RESEARCH INFORMATION PROTECTION POLICY

1. PURPOSE: To establish a Research and Development (R&D) Service policy assuring compliance with VHA regulations governing security and protection of the confidentiality of research information, which includes all research data, and the privacy of research subjects participating in human research. Research information is any information accessed, collected, recorded, generated and/or disclosed for the purposes of conducting an approved research protocol.

2. DEFINITIONS:

a. **Coded Data**: Identifying information (such as name or social security number) that has been replaced with a number, letter, symbol, or combination thereof that prevents a person's ability to readily ascertain the identity of the individual to whom the private information or specimens pertain (i.e., the code); and a key to decipher the code exists, enabling linkage of the identifying information to the private information or specimens.

b. **De-identified data (anonymous):** Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. In order to be considered de-identified, the following 18 elements must be removed: name; address; names of relatives; names of employers; birth date; telephone number; fax number; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or device serial number; web URL; Internet Protocol (IP) Address; finger or voice prints; photographic images (e.g. full facial photographs); and any other unique identifying number, characteristic, or code. Information may also be statistically de-identified. De-identified data is not VA-sensitive data (see e. VA-Sensitive Information below).

c. **Identifiable Data:** Any data that can be connected directly to an individual which includes

1) **Individually-identifiable information:** Any information about an individual that is maintained and retrieved by VHA using the individual's name or other unique identifier, and either directly identifies the record's subject, or may be used with other information to identify the individual. Individually-identifiable information is also referred to as personally-identifiable information (PII). Individually-identifiable health information is included in this definition whether or not the information is retrieved by name.

a) **Individually-identifiable health information:** A subset of health information, including demographic information collected from an individual that is created or received by a health care provider, health plan, or health care clearinghouse. This information relates to the past, present, or future condition of an individual and the provision or payment of health care; and it identifies the individual or, a reasonable basis exists to believe the information can be used to identify the

individual. Individually-identifiable health information is also referred to as protected health information (PHI).

d. **Limited Data Set:** 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), IP address numbers, biometric identifiers, and full-face photographic images. A limited data set is not de-identified information or data.

e. **VA-Sensitive Information/Data:** 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 specific 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.

f. **Additional definitions and guidance are found in the PVAMC policy "Health Insurance Portability and Accountability Act in Human Subjects Research."**

3. POLICY: All individuals working in PVAMC research must appropriately protect and secure all research information.

a. All VA-sensitive information must be stored in a locked file cabinet in a locked office or, if electronic, on a secure VA server in a password-protected file unless an exception is authorized.

b. Only personnel who have completed all credentialing, education and training requirements, been appointed to a VA-paid or without compensation (WOC) position and approved for specific human research protocols by the IRB may access identifiable data. (See PVAMC policies: Credentialing of Personnel Involved in Research and Education for Conducting Research).

c. Accessing, recording, and disclosure of identifiable data for research purposes may occur only within the parameters of a research protocol submission approved by the appropriate subcommittees, e.g., the IRB, and the R&D Committee. Approved protocols must include an IRB approved-Informed Consent Form and Privacy Officer-approved HIPAA Authorization or an IRB-approved waiver for these forms and processes. Protection of research data is additionally assured by completion and approval of the Initial Review Questionnaire (IRQ), IRQ Appendices H (Use of Audio/Videotapes), I (HIPAA: Safe Harbor De-Identification Certification), J (HIPAA: Statistical Analysis De-Identification Certification). All submissions for research approval to the IRB must also be reviewed and approved with regard to information security and privacy by the PVAMC Privacy Officer (PO) and Information Security Officer (ISO) using the VA Checklist for

Reviewing Privacy, Confidentiality and Information Security in Research. (Checklist available at http://www.va.gov/oro/; all PVAMC forms are available at http://www.portland.va.gov/Research/piservices/rd_forms.asp#alphabetical.)
d. Data repositories must be established, maintained and used in compliance with the PVAMC HRPP policy, "IRB Review of Research Repositories" (http://www.portland.va.gov/Research/hrpp/index.asp#policies).
e. Research preparation involving identifiable data may occur only after submission and approval of a Research Preparation Application which governs the access to and use/disclosure of identifiable information for this purpose.
f. Breaches of data security and protection must be reported in compliance with the PVAMC policy, Required Reports for Research Information Protection (http://www.portland.va.gov/Research/hrpp/index.asp#reporting).
g. Data Use Agreements (DUA), Data Transfer Agreements (DTA), and combined Data Use-Data Transfer Agreements (DUA-DTA) identified **as applicable on the IRQ** (or Continuing Review Questionnaire) must be approved and signed before research or applicable research preparation may begin (or continue if using CRQ). These agreements are optional when transferring de-identified data and may be used if the sender would like to restrict the recipient's use of data. (Templates available at http://www.portland.va.gov/Research/piservices/rd_forms.asp)

1) A DUA , DTA or combined DUA-DTA is required when disseminating information or tissue from within a repository.
   a) A DUA can be used when the use is temporary (of limited duration) and there is a need to include final destruction information (i.e., return data/tissue; delete all electronic copies of data and shred hard copies, etc.).
   b) A DTA can be used when the sender wants to transfer ownership to the recipient. Once ownership is transferred the VA may no longer have control over the use and future dissemination of the information/tissue.
   c) A combined DUA-DTA is used when information/tissue is transferred VA to VA whether internal or to a different facility.

4. RESPONSIBILITIES and PROCEDURES:

a. The **Associate Chief of Staff / Research & Development (ACOS/R&D)** is responsible for developing, managing, and following policies and procedures that ensure compliance with all applicable state and federal regulations pertaining to research information protection. Policy development and management may be delegated to the Administrative Officer/R&D and the Research Assurance Officer. The ACOS/R&D is also responsible for assuring that all PVAMC investigators and R&D staff are aware of and comply with the regulations and local policies.
b. The **Research & Development Committee (R&DC)** is responsible for reviewing and approving this policy and providing initial approval of all research per the Standard Operating Procedures for the Research & Development Committee.

c. **R&D Subcommittees (IRBs, Institutional Animal Care and Use Committee (IACUC), Subcommittee on Research Safety)** are responsible for adhering to all rules and regulations governing research information protection.

1) IRBs must review all information security breaches, e.g., loss of PHI, possible loss of confidentiality or privacy of research subjects per the IRB SOP (http://www.portland.va.gov/Research/hrpp/index.asp#policies).

d. **The PO and ISO** are responsible for the following

1) Reviewing all proposed human research protocols per the IRB SOP and the VA Checklist for Reviewing Privacy, Confidentiality, and Information Security in Research.
2) Review and approval of all Health Insurance Portability and Accountability Act (HIPAA) Authorizations (PO only).
3) Fulfilling other duties per the Required Reports for Research Information Protection policy.

e. **Principal Investigators** are responsible for protection of all research information/data per this policy, as well as

1) Adhering to all rules and regulations governing research information protection and reporting the loss of any VA-Sensitive information and potential loss of research subjects' privacy to the ACOS/R&D, PO and ISO (see Required Reports for Research Information Protection)
2) Assuring all research team members are appropriately appointed, credentialed, trained and aware of the regulations and local policies and procedures.

f. **Research Employees and other Medical Center Staff** working on approved research projects are responsible for adhering to all rules and regulations governing research information protection and reporting the loss of any VA-Sensitive information and potential loss of research subjects' privacy to the ACOS/R&D, PO and ISO (see Required Reports for Research Information Protection).

g. **Non-Research employees with access to research areas** are responsible for adhering to all rules and regulations governing research information protection and reporting the loss of any VA-Sensitive information and potential loss of research subjects' privacy to the ACOS/R&D, PO and ISO (see Required Reports for Research Information Protection).

5. REFERENCES:

a. VHA Handbook 1200.05 - Requirements for the Protection of Human Subjects in Research
b. VHA Handbook 1200.12 - Use of Data and Data Repositories in VHA Research
c. VHA Handbook 1605.1 - Privacy and Release of Information
d. VHA Handbook 1605.2 - Minimum Necessary Standard for Protected Health Information
e. VHA Handbook 1605.03 - Privacy Compliance Assurance Program and Privacy Compliance Monitoring

f. VHA Handbook 1605.04 - Notice of Privacy Practices
g. VHA Handbook 1907.01 - Health Information Management and Health Records
h. VA Handbook 6502.1 and VA Handbook 6508.1 - Regarding the privacy program, One VA Privacy Violation Tracking System (PVTS), and Privacy Impact Assessment (PIA)
i. VA IT Directive 06-2 - Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations
j. VA Directive 6500 - Information Security Program rescinds Directive and Handbook 6210 and 6212
k. VA Directive 6502- regarding the privacy program, One VA Privacy Violation Tracking System (PVTS), and Privacy Impact Assessment (PIA)
l. 45CFR46 The Common Rule (HHS - Protection of Human Subjects)
m. PVAMC IRB Standard Operating Procedures (SOP)
n. PVAMC HIPAA Human Subjects Research Policies and Procedures

6. CONCURRENCES: Endorsed by the R&D Committee 10/03/2011.

7. RESCISSION: Research Program Policy & Procedure, Research Information Protection Policy, 03/05/2012.

8. FOLLOW-UP RESPONSIBILITY: ACOS, Research & Development Service (R&D)

Michael P. Davey, M.D., Ph.D.
ACOS, Research & Development Service