

PROTECTION AND SECURITY OF SENSITIVE RESEARCH INFORMATION AND DATA

1. **PURPOSE:** To establish policies and procedures for information security for research studies conducted at the Louis Stokes Cleveland Department of Veterans Affairs Medical Center (Louis Stokes VAMC), which involve VA patients or VA resources, and involve VA employees, including part-time and full-time staff, and without compensation employees as investigators, collaborators and study staff.
2. **POLICY:** To ensure that sensitive information collected as part of research conducted under or within the auspices of the Louis Stokes VAMC is securely and adequately safeguarded. All sensitive data collected and stored, whether in print or electronic form, are to be protected and secured against inadvertent or deliberate misuse, loss, or improper disclosure. Only authorized individuals are to have access to identifiable data.
3. **RESPONSIBILITY**
 - a. **Medical Center Director** – The Medical Center Director is the Institutional Official for the Human Research Protection Program (HRPP) at the Louis Stokes VAMC, and, as such, has ultimate responsibility for the overall conduct of the Research & Development (R&D) program, including the welfare of human research participants.
 - b. **Associate Chief of Staff (ACOS) for Research** – The ACOS for Research is responsible for the operation of the Research program, including the welfare of human subject participants.
 - c. **Administrative Officer (AO) for Research and staff** – The AO for Research supervises the day-to-day operations of the Research office and provides staff support to the R&D Committee and Institutional Review Board (IRB).
 - d. **Research Compliance Officer (RCO)** – The RCO is responsible for developing and continually reviewing policies and procedures to ensure compliance with current regulations.
 - e. **Research and Development (R&D) Committee** – The R&D Committee provides overall direction and oversight to the R&D program, which includes a human subject research component.

f. **Institutional Review Board (IRB)** – The IRB is a subcommittee of the R&D Committee. It is the primary organizational unit charged with the responsibility of protecting the rights and welfare of all individuals, whether patient, employee, or volunteer, who participate as subjects in the VA research program. As such, the IRB will investigate any unanticipated problems involving a breach in security involving sensitive information.

g. **IRB Administrator and Staff** – The IRB Administrator and staff advise and educate investigators and all research personnel regarding operational procedures for obtaining and maintaining approval to conduct human subject research.

h. **Chief, Information Resource Management Services (IRM) and staff** – The Chief, IRM is responsible for configuration of all government owned equipment storing any sensitive information. IRM will advise on procurement hardware, minimum requirements, and assist with configuration to ensure security requirements are met.

i. **Information Safety Officer (ISO)** – Will ensure that all security regulations are followed. The ISO is a resource for guidance on all security requirements for the agency. All security incidents must be reported to the ISO as soon as possible following the incident.

j. **Principal Investigators (PI) and Research Staff** – Every member of the research team is responsible for protecting human subjects. Every member should employ adequate safeguards for the secure maintenance of sensitive research information and data. PIs are ultimately responsible for protection of human subjects participating in their research. PIs must ensure that all co-investigators/research staff are trained and employ adequate safeguards and protections for the secure maintenance of sensitive information and data.

4. DEFINITIONS

a. **VETERANS HEALTH INFORMATION SYSTEMS & TECHNOLOGY ARCHITECTURE (VISTA)** is the primary system of records for all patient information. VISTA contains all information accessed via CPRS

b. **COMPUTERIZED PATIENT RECORD SYSTEM (CPRS)** is the client software providing access to all clinical data for patients. This data is stored in the VISTA system as described above.

c. **VIRTUAL PRIVATE NETWORK (VPN)** is software available for remote desktop or laptop computers to allow access into the VA network.

d. **INDIVIDUALLY IDENTIFIABLE INFORMATION** refers to any information that can directly (or indirectly) identify an individual. For example, name, social security number or portion thereof, etc.

e. **SENSITIVE INFORMATION** – refers to, but is not limited to, patient/subject/participant/employee identifiable personal information (e.g. name, social security number, telephone number codes, etc.).

f. **UNANTICIPATED PROBLEM** – any research-related event involving risk to anyone (including investigators and research staff as well as subjects) associated with the research in any way that are not included in the protocol and informed consent document. It includes not only unanticipated adverse events, but other unanticipated problems (e.g., breeches of confidentiality, equipment malfunctions that may injure the investigator, loss of data that results in the need to enroll additional subjects, thus exposing additional subjects to the risks of the research).

5. PROCEDURES

All investigators and research staff have responsibility for ensuring both physical and electronic security of records especially those records that contain sensitive information.

Physical Security

a. Portable devices such as laptops are to be secured with chains and/or placed in a locked file cabinet when not in use or when an office is unoccupied. Whenever the user leaves his/her workstation, he/she must log out of the system and secure any portable devices. Utilization of time-out functionality is recommended. Offices should be locked whenever not in use.

b. Laptops are not permitted to leave the Medical Center without express authorization of the employee's supervisor.

c. There are times when data files need to be removed from the VA in order to conduct the study off-site, e.g. analyses. All jump drives/portable data devices utilized are to be encrypted when data containing sensitive information is transported on such devices. Nothing should be permanently stored on these devices. If a jump drive is to be utilized, a plan should be in place to secure data. The physical transport of such devices should be done with thought to safeguarding the device. Transport of paper copies of data should receive the same careful consideration.

d. Data and system backups that include VA information have the same confidentiality classification as the originals. Therefore, these materials must be protected with the same or equally effective physical security as that provided for the source computer, its media, and information contained therein.

e. When in an uncontrolled environment such as traveling on an airplane or in an airport, investigators and research staff must guard against information disclosure through eavesdropping, overhearing or overlooking (shoulder surfing) by unauthorized persons. When traveling, investigators and research staff must keep portable computers or storage devices in their possession, and may not check them as baggage.

f. Physical locks must be used to secure portable computers to immovable objects when the computers must be left in a meeting room or other semi-public area when individuals other than the authorized employee have access. Portable computers used in this manner should not contain sensitive data.

g. Keys to desks, file cabinets and/or other data storage areas should not be easily accessible to non-authorized individuals.

Electronic Security

a. All laptop/desktop computers that use information provided from VISTA, *including* CPRS, are to be configured in accordance with VA IRM requirements and policies, regardless of the ownership of the computer equipment. Thus, computer equipment purchased through VA, NIH-sponsored, privately sponsored, and/or other non-VA sponsored funds must be configured by IRM.

b. Electronic data should not be stored on either the desktop or laptop. Rather a network drive should be utilized. Patient/subject/participant data should be stored utilizing a unique identifier on a network drive. (The last name or portion thereof and/or the last 4 digits of a social security number are not unique identifiers.) The code should be kept in a separate password protected file or in a locked file cabinet/desk.

c. Passwords are never to be shared nor stored in an obvious location.

d. There are times when data files need to be removed from the VA in order to conduct the study off-site, e.g. analyses. Although nothing should be permanently stored on these devices, all jump drives/portable data devices utilized are to be encrypted when data containing sensitive information is transported on such devices.

e. A plan should be in place to secure data to be transmitted via the internet.

f. Security regarding email/fax transmissions. Sensitive information should not be sent via e-mail or fax, unless encrypted or proper precautions, in accordance with VA directives, are utilized.

g. Remote access – VPN must be acquired from the ISO.

h. Random (often unannounced) audits of equipment/work stations and/or study record security/storage may be conducted at any time. These random reviews may be done by the R&D (member and/or staff), IRB (member and/or staff), ACOS, RCO, Privacy Officer, etc.

i. **EDUCATION:** All research personnel working on studies with access to the sensitive data, whether located at the VA or not, must complete the VA Privacy and Cyber Security training annually. Such training is to be completed by the date established by VA directives.

Use of Individually Identifiable and/or Sensitive Information

a. All human subject research studies should include information regarding the use, disclosure, transfer/transmission, storage, and return or destruction of individually identifiable information. A plan delineating these points must be included as part of individual protocol submissions. For currently-approved studies, deficient areas, if any, must be addressed with a modification to the current IRB protocol. These plans must be reviewed and approved by the IRB.

b. At the close of a human subject study, investigators are required to reiterate either how data, to be kept indefinitely will be stored or how data will be/has been destroyed. If the plan has changed from what was previously reviewed and approved by the IRB, IRB approval of the new plan will be required prior to implementation.

6. **REPORTING REQUIREMENTS:** Should a security breach occur, the PI and/or Research Staff must immediately report the event to the IRB, Louis Stokes VAMC Privacy Officer, Medical Center Director, Chief(s) of Staff, ACOS, AO, RCO, and VA Police, and Case Western Reserve University, if applicable Agency(ies) that may need to be notified include, Office of Research Oversight (VA), Office of Human Research Protection (NIH), and/or the FDA.

7. **REFERENCE:** Medical Center Policy 151-018 (Human Research Protection Program); IRB SOP Manual, VHA HB 1200.5, 65 F.R. 82462-82829; 45 C.F.R. § 164.501; VHA HBs 1605.1, 1058.1 and 1907.1; 21 CFR Part 50; VA Directive 6504

8. **RESCISSION:** Medical Center Policy 151-019, Protection and Security of Sensitive Research Information and Data, dated December 1, 2006. The review date of this policy is December 1, 2009.

9. **FOLLOW-UP RESPONSIBILITIES:** Associate Chief of Staff for Research

WILLIAM D. MONTAGUE
Medical Center Director