment does not meet VA requirements, the PI is responsible for immediately ensuring that the data are returned to reside within the VA firewall.*

The TVAMC Information Security Officer is responsible for reviewing and, when appropriate, approving PIs’ requests for storing or transmitting VA research data outside the VA, providing help for local R&D office and investigators in completing the certification checklist requirements, coordinating requests for remote access within their region and facility, reviewing all policies and procedures pertaining to transportation, transmission, remote access and use of VA IT equipment, and ensuring that remote access accounts are immediately disabled for all persons no longer requiring remote access.

The TVAMC Privacy Officer is the authoritative source for privacy within VHA and is responsible for developing and implementing a VHA Privacy Program; developing, issuing, reviewing and coordinating privacy policy for VHA in conjunction with policy efforts by VA; coordinating requirements and monitoring compliance with all Federal privacy law, regulations and guidance within VHA; and issuing direction on VHA privacy policies, practices and activities to the field. Specifically, the TVAMC Privacy Officer is responsible for ensuring the facility’s overall compliance with privacy policies and requirements, ensuring the facility has a process to review all IRB-approved VA research for compliance with privacy requirements prior to the data’s being provided to the principal investigator, reporting incidents regarding protected health information (PHI) to the Privacy Violation

Tracking System and participating in the investigation of such incidents, and ensuring all employees are trained on privacy annually.

3. DEFINITIONS

- a. **Sensitive VA research data** consist of information that has been collected for, used in or derived from the conduct of VA research which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information.

For purposes of the VA Data Security Checklist for Principal Investigators (Appendix C and D of VA Memorandum, February 6, 2007, "Certification by Principal Investigators: Security Requirements for VA Research Information"), sensitive VA research data is defined at the Tuscaloosa VA Medical Center as data that contains personal identifiers (one of the 18 identifiers listed by HIPPA).

- b. **VA Protected Health Information (PHI)** is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information.
- c. **De-Identified Data** is health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. VHA would consider health information no longer protected health information (PHI) if it has been appropriately de-identified in accordance with the HIPAA Privacy Rule as outlined in VHA Handbook 1605.1, Appendix B. For protected health information to be de-identified, all of the following 18 types of identifiers must be removed:

1. Names or initials
2. All geographic subdivisions smaller than a state
3. All elements of dates except the year and all ages over 89
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security Numbers (or scrambled Social Security Numbers)
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and license plate numbers
13. Device identifiers and serial numbers
14. URLs

15. IP addresses
16. Biometric identifiers, including finger and voice prints
17. Full-face photographs and any comparable images
18. Any other unique identifying number, characteristic or code, unless otherwise permitted by the Privacy Rule for re-identification

HIPAA identifiers also pertain to the person's employer, relatives, and household members. Along with removing the 18 identifiers, HIPAA also states that for the information to be considered de-identified, the entity does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify an individual who is the subject of the information.

According to the Common Rule, de-identification involves removal of all information that would identify the individual or would be used to readily ascertain the identity of the individual.

Note: For VA research purposes, VA research data are considered to be "de-identified" only if they meet the de-identification criteria of BOTH HIPAA (i.e., removal of all 18 identifiers) AND the Common Rule.

d. **Limited Data Sets**

The use of limited data sets does **not** require HIPAA-Compliant authorization or a waiver of HIPAA-Compliant authorization, but does require a data use agreement (DUA) or Data Transfer Agreement (DTA). Their use is only allowed for research, public health, or health care operations. Limited data sets have the following characteristics:

They exclude certain direct identifiers that apply to

- The individual
- The individual's relatives
- The individual's employers
- The individual's household members

They may contain

- City, state, ZIP code
- Elements of a date and other numbers
- Characteristics or codes not listed as direct identifiers
- Identifiable information, such as scrambled Social Security Numbers (SSNs)

e. **Coded Data:** Coding consists of labeling information with a code that

- Does not include any patient identifiers (18 HIPAA identifiers)
- Is not derived from or related to the 18 HIPAA identifiers
- Cannot be translated so as to identify the individual. Thus, initials, Social Security Numbers (SSNs) and so on may not be used as codes, even in partial or scrambled form.

Codes provide a link by which identities can be accessed through a key held separately from the coded data. For example, the code might be a barcode or a combination of random numbers and letters. If sensitive VA research data are coded, the key to linking the code with these identifiers must be stored within the VA and on VA servers.

- f. **Nonsensitive VA research data:** Once data have been summarized, submitted for publication, or published, the data are **not** considered “sensitive.”

4. **PROCEDURES**

a. **Data Security Plan for a Research Protocol**

During the early stages of planning a research project, an investigator should think about how sensitive research data will be stored and accessed, as well as how to protect subjects’ privacy. When the principal investigator submits a research study that involves the collection, use and/or storage of sensitive information (e.g., subject identifiers or protected health information (PHI)) to an IRB and a R&D Committee, his/her submission for approval must contain specific information on

- All sites where the data will be used or stored
- Specifically who will have access to the data
- How the data will be transmitted or transported
- How the data will be secured
- If copies of the data will be placed on laptops or portable media, a discussion of the security measures
- If the data will be re-used for subsequent or future research protocols, provisions for future use in the informed consent form, and HIPAA-Compliant authorization
- If relevant, provisions to ensure sponsor data storage guidelines are met and do not conflict with VA policies
- Inclusion of a description of any reasonable foreseeable privacy risks to the subject (included in the informed consent)
- Information about where and how a veteran could verify the validity of a study and authorized contacts (included in the informed consent)

- b. *Note: The principal investigator (PI) must certify that all VA sensitive information associated with each specific study is being used, stored and secured in accordance with applicable VA and VHA policies and guidance. This certification is done at the time of the initial review using Appendix C and D of VA Memorandum, February 6, 2007, “Certification by Principal Investigators: Security Requirements for VA Research Information.” For purposes of this VA Data Security Checklist for Principal Investigators, sensitive VA research data is defined at the Tuscaloosa VA Medical Center as data that contains personal identifiers (one of the 18 identifiers listed by HIPAA). The Data Security Checklist for Principal Investigators and Principal Investigator’s Certification: Storage and Security of VA Research Information (Appendix C and D of VA Memo February 6, 2007) is reviewed by the*

R&D committee at the time of initial review and the form must be stored with the research protocol files.

b. **Restricted Access:** Access to sensitive VA research data is restricted to:

- Individuals named in the approved research protocol, on the approved research informed consent (if applicable) and the HIPAA authorization form (if applicable)
- Individuals who are responsible for oversight of the research program
- Individuals named in the approved TVAMC R&D Data Removal Permission Form
- VA investigators who require access “preparatory to research” if their activity meets requirements set forth in VHA policy

Persons not employed by VA are given access to medical and other VA records for R&D purposes only when necessary VA approvals have been issued that are in compliance with legal restrictions (i.e. WOC appointments, CRADO or Data Transfer Agreements)

c. **Technical Safeguards:** The appropriate use of technical safeguards is extremely important to protect against unauthorized access, disclosure or loss of VA research data. These safeguards include the following:

- **Data Storage:** Whenever possible, VA research data should be stored on a VA server or VA network drives with restricted access, not on desktop computer, laptop or portable media devices. If research data need to be accessed or stored on a laptop or portable media device, the equipment must be encrypted.
- **Password Protection:** Passwords must meet VA password requirements. “Blank” and default user names and passwords cannot be used. User credentials, including passwords, must be protected appropriately because they are considered VA sensitive information. Passwords should never be shared with anyone else. Passwords must be stored in a safe and secure place that no one else knows about. Passwords or other authentication information cannot be stored on remote systems unless those systems have been encrypted according to VA requirements
- **Encryption:** Additional security controls, such as encryption, are required to guard sensitive research data stored on computers used outside VA facilities or when transmitting sensitive data via remote access or through emails. Encryption must be used for the following:
 - VA-owned or non-VA equipment in a mobile environment (i.e. laptop)
 - A personal computer (PC) at an alternative work site
 - Any portable storage media device containing personally identifiable health information or personal identifying information
 - Email systems that deliver sensitive research data

Note: All encryption modules used to protect sensitive VA research data (i.e. data with personal identifiers) must meet National Institute of Standards and Technology (NIST) standards and be Federal Information Processing Standards (FIPS) 140-2 certified, as required by Federal Information and Security Management Act of 2002 (FISMA). The TVAMC ISO can supply a list of products that meet NIST and FIPS standards.

- **Protection from Viruses and Other Malicious Codes:** It is important to protect VA research data from computer viruses and other malicious codes. VA-approved antivirus software must be used on all computers operated by VA investigators that contain sensitive VA research data. The TVAMC ISO will provide the software for VA-owned equipment.
- d. **Physical Safeguards** are important for protecting VA research data. The following rules for physical security of data apply to all VA employees, and they apply whether the data are stored on VA-owned or non-VA equipment, inside or outside of VA facilities:
- Do not take equipment, information, or software containing sensitive VA research data to non-VA sites without the required authorization.
 - See that equipment is housed and protected to reduce the risks from environmental threats and hazards, and protected against opportunities for unauthorized access, use, loss, removal or theft
 - Do not leave storage media or hard copies containing sensitive VA research data unsecured. When not in the physical possession of the authorized user, such materials must be stored behind no less than two locks to which only authorized VA personnel have access.
 - When traveling, do not check portable computers and storage devices as baggage
 - Protect data and system backups with the same or equally effective physical security as provided to the source computer, its media and the information contained on them
 - Store backups where they are physically secure. When not in the physical possession of the authorized user, such materials must be stored behind no less than two locks to which only authorized VA personnel have access.
- e. **File Sharing:** Sensitive VA research data may be shared through authorized VA servers (i.e. shared drive on a VA server).
- f. **Data Off-site Storage, Transport or Transfers:** Employees who remove confidential and Privacy Act-protected data (i.e. containing one of the 18 HIPPA identifiers) from VA premises must have written authorization to do so. To store, transport, transmit, access and use sensitive VA research data (i.e. data containing any of the 18 HIPPA identifiers) on non-VA computer systems/servers outside the VA, the principal investigator must obtain a Data Transfer Agreement between the TVAMC investigator and the recipient and also obtain permission using the TVAMC Data Removal Permission Form from ALL of the following:

- His/her supervisor
- The Chief for Research and Development (C/R&D)
- The Information Security Officer (ISO)
- The Privacy Officer (PO)
- The TVAMC Chief of Staff
- The TVAMC Medical Center Director

The TVAMC Data Removal Permission Form includes the name of the protocol, name of principal investigator, type(s) of research information to be removed, reason for removal of VA research information, name and address of any non-VA personnel/entity who will have access to the VA research information, and how the research information will be transmitted. This form should be completed and reviewed by the R&D Committee. Signatures of the Chief of Staff and Medical Center Director can be obtained at the time of their review and signature of the R&D minutes.

The employee authorized to remove electronic data may consult with their supervisor and the TVAMC ISO to ensure that the data are properly encrypted and password-protected in accordance with VA policies. All removable or transferable storage media (Flash drives, CD ROMs, laptops, etc) are subject to review by the ISO to remove or secure sensitive information.

Note: "Outside the VA" means storage or use on any non-VA computer system, server, desk top computer, laptop or any other portable storage medium (e.g., CD, floppy disk, or thumb drive).

- g. **Remote Access:** Laptops and handheld computers, such as personal digital assistants (PDAs), owned by the VA are called Government Furnished Equipment (VAGFE) and are issued to authorized persons who must have a property pass for the equipment. These electronic devices may be used to access the VA Intranet remotely. Only VA-approved remote access solutions may be used, and all remote connections to VA networks must be through VA-authorized configurations and access points. Access to the VA Intranet using non-VA owned equipment will be provided via approved VA Virtual Private Network (VPN) access protocols, which will offer access to a limited set of VA applications and services. Only remote access users with VA government furnished equipment (VAGFE), with supervisory approval, with all required security software installed and updated, will be permitted to connect to the VPN in such a way that grants full VA access. Remote access is handled and authorized by the TVAMC ISO. The ISO disables the remote access account if it is not used for a period of 90 days and removes the account if it is not used for 6 months.
- h. **Data Retention and Destruction:** VA research data must be retain in accordance with VA, VHA, local and IRB policies, protocol sponsor guidelines, or Privacy Act system of records notice, whichever is most restrictive. During the period that

data are retained after a protocol closes, the investigator must provide the same security and privacy measures as when the protocol was active, including all physical and technical safeguards. Once the required retention period has lapsed, the data may be destroyed using a method that will render them unreadable, undecipherable and irretrievable. *Note: This pertains to both VA and non-VA owned computer equipment and storage devices.*

- i. **Backups:** Sensitive VA research data and essential data and software must be backed-up at regular intervals and the backups and archives according to their VA security classification. *Note: As mentioned above, a VA server is the best place to create a backup because VA information technology (IT) staff ensures the safety of the network and that it is routinely backed up.*

- j. **Reporting Requirements for Misuse, Loss or Theft:** The loss or theft, or any other unauthorized access to research data containing sensitive personal information or portable media such as laptops is covered in VHA Handbooks 6500. The TVAMC policy will comply with VHA policies on prompt reporting of loss, theft, or actual or suspected breaches involving sensitive information, along with any other privacy or security incident or complaint. The ISO will promptly determine whether an incident warrants further reporting and actions. 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 the VA security/police officers immediately
 - During 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
 - The persons' immediate supervisor
 - The local Information Security Officer (ISO)
 - The Chief of Staff
 - The Medical Center Director.
 - The Chief of Research and Development
 - The Privacy Officer must be notified when there is any unauthorized use, loss, or disclosure of individually-identifiable patient information.
 - Any such event must also be reported to the IRB as an unexpected adverse event.

- k. **Notifying Veterans of Incidents Involving Compromised Personal Information:** Should notification letters be deemed necessary, all notification letters are reviewed by facility incident response team, facility Office of Public and Intergovernmental Affairs, and Regional Counsel, as well as the VISN and National Level Incident response team, if appropriate. **NOTE: These notifications are NOT sent from the investigator.** All notifications use a specified template. The substance of the notice to the veteran about an incident

involving personal information is reduced to a stand-alone document and written in clear, concise, and easy-to-understand language, capable of individual distribution and/or posting on VA's website and other information sites. Written notifications to veteran include the following elements:

- A brief description of what happened
- To the extent possible, a description of the types of personal information that were involved in the incident
- A brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches
- Contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, website, and/or postal address
- Steps individuals should take to protect themselves from the risk of identity theft, including steps to take advantage of Equifax credit protection and contact information for the Federal Trade Commission (FTC) website and publications.

VISN Director and VACO-assigned VISN DUSHOM Health System Specialist of designee are notified after the Notification Letters receive local clearance and prior to mailing to veterans. The medical center Director is responsible for notifying the VISN DUSHOM Health System Specialist or designee. No notification letters are mailed to the veterans without first obtaining DUSHOM and VHA Privacy Office concurrence. Notification letters regarding deceased veterans are sent to veterans' next-of-kin, and information in the letters is tracked using a spreadsheet. Determination that credit protection services should be offered, of how promotional codes for credit protection are dispersed and the provisions for an 800-number or local call line to impacted veterans with questions are made and implemented by the facility.

5. REFERENCES

- VA Directive 6500, "Information Security Program"
- VA Directive 6502, "VA Enterprise Privacy Program"
- VA IT Directive 06-02, "Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations"
- VA IT Directive 06-06, "Safeguarding Removable Media"
- VA Memorandum, February 6, 2007, "Certification by Principal Investigators: Security Requirements for VA Research Information"
- Office of Research Oversight website at <http://vaww1.va.gov/oro/>.
- The Freedom of Information Act (FOIA), 5 U.S.C. 552
- The Privacy Act (PA) of 1974, 5 U.S.C 552a
- The VA Claims Confidentiality Statute, 38 U.S.C. 5701
- Confidentiality of Drug Abuse, Alcoholism & Alcohol Abuse, Infection With the Human Immunodeficiency Virus (HIV) and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332

- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 Code of Federal Regulations Parts 160 and 164
- Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705
- VHA Handbook 1200.5

6. ATTACHMENTS

- **Data Transfer Agreement**
- TVAMC Data Removal Permission Form
- Appendix-C-D (2)

7. RESCISSIONS

TVAMC HRPP SOP#10 dated May 7, 2007.

8. REVIEW DATE

January 1, 2012

Signature on File in R&D Office.

Lori L. Davis, MD

Chief of Research and Development