



# Stratton VA Medical Center

## R&D Standard Operating Procedure:

### SECURING VA RESEARCH INFORMATION WHEN EMPLOYMENT TERMINATES

1. **PURPOSE:** This policy describes the Stratton VA Medical Center (SVAMC) Research and Development (R&D) measures to protect VA research/information and personal health information (PHI) obtained for research purposes when an investigator resigns or transfers from the SVAMC.

2. **POLICY:** It is the responsibility of all VA employees to uphold the standards of cyber security and privacy as established by the VA for the protection of research including sensitive research information. This responsibility includes protection of sensitive and non-sensitive research information when an investigator resigns or transfers from the SVAMC.

a. 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 is 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, IIR, original notes, documents, and records produced by VA in the course of the protocol are the property of VA.

b. VA sensitive information is defined in VA Handbook 6500, Information Security Program 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, and records about individuals requiring protection under various confidentiality provisions such as the Privacy Act or Health Insurance Portability and Accountability Act (HIPAA). VA sensitive information belongs to and at the VA.

c. The following 18 items relating to the individual or of relatives; employees; or household members of the individual, are considered PHI identifiers under HIPAA: 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.

3. **ACTION:** 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 the following two items to R&D staff for the e-PROMISE system; a page 19 and a final summary/progress report of the research study.

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 is to remain at the SVAMC, 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) is 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 Marilyn Mason from the 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 it's 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 Medical Center SOP on Data Security. The research office will be able to assist you in locating this document.

g. Destruction of Data: At this time VA sensitive and non-sensitive data in research must not be destroyed until further notice and direction from VA Central Office (CO). The ISO, Privacy Officer (PO) and Chief Information Officer (CIO) are both available to assist with compliance of this VA regulation.

#### 4. REFERENCES:

VA IT Directive 06-02, Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations.  
VA IT Directive 06-05, Use of Personal Computing Equipment.  
VA IT Directive 06-06, Safeguarding Removable Data.  
VA Directive 6500, Information Security Program.  
VA Directive 6502, Privacy Program.  
VA Handbook 1200.5, Requirements for the Protection of Human Subjects in Research  
VHA Handbook 1605.1, Privacy and Release of Information.  
VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information.  
VA Handbook 6500, Information Security Program.  
VA Handbook 6502.1, Privacy Violation Tracking System (PVTS).  
VA Handbook 6502.2, Privacy Impact Assessment.  
VA Memo DUSHOM/CRADO, Certification by Principal Investigators: Security Requirements for VA Research Information.  
VA Memo DUSHOM/CRADO, Research Responsibilities for Protecting Sensitive Information.  
VA Memo DUSH/CRADO, Cyber Security and Privacy.

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