DEPARTMENT OF VETERANS AFFAIRS
South Texas Veterans Health Care System
San Antonio, Texas 78229-4404

Policy Service Policy Memorandum 11-35

March 2, 2011

RESEARCH STANDING OPERATING PROCEDURES (SOP)
Protection of VA-Sensitive Research Information

1. **PURPOSE:** To outline the policy and procedures that have been established to ensure the security of VA-sensitive research data and protected health information.

2. **DEFINITIONS:**

   a. De-identified information. Information that does not identify an individual, (or relative, employers, or household members of an individual) and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. It must also meet the Common Rule (38 CFR 16) definition of de-identified. De-identified information may not include any of the 18 direct identifiers stipulated by the HIPAA Privacy Rule.

   b. Disclosure of VA-sensitive information. The release, transfer, or provision of access to, or divulging in any other manner information outside VHA.

   c. Encryption. The conversion of information or data stored in an electronic file or drive into a cipher or code, to prevent unauthorized access. Accomplished by loading encryption software on the electronic device. All encryption modules used to protect VA data must be validated by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140.

   d. Individually Identifiable Information. Any information, including health, financial, and employment information, maintained by VHA pertaining to an individual that also identifies the individual by name or other unique identifier. Privacy Act systems of records, medical records, personnel files, and limited data sets are all considered individually identifiable information.

   e. Protected health information (PHI). Information protected by the HIPAA Privacy and Security Rules, 45 CFR Parts 160 and 164.

   f. Remote access. Access to VA information from locations other than sites within a VA facility.

   g. Thumb Drive: A USB Flash Drive is essentially NAND-type flash memory integrated with a USB 1.1 or 2.0 interface used as a small, lightweight, removable data storage device. This hot swappable, non-volatile, solid-state device is usually compatible with systems that support the USB version that the drive uses.

   h. VA protected information (VAPI). VA sensitive information, Privacy Act Information (PAI), PHI, or other VA information that has not been deliberately classified as public information for public distribution. VA information that VA would have to release under the Freedom of Information Act is not VA Protected Information. All VA Protected Information should be classified as one of the following: VA Proprietary, VA Restricted, or VA Highly Restricted.

   i. VA Sensitive Information. VA sensitive information is 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

(6) All protocols involving the collection, use and/or store of research information including subject identifiers and PHI that are submitted to an IRB and R&D Committee for approval must contain specific information on all sites where the data will be used or stored, how the data will be transmitted or transported, who will have access to the data, and how the data will be secured.

(7) Access to data must be restricted to those individuals named in the research protocol and individuals who are responsible for oversight of research programs.

(8) Obtaining and using medical, technical, and administrative records from other VA facilities or VA databases (national, regional, or subject specific) for R&D purposes must be in compliance with all VHA regulations and with the Standards for Privacy of Individually-Identifiable Health Information (45 CFR Parts 160 and 164).

(9) Obtaining and disclosing individually identifiable patient records must be in compliance with all applicable confidentiality statues and regulations. Provisions must be taken to protect the privacy of subjects and to maintain the confidentiality of individually identifiable data. Such provisions must consider the requirements of Standards for Privacy of Individually-Identifiable Health Information (HIPAA Privacy Rule), 45 CFR Parts 160 and 164, and other laws regarding protection and use of veterans' information, including Privacy Act of 1974, 5 U.S.C. 552a; VA Claims Confidentiality Statute, 38 U.S.C. 5701; Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with Human Immunodeficiency Virus (HIV), and Sickle Cell Anemia Medical Records, 38 USC 7332; and Confidentiality of Healthcare Quality Assurance Review Records, 38 USC 5705.

(10) Persons not employed by VA can be given access to medical and other VA records for R&D purposes only within the legal restrictions imposed by such laws as the Privacy Act of 1974 and 38 U.S.C. Requests for such use must be submitted to the CRADO in VA Central Office at least 60 days before access is desired. Requests for information filed pursuant to the Freedom of Information Act ordinarily requires a response within 10 working days. This does not apply to those individuals having access for the purpose of monitoring the research. Obtaining and using the records must be in compliance with all VHA regulations and with the Standards for Privacy of Individually-Identifiable Health Information (45 CFR Parts 160 and 164).

b. Protection of electronic VA-sensitive information. The preferred means of storage of VA-sensitive information is on a STVHCS server located in the secure IT server room. In only unusual circumstances, should VA-sensitive data be stored on an individual computer workstation. VA-sensitive information that is maintained on electronic storage devices must be protected by adherence to the following:

(1) Only VA personnel (salaried or without-compensation appointments) who are approved to participate in the research protocol may access VA-sensitive information.

(2) Only VA-owned (VA Government Furnished Equipment; VAGFE) equipment may be used to store and process VA-sensitive information or access VA processing services. VAGFE and OE that contain VA-sensitive information must be encrypted and equipped with, and use, a VA-approved antivirus (AV) software and a personal ("host-based") firewall that is configured with a VA-approved configuration. Approved encryption software must be used when employees use VAGFE or non-VA OE in a mobile environment [e.g. laptop or Personal

Digital Assistant (PDA) carried out of a VA office] and VAPI is stored on the computer, file, or electronic storage media.

(3) Employees may not simultaneously connect to VA and one or more non-VA networks while using VAGFE.

(4) Employees must use only computers and electronic storage media configured to conform to all VA security and configuration policies to store, transport, transmit, use and access VAPI. The following requirements apply to the use of both VAGFE and OE in the access of VAPI:

(a) VA employees must use passwords that meet VA password requirements.

(b) The "save password" feature must not be used for passwords that provide access to the operating system or VA network services

(c) "Blank" and default user names and passwords must not be used

(d) User credentials including passwords are considered VA sensitive information and must be protected appropriately

(e) A shared file or drive containing VAPI must not be created on a device used for remote computing. File sharing of VAPI must only be accomplished through the use of authorized VA servers.

(f) VAPI or VA-specific software must be segregated in dedicated directories that are protected

(g) If VAPI such as Protected Health Information (PHI), privacy information, or information that could be used by unauthorized persons to gain access to VA systems is to be stored outside of the VA intranet or outside of the physical protection of VA facilities, it must be protected.

(h) Password-protected screensavers must be configured to activate after five minutes of inactivity.

(i) The screen saver must be activated manually when the workstation is unattended.

(j) Anti-virus software must be installed and operational.

(k) All devices must conform to operating system hardening guidelines as specified in VA Information Security guidance.

(5) Removable and transportable storage media, including flash drives, thumb drives, CD-ROMs, DVDs, external hard drives, and laptops, may not be used to store or transport VA-sensitive information unless they have been encrypted using VA-approved encryption software.

c. Remote access to electronic VA-sensitive information stored within the VA

(1) Employees must obtain supervisory approval for remote access to the VA Intranet.

(2) Only VA-owned Government Furnished Equipment (VAGFE), including laptops and handheld computers, are used when accessing the VA intranet remotely, and all required security software is installed and updated to connect to the VA Virtual Private Network (VPN) in such a way that grants full VA access.

(3) Access to the VA Intranet using non-VA owned Other Equipment (OE) requires the use of approved VA VPN access protocols, which offer access to a limited set of VA applications and services.

(4) If a remote access account is not used for a period of 90 days it will be disabled by the ISO, and if it is not used for 6 months the ISO will remove the account.

(5) Upon termination of a research employee's required access privileges, the employee's supervisor must confirm and notify the ISO that the employee has returned all VAGFE related to remote access.

d. Storage of VA-sensitive information outside of the STVHCS

(1) VA-sensitive information may not be stored outside the STVHCS except in unusual circumstances and with the appropriate institutional approval.

(2) Permission from the supervisor, ACOS/R&D, PO, and ISO is required to remove VA-sensitive data from the STVHCS, or to store VA-sensitive research information on non-VA computer systems/servers, desk top computers located outside the VA, laptops, or other portable media.

(3) Electronic data may be maintained on non-VA servers only when the servers are certified and accredited as required by Federal Information and Security Management Act of 2002 (FISMA).

(4) All laptops, other portable media, or personal computers that store VA-sensitive information, regardless of their location, must be encrypted and password protected. The original data must not be stored on laptops or portable media. All laptops, whether within or outside the VA, are encrypted if used for any research purposes.

(5) Where possible, during the collection of VA-sensitive research data, the data should be de-identified (e.g. removal of names, addresses, SSNs (real or scrambled)) and stored in coded form, and all identifiable information and the key linking to the coded data must be stored only within the STVHCS (preferably on the research server).

(6) Research subjects properly executing a HIPAA authorization for disclosure of their PHI to the UTHSCSA affiliate constitutes a disclosure under HIPAA after which VA no longer owns the transferred information. Thus, with a valid HIPAA authorization (or IRB-approved waiver of authorization) the subjects PHI stored on the affiliate's server in not considered "VA Sensitive Information" because the data no longer belongs to VA. A VA CIO waiver is not required under these circumstances.

e. Disclosure, transport, transmission, access, and use VA data outside VA facilities

(1) VA research employees must obtain written authorization from their supervisor and STVHCS officials (ACOS/Research, Information Security Officer, and Privacy Officer) to disclose VHA individually-identifiable health information involving research subjects to non-VHA investigators for research purposes.

(2) VA research employees must obtain written authorization from their supervisor and STVHCS officials (ACOS/Research, Information Security Officer, and Privacy Officer) to transport, transmit, access, and use VA-sensitive data outside the STVHCS. Research personnel authorized to remove electronic data must ensure the data are properly encrypted and password-protected in accordance with VA policies, and should consult with their supervisors and ISOs if there is any question of the security of the data. outside the STVHCS.

(3) Employees authorized to remove confidential and Privacy Act-protected data from VA must take all relevant precautions and use VA-approved protection mechanisms to safeguard the data until it is returned.

(a) Employees use only computers and electronic storage media configured to conform to all VA security and configuration policies to store, transport, transmit, use, and access VA-sensitive information.

(b) All removable or transferable storage media (flash drives, CD ROMs, laptops, etc.) are reviewed to remove or secure sensitive information (also see D8, D20, D23, & D25).

(c) Data may be attached only to encrypted emails, and sent on portable media by mail or delivery service only after they are encrypted.

(d) For all VAGFE used to transmit, transport, access, process, or store VA data, the research employee may not take equipment, information, or software off-site without prior authorization by his/her supervisor.

(4) Disclosure of individually-identifiable information to non-VHA investigators, independent of an approved VA research protocol, for research purposes must be approved by the Chief Research and Development Officer in VA central office.

(5) Without prior written authorization, disclosure of individually-identifiable health information, excluding 38 USC §7332-protected information, to Federal investigators may be made only when the Under Secretary for Health or designee has approved the research and an IRB or Privacy Board has waived the authorization requirement.

(6) Title 38 USC §7332-protected information may be disclosed without written authorization only when the following conditions listed in VA Handbook 1605.1 §13b(1)(d) are met The research protocol must indicate:

(a) The information must be maintained in accordance with the security requirements of 38 CFR Section 1.466, or under more stringent requirements;

(b) The information will not be re-disclosed except back to VA; and

(c) The information will not identify any individual patient in any report of the research, or otherwise disclose patient identities.

(7) The individually-identifiable information collected from research subjects in their capacity as VHA employees, excluding health information, may be disclosed to non-VHA Investigators for research purposes without written authorization only in accordance with the Privacy Act and applicable VA privacy policy.

f. Security of portable electronic storage devices

(1) Portable computers. Portable computers that have VA-sensitive information on their storage device(s) or have software that provides access to VA private networks, must be secured under lock and key when not in the immediate vicinity of the responsible employees. Employees must use physical locks to secure portable computers to immovable objects when the computers must be left in a meeting room or other semi-public area to which individuals other than the authorized employees have access. When traveling, employees must keep portable computers or storage devices in their possession, not in check-in baggage. A property pass for the portable electronic storage device (e.g. laptop, etc.) must be obtained before removal from the STVHCS.

(2) Removable storage media. Information contained on USB devices (e.g. thumb drives, external hard drives) can be easily compromised if the device does not have adequate protective features. All VA research personnel who have access to and store VA information must have permission from a supervisor and Information Security Officer (ISO) to use such devices. Only USB thumb drives that are Federal Information Processing Standards (FIPS) 140-2 certified can be utilized. VA employees are not authorized to access or store any VA information using a thumb drive that has not been procured by the VA. Utilization of personally-owned USB thumb drives within the Department is prohibited.

g. Storage and security of VA-sensitive data on hard copy (paper; radiographs, etc).

(1) Individually identifiable VA-sensitive research data maintained on paper copy (e.g. case report forms, data forms, etc.) must be stored under physical security controls that meet the National Institute of Standards and Technology (NIST) standards.

(a) If the data are to be stored in a room that is accessed by personnel other than the research staff (e.g. housekeeping or environmental management personnel), the data must stored in a locked cabinet and the room must be locked when the research staff are not present. Key access to the locked cabinets must be limited to the research staff.

(b) If the data are to be stored in a room that is accessed only by the research staff (with the exception of emergency security and environmental safety personnel), the data may be stored in the locked room outside of a locked cabinet. Key access to the room will be limited to the research staff.

(2) Access to the data is limited to authorized individuals who are designated on the VA approved protocol.

(3) Any loss or compromise of the VA-sensitive research data must be reported promptly to the ACOS for Research and Information Security and Privacy Officer at the STVHCS.

(4) Any transmission, transport, or use of the VA-sensitive data outside the above location must be approved by the ACOS for Research, Information Security Officer, and Privacy Officer of the STVHCS.

h. Destruction of VA sensitive information. When no longer needed, VA-sensitive information must be destroyed by a method rendering it unreadable, undecipherable, and irretrievable as prescribed in the most current version of "Fixed Media Sanitization" (VA Memo, April 20, 2004) and its attachment.

i. Training. All employees must be current in the mandatory annual training for *Good Clinical Practices and the ethical principles of human subjects protection, VA Cyber Security Awareness, VHA Privacy Policy,* and *VA Research Data Security*.

(1) R&D office administrative staff will maintain an active database with training completion dates for all research personnel.

(2) The database will be queried monthly to generate reminders and follow ups for annual training requirements.

(3) Training dates will be verified and updated daily by R&D administrative staff.

j. Loss or compromise of VA-sensitive information

(1) Procedures for reporting the loss or theft of VA sensitive data or portable media containing sensitive data must be familiar to researchers and all others who have access to use, store, or transport the data.

(2) Research personnel must report the loss of confidential or Privacy-Act protected data immediately to his/her supervisor, the ACOS for research, the STVHCS Information Security Officer and Privacy Officer, and the IRB (reported as an Unanticipated Problem Involving Risk to Subjects or Others [UPIRSO]).

(3) Research personnel must immediately report incidents involving theft, loss, or compromise of any VAGFE or non-VA OE device used to transport, access or store VA-sensitive information to his/her supervisor, the ACOS for research, and the local ISO.

(a) If research personnel are within a VA health care facility the VA police must also be notified.

(b) If research personnel are on travel or at another institution the security/police officers of that institution must be notified. The case number and name and badge number of the investigating officer(s), and a copy of the case report if possible, should be obtained.

k. **ACOS/Research and Research Office Responsibilities**. The ACOS/Research and Research Office staff will provide ongoing educational activities and reminders to insure that all investigators and their research personnel are fully informed of the importance of the protection of VA-sensitive research information, and the policies and procedures related to its protection. Research Office staff will monitor the completion of relevant training modules (VA Privacy, VA CyberSecurity, VA Research Data Security) to ensure that each investigator and research personnel are compliant with the required training. The ACOS/Research is responsible to ensure effective communication between the Research Office and Information Security Officer, Privacy Officer, and IRB.

l. **Principal Investigator (PI) Responsibilities**. The principal investigator is responsible to safeguard VA sensitive information. The PI must ensure that all research personnel understand and abide by existing policies, procedures, and directives regarding the protection of human subjects in research and the use and disclosure of individually-identifiable information.

m. **Research and Development Committee Responsibilities**. The R & D Committee through the Data Security and Privacy Subcommittee will ensure that protocols involving the collection, use, and/or storage of research information including subject identifiers and PHI have procedures in place that adequately protect VA sensitive information. The R & D Committee through the Data Security and Privacy Subcommittee will ensure that each protocol approved contains specific information on all sites where the data will be used or stored, how the data will be transmitted or transported, who will have access to the data, and how the data will be secured.

4. **REFERENCES:**

a. VHA Handbook 1200.05

b. VA IT Directive 06-2

c. VHA Handbook 1605.1

d. VA Directive 6504

e. VA Memorandum, "Fixed Media Sanitization", April 20, 2004

f. VA Directive 6601

g. VA Memorandum, "Further Guidance on ORD Implementation of VA Handbook 6500 6c(4)(j): Update to ORO Memoranda dated May 29, 2008 and January 30, 2009", dated May 14, 2009

h. VA Memorandum, "Researcher Contacts with Veterans", dated July 10, 2006

5. **RESPONSIBILITY:** ACOS for Research and Development (151)

6. **RESCISSION:** Research Service Memorandum 07-35, dated April 27, 2007

7. **RECERTIFICATION:** March 2016

Kimberly K Summers, PharmD
KIMBERLY K. SUMMERS, PHARM.D.
Acting ACOS for Research and Development