VAPHS RESEARCH & DEVELOPMENT

POLICY NUMBER: 017

TITLE: Research Information Protection Program

1.0 PURPOSE

The VA Pittsburgh Healthcare System (VAPHS) recognizes that the security and confidentiality of research information, and the privacy of the research subject we serve are of the utmost importance. Therefore, the purpose of this policy is to describe the Research Information Protection Program (RIPP) at VAPHS and to outline the mechanisms and procedures utilized to ensure that any research information collected, transferred, transmitted, and/or stored in conjunction with VAPHS research is done so in a manner that is compliant with VA Information Security and Privacy requirements.

2.0 DOCUMENT HISTORY

R&D Committee Approval Date	Version	Change	Reference Section(s)	Effective Date
07/25/2017	2.1	Updated definition of VA sensitive information. Addition of requirements related to non-VA equipment and the air gapped network.	4.0 6.3	07/26/2017
04/11/2017	2.0	Addition of requirements related to transmission, storage, and requests for research data. Removal of reference to audio recordings. Significant formatting revisions to compile requirements specific to human subjects as an addendum, and to include requirements related to communication methods. Rescinds R&D Policy #004 "Research Records Transfer Policy"	1.0, 2.0, 4.0, 6.1, 6.3 7.0, Addendum A	05/01/2017
04/28/2015	1.2	Clarifications regarding the use of PittNet. Inclusion of requirements regarding photographs. Additional information added regarding the use of national data sets for research.	6.3 & 6.4	05/01/2015
02/24/2015	1.1	Signification revisions regarding the requirements for electronic storage. Revisions to section regarding Human Subjects Research to align with 11/2014 version of VHA Handbook 1200.05	6.3 & 6.4	02/27/2015
05/13/2014	1.0	NEW POLICY		05/14/2014

3.0 SCOPE

This policy applies to all research activities conducted under the jurisdiction of the VAPHS Research and Development Committee and all personnel working on such projects.

4.0 DEFINITIONS

NOTE: *The terms defined below are contained in statutes or regulations. The following definitions are intended to have the same meaning contained in the statutes and regulations, unless otherwise specified, and are meant to be easy to understand without changing the legal meaning of the term.*

A. Anonymous: For the purposes of VA research, anonymous means de-identified in accordance with both:

(1) The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR 164.514(b), and

(2) The Common Rule provision that the identity of the subject cannot be readily ascertained by the investigator or associated with the information (38 CFR 16.102(f))

B. Coded Data: The term "coded data" means "coded private information" as defined in guidance published by HHS entitled Guidance on Research Involving Coded Private Information or Biological Specimens, currently available at: http://www.hhs.gov/ohrp/policy/cdebiol.html

C. VA Data: Information derived directly from VA approved research.

D. Data Repository: A data repository is a database or a collection of databases that have been created or organized to facilitate the conduct of multiple research protocols, including future protocols not yet envisioned. It also may have been created for other purposes such as administrative and clinical purposes (VHA Handbook 1200.12).

E. De-Identified Data: For the purposes of VA research, de-identified data are data that have been de-identified in accordance with both:

(1) The HIPAA Privacy Rule (45 CFR 164.514(b) (see VHA Directive 1605.01), and

(2) The Common Rule provision that the identity of the subject cannot be readily ascertained by the investigator or be associated with the information (38 CFR 16.102(f))

De-Identified data may also be known as "anonymous".

NOTE*: Coded data is data identifiable by the individual(s) who has access to the code. Therefore, coded data are not considered to be de-identified or anonymous.*

F. HIPAA Authorization: The term HIPAA authorization means prior written permission for use and disclosure of protected health information (PHI) from the information's source person, research subject, or legally authorized personal representative, as required under law, including HIPAA. The written authorization must include all elements of a compliant authorization (see VHA Directive 1605.01) prior to any disclosure of information.

G. Human Biological Specimens: Human biological specimens are defined as materials derived from human individuals, such as blood, urine, tissue, organs, hair, nail clippings, buccal swabs, or any other materials that are either collected specifically for research purposes or as residual specimens from diagnostic, therapeutic, or surgical procedures. Bacteria, fungi, or viruses obtained from human biological specimens are not considered human biological specimens, as long as the human material has been removed.

H. Human Subject: A human subject is a living individual about whom an investigator (whether professional or student) conducting research obtains: (1) data through intervention or interaction with the individual or (2) identifiable private information. Individuals who receive test articles or who serve as controls in clinical investigations, including clinical investigations as defined under FDA regulations in 21 CFR 50.3, 312.3(b), and 812.3(h), are also considered human subjects.

I. Individually-Identifiable Information: The phrase Individually Identifiable Information (III) means any information, including health information, maintained by VHA pertaining to an individual that identifies the individual and, except for individually identifiable health information, is retrieved by the individual's name or other unique identifier. Individually identifiable health information is covered by VHA policies regardless of whether or not the information is retrieved by name.

J. Individually-Identifiable Health Information: The phase Individually Identifiable Information (III) is a subset of health information, including demographic information, collected from an individual that is:

(1) Created or received by a health care provider, health plan, or health care clearinghouse;
(2) Relates to the past, present, or future condition of an individual and provision of or payment for health care; and
(3) Identifies the individual, or a reasonable basis exists to believe the information can be used to identify the individual.

NOTE: *IIHI does not have to be retrieved by name or other unique identifier to be covered by the VHA Directive 1605.01*

K. Institution: An institution is any public or private entity or agency (38 CFR 16.102(b)).

(1) ***VA Institution:*** A VA institution is any entity that is operated by VA, including but not limited to: VA hospitals, medical centers, clinics, and health care systems; space owned, leased, or rented by VA; and space that is "shared" with a non-VA entity (unless the VA space is leased to a non-VA entity and specifically designated in writing not to be used by VA or VA employees for research). A VA facility may include multiple campuses and satellite components.
(2) ***Non-VA Institution:*** A non-VA institution is an entity not operated by VA. Non-VA institutions include, but are not limited to:
   a. Any entity that is not a legal component of VA or of a VA facility, including a contract research organization (CRO), industry or private sponsor, or public or private research company, foundation, or group.
   b. Entities operated under a contract with VA including, but not limited to, contract Community-based Outpatient Clinics (CBOCs), contract nursing homes, contract outpatient clinics.
   c. Academic institutions, including VA–affiliated medical schools, dental schools, and other academic affiliates
   d. VA-affiliated Non-Profit Research and Education Corporations (NPCs).
   e. Other Federal, state, or local departments or agencies.

L. Limited Data Set: A limited data set is protected health information from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, Email address, Social Security Number (SSN), medical record number, health plan number, account number, certificate or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, State, or zip code. Thus, a limited data set is not de-identified information, and it is covered by the HIPAA Privacy Rule. A limited data set may be used or disclosed without obtaining either an individual's authorization or a waiver of authorization granted by the Institutional Review Board (IRB). The limited data set may be used only for the following purposes: research, public health, or health care operations. A limited data set may contain some

direct identifiers, therefore, research conducted using the data may constitute human subjects research.

M. Private Information: Private information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a health record). Private information must be individually identifiable (i.e., the identity of the subject is provided or may readily be ascertained or associated with the information) in order for obtaining the information to constitute research involving human subjects (38 CFR 16.102(f)).

N. Protected Health Information (PHI): PHI is individually identifiable health information maintained in any form or medium. ***NOTE:*** *PHI excludes health information in employment records held by a covered entity in its role as an employee.*

O. Research: Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes. For example, some demonstration and service programs may include research activities. Clinical investigations, including clinical investigations as defined under FDA regulations in 21 CFR 50.3, 312.3(b), and 812.3(h), are considered research for purposes of VHA Handbook 1200.05.

P. Research Records: Research records include, but are not limited to, IRB and R&D Committee records, records of all observations, subject recruitment activities, other data relevant to the investigation, progress notes, research study forms, surveys, questionnaires, and other documentation regarding the study.

Q. VA Investigator: A VA investigator is any individual who conducts research approved by the VA R&D committee while acting under a VA appointment on VA time, including full and part-time compensated employees, trainees, without compensation (WOC) employees, and individuals appointed or detailed to VA under the Intergovernmental Personnel Act (IPA) of 1970.

R. VA Sensitive Information/Data: All Department information and/or 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 not only information that identifies an individual, but also includes other 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 applicable confidentiality provisions. (38 U.S.C. § 5727) Please see VHA Handbook 1200.12 (Use of Data and Data Repositories in VHA Research) for specific examples of VA sensitive information.

S. VA Research: VA research is research conducted by VA investigators (serving on compensated, WOC, or IPA appointments) while on VA time. The research may be funded by VA, by other sponsors, or be unfunded. VA research must have R&D Committee approval.

5.0 RESPONSIBILITIES

It is the expectation that everyone involved with research conducted at VAPHS will ensure the security and confidentiality of any sensitive research information collected, used, transmitted, transported, or stored as part of that research. Furthermore, it is also expected that the appropriate safeguards will be put into place to protect the privacy of our research subjects. Members of the research community are expected to be familiar with the policies and procedures of the VAPHS Research

Information Protection Program which may be described in this policy, as well as other relevant VAPHS policies and/or Standard Operating Procedures.

6.0 POLICY

6.1 Training

All staff involved in VA research, including, but not limited to, all VAPHS Research Office personnel, investigators, study coordinators, research assistants, trainees, such as house officers and students, administrative support staff (including secretaries and clerks) and members of the VAPHS Institutional Review Board (IRB) and Research and Development Committee (R&DC) must comply with current VA requirements regarding information security/privacy trainings.

The VAPHS Research Office maintains a database of training status for all research staff members. Staff members and their supervisors are notified approximately 30, 14, and 7 days prior to training expiration. Individuals who allow their training to expire will be notified of the expired status, as will their supervisors. Having expired training may result in being removed from studies and being unable to perform any research activities.

6.2 Procurement and use of Information Technology (IT) Equipment for Research Purposes

A. IT Equipment Procurement

The purchase of computers and related accessories is dependent upon the source of funds allocated for said purchases. Investigators and other members of the VAPHS research community may be allocated funding from VA Central Office or the Veterans Research Foundation of Pittsburgh (VRFP).

(1) All equipment purchased using research funds, regardless of funding source are the property of VAPHS or VRFP. Use of such equipment is subject not only to all VHA policies but also to all VAPHS policies and procedures regarding data security and privacy.
(2) When VA Central Office is the funding source, funds will be sent from Central Office for the purchase of a specific Information Technology (IT) item. The VAPHS Research Office will be required to request and receive IT tracking approval and the investigator will be responsible for working closely with the Research Office Budget Assistant to obtain appropriate bids and approvals for the IT purchase.
(3) In the case of VRFP funding, sufficient funds must be available in the account of the research investigator in order to make the purchase. Approval must be requested in advance of the purchase and the research investigator must work closely with the VRFP Office Staff to provide the necessary details to make the purchase.

B. Delivery and Set-up

The specific requirements related to the delivery and set up of IT equipment are detailed below:

(1) Desktop Computers: Desktop computers may be delivered directly to the site of use. All desktop computers which will be connected to the VA network will need to have the appropriate software installed to disable USB ports and will not be able to have CD burning software unless approval has been granted by VAPHS Chief Information Officer.

(2) Laptop Computers: All newly purchased laptop computers will be delivered to the Research Office before issuance to the user. The laptop computer will be encrypted by OI&T prior to any use for research purposes. If the laptop will be connected to the VA network, the appropriate software will be installed to disable the USB ports. The laptop will not be able to have CD burning software unless approval has been granted by the VAPHS CIO. Laptop computers connected to the Pitt Network may contain the USB and CD Burning capability only with approval from the VAPHS Research and Development Office and receipt of a signed Research Funded Portable Device User Agreement.

(3) Other Portable Storage Devices: Other portable/mobile storage devices, such as USB Thumb Drives, portable hard drives, and digital audio recorders may be purchased and used for research purposes. Such devices must be encrypted using FIPS 140-2 validated encryption. If such encryption is technically not possible, approval for use must have been obtained from the VAPHS ISO, CIO, and Deputy Assistant Secretary for VA's Office of Information Security.

(4) Other IT Equipment (e.g. IT peripherals and equipment such as monitors, printers, scanners etc.): These purchases or issuance of these types of equipment must be approved by the VAPHS Research Office.

C. Conditions for Use and Assignment of IT Equipment

(1) Inventories:

a. *Annual Inventory:* An annual inventory of all IT (VA, VRFP Purchased, and University Purchased) Equipment will be conducted by the VAPHS Research Office. The user will note condition of the equipment and its location. Failure to respond to inventory requests will result in confiscation of the equipment.
b. *Quarterly Health Checks:* VAPHS OI&T staff performs health checks of VA issued laptop computers.

(2) Assignment:

a. All equipment assigned to any research staff member, whether or not it contains research data should be documented without exception. This documentation should include the terms of use and procedures for reporting theft or loss of such equipment. All initial assignments of equipment are made by the VAPHS R&D Office.
b. If a member of the research staff resigns from his/her VA position, the proper clearance procedures should be followed, which includes clearance through the VAPHS R&D Office and Human Resources. At that time all assigned equipment will be collected.

(3) Off Station Use: All requests to use equipment off VA property must be submitted to the VAPHS R&D Office for review and processing. Any request must be made using the appropriate form. The circumstances under which, a specific form must be used are described below:

Type of Equipment	Appropriate Request Form
Government Furnished Equipment (GFE)	GFE Check out Sheet
Government Furnished Equipment (GFE)	Revocable License
Veterans Research Foundation of Pittsburgh (VFRP) Purchased	Portable Device User Agreement

a. Forms can be obtained from the Administrative Officer for the ACOS/R&D. Off-station use cannot occur until the approval has been granted.
b. All research information residing on laptops and other portable media not within a VA health care facility must be encrypted and password protected. The original data may not be stored on laptops or portable media and the laptops must be encrypted if used for any research purpose.

D. Transfer and Reassignment of IT Equipment

All equipment reassignments must be approved in advance by the Associate Chief of Staff for Research and Development (ACOS/R&D) or his designee. Research IT equipment can be moved/relocated only by authorized IT personnel only.

E. Return and Disposal of IT Equipment

When the equipment is considered obsolete, beyond economical repair, or no longer needed; it should be disposed through the equipment turn-in process. The turn-in of VA purchased equipment must follow the procedures outlined in VAPHS Medical Center Memorandum LD-025 Management and Control of Non-Expendable and Expendable Equipment. The turn-in of VRFP purchased equipment must be coordinated through the VAPHS Research Office.

F. Equipment Loans

Please refer to VAPHS Medical Center Memorandum LD-027 Loans and Removal of Property.

6.3 Storage and Transmission of Research Data and Project Related Information

A. Electronic Storage and Transmission

(1) VA Information Systems:

a. VA Research data and project related information must be stored on the VA network, unless written permission has been granted from the appropriate officials (e.g., the facility Information Security Officer and appropriate research review committees). VAPHS Researchers and staff must establish and utilize shared drives on VA network servers to store VA data, as well as project related information, including, but not limited to forms, templates, reports, etc. Permission to the share drive(s) must be carefully monitored so that only those personnel authorized to access the information have such access. In the case of human subjects research, only those individuals approved to have access (as outlined in the IRB approved protocol) should have access. Under no circumstances should such data or information be stored on the hard drive of a VA desktop or laptop computer. Additionally storage of such data/information on an employee's personal drive of "N" drive on the VA network is strongly discouraged.
b. Investigators can only store VA sensitive research data on VA servers on the VA network unless otherwise approved by the ISO and appropriate research

committees. Examples of VA sensitive research information include: Protected Health Information (PHI), patent applications, Institutional Animal Care and Use Committee (IACUC) correspondence, data that would be included in an invention disclosure, and compliance issues. Any data that involves human subjects, but does not contain PHI, may also be considered sensitive, but such a determination would need to be made on a case-by-case basis.

(2) Pitt Network (PittNet):

VA research may be conducted using "PittNet" (the Pitt Network established at the VAPHS) provided that a MOU is in place which documents the terms and conditions for the development, management, operation and security of the network. Furthermore, the MOU will define the purpose, identify relative authorities, specify the responsibilities of both organizations, and define the terms of the agreement. The MOU, held through OI&T, must be reviewed annually or it will expire. The components connected to the air-gapped network may never touch the VA network. VA sensitive data or limited data sets cannot be transferred or transmitted over the Pitt Network connection or stored on University devices connected to the Pitt Network. VA data, such as scientific data obtained directly from scientific instruments, may be stored on computers connected to the Pitt Network with written permission from the VAPHS ACOS/R&D, ISO, and CIO. VA research data must be stored on the VA network; therefore, VA research data collected on non-VA equipment connected to the Pitt network must be transferred to the VA network via secure methods, such as VA-issued encrypted thumb drive or email.

(3) Other Non-VA (External) Information Systems:

Any other external information system used to process, store, or transmit VA sensitive information must have the security controls/requirements for use documented in a VA approved MOU/ISA, VA contract or other VA approved agreement (e.g., Data Use Agreement) before such use will be authorized. Personally owned or equipment owned by the affiliate institution will be approved for use by the Information System Owner, local CIO, or designee. Equipment owned by the affiliate will be included on the Research Equipment Inventory List (EIL) contained in the facility property management system.

(4) Laptops:

a. *VA/Veterans Research Foundation of Pittsburgh (VRFP) Purchased:* All VA/VRFP purchased laptops are encrypted and imaged prior to issuance. Storage of direct identifiers (i.e., names, addresses, SSN's) is not permitted however, storage of information that has been de-identified, but is still considered VA sensitive information is permitted, as are limited data sets, provided that the data stored on the laptop is not the only copy. Such laptops may be connected to the VA network, if they have been set up by OI&T and imaged.
b. *University Purchased or Laptops Purchased in Conjunction with an approved protocol:* Laptops purchased with University funds or other funds in conjunction with an IRB approved protocol may not be used to store VA sensitive research information. Such laptops may not be connected to the VA network. These devices can, however be connected to the Pitt Network/air gapped network and must be included on the Research EIL.

c. *Personal Laptops*: Personally owned information systems (capable of storing data) used on site at VAPHS to connect to VA's network or to perform assigned official duties must be approved by the VAPHS CIO and ISO.

(5) Portable Storage Devices (e.g. USB Thumb Drives, Portable Hard Drives, Recordable Optical/Magnetic Media, Digital Storage Devices, CDs and DVDs):
All sensitive information and limited datasets must be stored on a VA owned FIPS 140-2 compliant encrypted storage device. VA encrypted USB drives can be requested by completing the Request for a USB Flash Drive form. CD burning is not allowed by default at VAPHS. Any individual required to store information on a CD/DVD must request CD burning privileges by completing a Request for CD/DVD Write Access waiver. Please consult the ISO office for recommended devices and device use procedures. Members of the VAPHS research community must have permission from a supervisor and the ISO to use portable storage devices to access or store VA information.

B. Hard Copy and Media Storage

VAPHS investigators are responsible for ensuring that hard copy documents or physical media such as audio and videotapes that contain sensitive VA research data are protected from improper disclosure, including inadvertent disclosure. The following methods should be utilized to ensure protection:

(1) Paper Records:
Paper copies or original documents containing sensitive information must be secured in such a way as to prevent non-authorized persons from accessing them. Paper copies should be stored using a "double lock" method such as filing in a locked cabinet within a locked office or within a restricted access floor or building.

(2) Video Recordings and Photographs:
Video recordings and photographs of research subjects are considered to be sensitive information unless the image has been altered in such a way as to make it impossible to identify the subject and no other identifiable information is present on the recording or picture. The video recordings should be transferred to the VA network as soon as possible following the recording. Digital video recorders must meet VA security requirements. Digital photographs must be uploaded to the network as soon as possible. For studies in which video tapes are being utilized, the tapes must be stored at VAPHS, using a "double-lock" method.

Whenever possible, research records in physical media or hard copy form should be stored in a single location in a locked cabinet with card access entry to the room. Investigators should avoid arrangements wherein research related data, identifiable or otherwise are kept in multiple locations. Researchers should make an effort to maintain all records in a single, tightly regulated environment with limited access and a log should also be maintained to track those accessing the information. For this reason, the VAPHS encourages the use of data cores, bioinformatics cores, etc.

6.4 Retention, Storage and Destruction of VA Research Data/Records

Investigators are required to retain VA research data 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, investigators are responsible for providing the same security and privacy measures as when the protocol was active, including physical and technical safeguards. ***NOTE:*** *VHA research data belongs to the VA. If an investigator leaves the VAPHS or the VA system, all data must be kept and stored within the VA so as to be easily accessible to facility officials. Investigators are not permitted to take copies with them.*

(1) Off-Site and Long Term Storage:
Storage of VAPHS research records off-site must be coordinated through the VAPHS Research Office in accordance with VHA Records Control Schedule and all applicable VA and VAPHS policies.

6.5 Additional Related Considerations

A. Biological Specimens

Investigators interested in using or establishing a VAPHS Biorepository should refer to VAPHS R&D Policy #020. ***NOTE:*** *For information related to human biological specimens, please refer to Addendum A.*

B. Written Agreements

VAPHS investigators are required to comply with the requirements for written agreements as outlined in VHA Handbooks 1200.05 and 1200.12.

C. Multi-Site Studies

The VAPHS PI is responsible for all aspects of the protocol conducted at VAPHS, including the privacy and security of the data. If the data are transferred outside of VAPHS, the transmission and storage of the data at the non-VAPHS site must be in compliance with all applicable polices and guidance.

D. Data Repositories

See VAPHS R&D Policy #018, Establishing a Research Data Repository.

6.6 Requirements Unique to Human Subjects Research

Please see Addendum A for additional requirements specific to Human Subjects Research.

6.7 Requests for VA Research Data From Non-VA Investigators or Institutions

In accordance with the VHA Records Control Schedule and VHA Handbook 1200.12:

(1) If an investigator leaves VAPHS and no longer holds an appointment as an employee (compensated or uncompensated) or an IPA, all research records, data, and data in repositories must be retained by VAPHS and remain under VA control.

(2) If at the time of departure, the grant is ongoing and the investigator leaves VAPHS to go to another VA facility, the investigator must obtain approval for a copy of the relevant materials to be provided to the new VA facility's research office.

(3) The investigator is not the grantee, nor does the investigator own the data. All data and records are the property of VA.

(4) The Privacy Officer must be consulted if an investigator receives a request for data from a non-VA investigator.

(5) **VA Research data may not be copied or removed unless all requirements for use of VA data by non-VA investigators or institutions are met.**

a. Investigators that leave VAPHS to go to a non-VA facility may request a copy of their research records.
b. Approval of such requests must be obtained from the VAPHS Research Office and any other relevant individuals or offices such as the applicable VAPHS R&D subcommittee (i.e. IRB, IBC, IACUC, etc.), privacy office, information security office, and the institutional official authorized to sign the written agreement.
c. These requests will be reviewed on a case-by-case basis.

(6) All requests from non-VA investigators or non-VA institutions for VA research data must be approved by the VAPHS Privacy Officer. The release of such data is controlled by the Privacy Act, VHA Records Control Schedule, HIPAA, VHA Handbook 1200.12, VA Directive 1605.01, and other privacy related regulations and policies.

(7) A waiver cannot be granted for data going outside of the VA.

(8) A written agreement defining what data may be used, how the data will be used, who may access and use the data, how the data must be stored and secured, and how the recipient will dispose of the data after completion of the research.

a. *Requests for Research Data that DOES NOT contain PHI or PII:* Must be submitted in writing to the Research Office via VHAPTHResearchOffice@va.gov
    i. Requests will be routed to the applicable VAPHS R&D subcommittee.
    ii. All requests must include a DUA/DTA.

b. *Requests for Research Data that DOES contain PHI or PII:* Must be submitted in writing to the Research Office via VHAPTHResearchOffice@va.gov
    i. Requests will be routed to the applicable individual(s) (e.g. VAPHS IRB or VA Central IRB Liaison).
    ii. The IRB will determine if the protocol, informed consent, and HIPAA authorization allow for the transfer of data.
    iii. All requests must include a DUA/DTA.

7.0 VIOLATIONS OF VAPHS RESEARCH DATA SECURITY AND PRIVACY POLICY

Any violation which meets the definition of a Research Information Protection Incident must be reported and managed in accordance with current policies including VAPHS R&D Policy #014 Research Information Protection Incident Reporting.

8.0 REFERENCES

VA Handbook 6500
VHA Handbook 1200.05
VHA Handbook 1200.12
VHA Directive 1605.01

9.0 SIGNATURES

//signature on file//

Gretchen Haas, PhD
Research and Development Committee Chair

//signature on file//

Steven H. Graham, MD, PhD
Associate Chief of Staff for Research and Development

Research Information Protection Program Requirements Unique to Human Subjects Research

Requirements listed in this addendum are to be followed in addition to all applicable requirements described throughout VAPHS R&D Policy #017.

A1.0 Requirements for the Collection of Human Subjects' Research Data

1.1 Individually Identifiable and Protected Health Information:

Research data containing subject identifiers and PHI may be collected: a) directly from a research subject and/or from their medical records after an informed consent and HIPAA authorization has been obtained or b) from pre-existing databases or third parties after the IRB has waived the requirement for informed consent and HIPAA authorization, in accordance with all applicable VA/VHA policies and regulations.

1.2 Limited Data Sets:

A limited data set is protected health information from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, e-mail address, Social Security Number (SSN), medical record number, health plan number, account number, certificate and/or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. A limited data set is not de-identified information or data. A limited data set may be used for research, health care operations, and public health purposes.

1.3 Coded Data Sets:

Often investigators may have data for which a special code is assigned. Coded data sets are NOT considered de-identified since the data is identifiable to those individuals who have the code.

1.4 De-identified Research Data:

Although rare, there may be instances in which, investigators are conducting research protocols that involve only de-identified data.

1.5 Access and Use of National Data Sets:

VAPHS Research Staff who plan to conduct research which requires use/access to national data sets such as the Corporate Data Warehouse must follow the procedures outlined by VA Informatics and Computing Infrastructure (VINCI). Access to these data sets is limited to those staff approved by the IRB (VAPHS IRB or VA Central IRB).

A2.0 Requirements for Off-Site Storage/Transfer/Transmission of VA Research Data

The processes for storage, transmission and transfer outside of the VA entity will be determined based upon the level of risk to subjects' privacy associated with the protocol. Please also review Section 6 of this policy.

A3.0 Risk Assessment and Classification

Each protocol will be assigned a risk level of Level I, Level II, or Level III based on the level of risk to privacy and data security. All protocols and applicable study related documents are reviewed by the

VAPHS Information Security Office and Privacy Officer for compliance with VA Information Security and Privacy requirements, and no off-site storage, transfer, and/or transmission can take place until IRB approval is granted.

3.1 Level I Protocols:

Level I protocols represent the greatest risk to privacy and include those protocols in which individually identifiable and/or Protected Health Information is collected or is proposed to be collected and used and the subjects are unaware of the use and disclosure of the research data. Level I protocols typically propose to use an IRB approved Waiver of Informed Consent and a Waiver of HIPAA Authorization in order to collect such information.

3.2 Level II protocols:

Level II Protocols are those protocols which represent an intermediate privacy risk to human subjects and include those protocols in which individually identifiable and/or Protected Health Information is collected and used and the subjects have been informed of the risks to privacy and have given permission for the use and disclosure of the information (i.e., an Informed Consent and HIPAA Authorization have been obtained).

3.3 Level III Protocols:

Level III protocols represent a low privacy risk to human subjects and typically refer to those protocols in which only de-identified data or limited data sets are being collected and used.

A4.0 Additional Use Considerations:

4.1 Use of Social Security Numbers:

Investigators can obtain and use real Social Security numbers only when real Social Security numbers are required to meet the specific aims of the research protocol or to enter information into the subjects' health records. The collection and use of real Social Security numbers must be approved by IRB, and the investigators must follow all applicable VA and other Federal requirements for obtaining and using real Social Security numbers. In addition the use of scrambled SSN or the last four digits of the SSN must be justified and approved by the IRB. If the IRB approves a protocol to include the use and/or disclosure of SSN, this must be clearly stated in the HIPAA Authorization. Investigators must also be sure to convey in the protocol and HIPAA Authorization the risks and benefits to the subjects as well as the measures that will be taken to protect the security of the data.

4.2 Use of Human Biological Specimens:

Human biological specimens may be sent to non-VA reference laboratories as required by an approved protocol. The accompanying data should not contain any of the HIPAA identifiers unless there is a compelling justification, and the data should remain there for the shortest time possible. See VAPHS IRB Tissue Banking SOP #103 for details regarding banking of biological specimens. Investigators interested in using or establishing a VAPHS Biorepository should refer to VAPHS R&D Policy #020.

4.3 Use of Electronic Mail:

Electronic mail shall be used for authorized government purposes and shall contain only non-sensitive information unless the information encrypted using one of the VA approved encryption methods. Research team members are prohibited from exchanging e-mail with potential study

participants and/or active study participants, unless the participants are VA providers and encryption can be utilized. Investigators interested in using e-mail as a method to transmit sensitive information, including PHI, to VA providers must outline this in their protocol/study application and must ensure that the proper encryption methods have been met.

4.4 Use of Text Messaging:

Text messaging cannot be used to transmit sensitive information between VA investigators and potential study participants and/or active participants. Investigators interested in using text messaging to communicate non-sensitive information with participants must describe this in their study application and such use will be considered by the IRB on a case-by-case basis.

4.5 Use of MyHealtheVet:

The use of Secure Messaging (SM), a tool available on the MyHealtheVet(MHV) website, for communication between VAPHS researchers and enrolled subjects is acceptable provided that the use of SM is included in the IRB approved protocol. Any investigator and his/her study team approved to use SM must receive appropriate training which can be coordinated through the facility's MHV Coordinators. The use of MyHealtheVet to recruit or communicate with potential research subjects is prohibited.

4.6 Use of Facsimile (FAX):

Care should be taken to assure confidentiality when faxing sensitive information. The following precautions should be taken:

(1) All fax coversheets should state:
   a. "This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

(2) Double check the recipient's fax number before transmittal and confirm delivery by telephone or review of the fax confirmation sheet.

(3) Save fax transmittal summaries and confirmation sheets to review for unauthorized access or use.

(4) Periodically remind regular fax recipients to provide notification in the event that their fax number changes.

(5) Utilize pre-programmed and tested destination numbers in order to minimize the potential for human error.

A5.0 Site Monitors and Access to Subjects' Electronic Medical Record Information

The VAPHS R&D Office recognizes that representatives (i.e. site monitors) from the VA Cooperative Studies Program and clinical trial sponsors have a duty to verify the content of case report forms from medical records. To facilitate reviews by external monitors, VAPHS has determined that monitors may access the information needed to conduct their jobs by utilizing one of the following methods:

5.1 The Employee Driver method which has been deemed compliant with VA's Information Security Program and VA Handbook 6500. Under this method, a VA employee "driver" accesses

the system with the monitor watching and shows the monitor only the information that the monitor needs and is authorized to see for the specific trial.

5.2 Research Coordinators may print copies of requested source documents, remove all direct identifiers (name, address and SSN), replace this information with the subject ID number or code and review them with the site monitor.