Certification by Principal Investigators: Security Requirements for VA Research Information

1. The Department of Veterans Affairs (VA) is committed to protecting sensitive information including veteran's personal identifiers and health information. This commitment to guard all sensitive information also includes protecting information collected for research purposes. The research may be related to human subjects, either data obtained on-site or brought from other institutions; research involving laboratory animals; or other sensitive research. It is imperative that VA be able to demonstrate this commitment and develop mechanisms that will allow for documentation of the actions taken to safeguard research information. This document combines the policies of both VA Headquarters and the Zablocki VAMC.

2. Investigators involved in animal research should consider the sensitivity of their data and the ramifications of a breach in security of animal data, especially regarding sensitive documents such as photographs.

3. For all active research protocols involving human subjects, the Principal Investigator(s) will certify that the use, storage, and security of all research 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 completing a “Data Security Checklist” and “Principal Investigator’s Certification: Storage & Security of VA Research Information” for each protocol. These documents will also be required for all new research protocols involving the use of human subjects.

Background, Definitions, and Requirements for Protecting VA Research Information

1. Additional Background. The ability of investigators to conduct research within the Department of Veterans Affairs (VA) is a privilege that comes with many responsibilities. One of these responsibilities is to ensure the security of all VA research information. In addition, there must be compliance with all applicable Federal laws, regulations, policies, and guidance related to privacy, confidentiality, storage, and security of research data. Research data generated by VA investigators during the conduct of VA-approved research is owned by the VA and its use and storage must meet all Federal standards including, but not limited to Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards and Technology (NIST) standards for computer systems and encryption, the Privacy Act of 1974, and the Health Insurance Portability and Accountability Act (HIPAA). Compliance requires that VA research information that is not encrypted and password protected may not be stored on non-VA servers, laptops, or portable media unless specific permissions have been obtained from the person's supervisor, the Assistant Chief of Staff (ACOS)/R&D, and the Information Security Officer (ISO) and all other requirements met as defined by VA policy. In addition there are a number of applicable VA and VHA policies to which investigators and research staff must comply. A list of these policies may be found on ORD's website, www.va.gov/resdev or on VHA's publication website: www.va.gov/vhapublications. A list of the current policies is attached.

2. Definitions: A first step in protecting this data is to clearly define research information. It is also necessary to understand that this term includes more than information found in a veteran's medical record. The definitions of these terms are found below.

   a. Data: Within this document the term data refers to both VA and extra-VA data collected for, used in, or derived from the conduct of a VA-registered research project.
b. **Preparatory Research:** Within VHA, "preparatory to research" refers to activities that are necessary for the development of a specific protocol. Privacy Health Information (PHI) from data repositories or medical records may be reviewed during this process, but only aggregate data may be recorded and used in the protocol. Within the VA, preparatory to research does NOT involve the identification of potential subjects and recording of data that would be used to recruit these subjects or to link to other data (unless it is approved by the IRB, as is the requirement at the ZVAMC). The preparatory to research activity ends once the protocol has been approved by the Institutional Review Board (IRB) and the Research and Development (R&D) Committee.

c. **Removed from the VA:** Means that the data's destination is other than sites within a VA facility.

d. **Research Information:** Information that is a subset of sensitive information that is or has been collected for, used in or derived from the conduct of a research project. This can include individually identifiable information and de-identified information derived from human subjects. It also includes sensitive data or information from research involving laboratory animals or other types of sensitive research.

e. **Individually Identifiable Information:** Any information, including health, financial information, 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.

f. **De-identified information:** Information that does not identify an individual, (or relative, employers, or household members of an individual) as required by VHA Handbook1605.1 Appendix B 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:

- Name
- Dates directly related to an individual, including date of birth, dates of hospital admission and/or discharge, or date of death (mm/dd/yyyy or mm/yyyy - does not include year only); and all ages over 89 and all elements of dates (including year only) indicative of such age, unless aggregated into a single category of age 90 or older
- Social security number
- Geographic information smaller than a state (includes street address, city, county, and zip codes), except for the initial three digits of the zip code as below *
- Telephone number
- Fax number
- Electronic mail address
- Web universal resource locator (URL)
- Health plan beneficiary number
- Certificate/license number
- Device ID and serial number
- Internet protocol address number
- Medical record number
- Account numbers
- Vehicle ID or serial number (including license plate)
- Biometric identifiers (including finger and voice prints)
- Full face photographic image
- Any other unique identifying number

*If according to the current publicly available data from the Bureau of the Census: a) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and b) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

De-identified information may not include any codes that are in any way derived from or related to these direct identifiers or other information about the individual, e.g., de-identified information may not include portions of social security numbers of scrambled social security numbers.

g. **VA Sensitive Data**: This term 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.

3. **Requirements for Protecting Research Information.** The Federal statutes, regulations, and policies (VA and VHA) listed at the end of this document contain a number of requirements. As defined within these statutes, regulations, and policies, investigators and other research staff must comply with the following requirements. **Note: This list is not inclusive of all requirements. Please consult the regulations, policies, and guidance documents for all requirements not listed below.**

- Computerized VA research data may not be stored outside the VA unless it is encrypted and password protected and permission has been obtained from your supervisor, the ACOS/R&D and the ISO. This includes data storage on non-VA computer systems/servers, desktop computers, laptops, or other portable media located outside the VA. This Medical Center's policy is that no hard copies of identified VA patient data will leave the VA. Written requests for an exception should be submitted in writing to the ACOS/R&D, who will review and forward to the ISO.

- Data transfer to a non-VA computer server must only occur after the required permissions have been obtained from the ISO and the transfer must be in compliance with requirements found in VA Directive 6500. The system must meet all requirements set forth in FISMA including the required Certification and Accreditation of the system.

- The data residing on all computers (including laptop computers) or on portable media other than the VA server must be password protected and encrypted, with only authorized individuals having access to the data.

- All research information residing on any computer (including laptops) or on other portable media not within a VA health care facility must be encrypted and password protected. **Note: The original data may not be stored on laptops or portable media and all laptops regardless of their location within or outside the VA must be encrypted if used for any research purposes.**

- Research subjects or veterans names, addresses, and Social Security Numbers (real or scrambled)
that are not password protected and encrypted may only be stored within the VA under lock and key or on VA servers. If the data is coded, the key to linking the code with these identifiers must also be stored within the VA. Requests for exceptions to this must be submitted in writing to the ACOS/R&D and to the ISO.

- All protocols that will include the collection, use and/or storage of research information including subject identifiers and PHI that are submitted to an IRB and to a 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, specifically who will have access to the data, and 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 for these media must be included.

- A copy of any files containing identified data used on computer must be maintained at the VA in a secure and separate location for possible VA or VHA review.

4. **Explanation of concepts or terms used in this document:**

a. **Restriction to access.** Access to data should be restricted to those:

   (1) Individuals named within the research protocol, on the research informed consent, in the HIPAA-compliant authorization form, and in the subject waiver of authorization form.

   (2) Individuals who are responsible for oversight of the research program.

   (3) VA investigators who require access "preparatory to research" if their activity meets requirements set forth in VHA policy.

b. **Procedures for reporting loss or theft.** The loss or theft of VA research data/information or portable media such as laptops or personal computers (PCs) is covered in VA Handbook 6500. The following should occur as soon as it is discovered that there has been a loss:

   (1) Report the loss or theft to security/police officers as soon as possible but within one hour of discovery.

   - If you are within a VA health care facility, the VA police must be notified.

   - 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.

   (2) As soon as possible but within one hour call or e-mail the following regarding the incident:

   - Your supervisor,
   - Elizabeth Jacobs, M.D., Associate Chief of Staff for Research, at Ext. 41430 (elizabeth.jacobs@va.gov)
   - Robert H. Beller, FACHE, Medical Center Director, at Ext. 41025
ORD Cyber Security and Privacy

The Office of Research and Development is dedicated to upholding the standards of cyber security and privacy is established by VA. It is also the responsibility of all VA researchers and staff to be familiar with and to comply with existing policies, procedures and directives regarding the protection of human subjects in research and the use and disclosure of individually-identifiable information.

1. Information Security and Privacy Policies
   - VHA Handbook 1200.05 - Requirements for the Protection of Human Subjects in Research.
   - VHA Handbook 1605.1 - Privacy and Release of Information.
   - VA Handbook 6500 – Information Security Program
   - VA IT Directive 06-2 - Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations
   - VA IT Directive 06-5 - Use of Personal Computing Equipment
   - VA IT Directive 06-6 - Safeguarding Removable Media
   - VA Handbook 6502.1 - One VA Privacy Violation Tracking System (PVTS)
   - VA Handbook 6502.2 - Privacy Impact Assessment (PIA)
   - 45CFR Parts 160 and 164 - Health Insurance Portability and Accountability Act (HIPAA)

3. Local Policies
   - Medical Center Memorandum ISO-200: Information Security (IS) Program
   - Medical Center Memorandum ISO-197: Internet Use and Security
   - Medical Center Memorandum ISO-193: User Computer Training Requirements
   - Medical Center Memorandum OQMS-152 Confidentiality of Patient Information

5. Any questions regarding these issues can be directed to your research office.

(Robert.Beller@va.gov)
- Matthew Feeks, J.D., Privacy Officer, at Ext. 41095 (matthew.feeks@va.gov)
- Rustine Johnson, Information Security Officer, at Ext. 42151 or 42194 (rustine.johnson@va.gov)