USE OF DATA AND DATA REPOSITORIES IN VHA RESEARCH

1. REASON FOR ISSUE. This Veterans Health Administration (VHA) Handbook establishes the procedures for the use of data for VHA research purposes, the storage of VHA research data, and the development of VHA research data repositories.

2. SUMMARY OF MAJOR CHANGES. This new VHA Handbook addresses both the use of data for research and clinical and administrative data repositories for research and addresses the development and use of data research repositories.

3. RELATED DIRECTIVES. VHA Directive 1200.

4. RESPONSIBLE OFFICE. The Office of Research and Development (12) is responsible for the contents of this VHA Handbook. Questions may be addressed to (202) 461-1700.

5. RESCISSION. None.

6. RECERTIFICATION. This VHA Handbook is scheduled for recertification on or before the last working date of January 2014.

Michael J. Kussman, MD, MS, MACP
Under Secretary for Health

DISTRIBUTION CO: E-mailed 3/11/09
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 3/11/09

CONTENTS

USE OF DATA AND DATA REPOSITORIES IN VHA RESEARCH

USE OF DATA AND DATA REPOSITORIES IN VHA RESEARCH

1. PURPOSE

This Veterans Health Administration (VHA) Handbook defines procedures on the research use of data and data repositories, including databases and data warehouses. It addresses both the use of clinical and administrative data repositories for research and the development and use of research data repositories.

2. BACKGROUND

Department of Veterans Affairs' (VA) data repositories developed for health care, administration of VA programs, or research, are extremely valuable resources for researchers. Any use of these resources for research must be consistent with the mission of VA including having relevance to the health of Veterans, protecting the privacy of the individuals from whom the data are collected, and complying with all applicable ethical and legal standards.

3. DEFINITIONS

a. **Authorization.** The term authorization means prior written permission for use and disclosure of protected health information (PHI) from the information's source person or research subject or legally authorized personal representative, as required under law, including The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. The written permission is documented on an authorization form.

b. **Coded Data.** The phrase "coded data" means "coded private information" as defined in guidance promulgated by the Department of Health and Human Services (HHS) entitled *Guidance Research Involving Coded Private Information or Biological Specimens*, currently available at: http://www.dhhs.gov/ohrp/humansubjects/guidance/cdebiol.htm.

c. **Common Rule.** The phrase "common rule" means the Federal Policy for the Protection of Human Subjects adopted by federal departments and agencies conducting or supporting human subject research. The Common Rule is codified for VA at Title 38 Code of Federal Regulations (CFR) Part 16.

d. **Data**. For purposes of this handbook, the term "data" means information derived directly from patients or human research subjects or indirectly through accessing databases; it includes information from Deoxyribonucleic Acid (DNA) sequencing. It does not include information derived from research involving animals or other types of research that do not involve human subjects.

e. **Database.** A collection of data or information elements organized in a manner to permit systematic retrieval.

f. **Data Repository.** The term data repository means 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 may also have been created for other purposes such as administrative and clinical purposes. The terms "data repository and "data warehouse" have the same meaning.

g. **Data Transfer Agreement.** This term means a written agreement between the provider and the recipient of data that are transferred from one to the other. It defines 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.

h. **Data Warehouse.** The term "data warehouse" has the same meaning as "data repository."

i. **Data Use Agreement.** For the purposes of this Handbook, the term "data use agreement" means a written agreement governed by 45 CFR § 164.514(e).

j. **Decedent Data**. Decedent data refers to information elements about individuals who are deceased.

k. **De-identified Data.** De-identified data is data that meet the HIPAA Privacy Rule (45 CFR 164.514(b)), VHA Handbook 1605.1, and the Common Rule (38 CFR Part 16) definitions of de-identified (see par.6).

l. **Existing Data.** The phrase existing data means data that have already been collected when the research is proposed to VA reviewing committees.

m. **Health Information.** The term "health information" means any information created or received by a health care provider or health plan that relates to the past, present, or future physical or mental health or condition of an individual or the provision of health care to an individual; or the payment for the provision of health care to an individual. "Health Information" includes information pertaining to examination, medical history, diagnosis, findings or treatment, and includes such information as laboratory examinations, x-rays, microscopic slides, photographs, prescriptions, and other similar data.

n. **HIPAA.** The acronym HIPAA means The Health Insurance Portability and Accountability Act of 1996.

o. **Human Subject**

(1) The term human subject means a living individual about whom an investigator is conducting research:

(a) Obtains data through intervention or interaction with the individual or

(b) Obtains identifiable private information.

(2) An intervention includes all physical procedures by which data are gathered and all manipulations (physical, psychological or environmental) of the subject or the subject's environment that are performed.

(3) Interaction includes communication or interpersonal contact between the researchers and the subject.

p. **Human Subjects Research.** The term "human subjects research" means research that involves human subjects as defined in the Common Rule (38 CFR Part 16) and VHA Handbook 1200.5.

q. **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.

r. **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 Handbook 1605.1.*

s. **Informed Consent.** Free and knowledgeable agreement to participate in research as required under the human subject protection regulations at 38 CFR 16.116. The written document approved by the IRB is sometimes referred to as the informed consent form and, when signed by a research subject, the written informed consent.

t. **Investigator.** An investigator is any individual who conducts research. The investigator must uphold professional and ethical standards and practices, and adhere to all applicable VA and other Federal requirements and to the local VA facility's policies and procedures regarding the protection of human subjects.

u. **Institutional Review Board (IRB).** The IRB is the Committee responsible for the review, approval, and continuing oversight of research involving human subjects in accordance with 38 CFR Part 16 and VHA Handbook 1200.05.

v. **Preparatory to Research.** Within VHA "preparatory to research" refers to activities that are necessary for the development of a specific protocol. 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 application. 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. The preparatory to research activity ends once the protocol has been submitted to the IRB and the Research and Development (R&D) Committee for review.
NOTE: *Pilot studies are not considered to be activities preparatory to research.*

w. **Principal Investigator (PI)**

(1) A PI is a qualified person or persons designated by an applicant institution to direct a research project or program and who usually writes the grant application. The PI oversees scientific and technical aspects of a grant and the day-to-day management of the research. In the event of an investigation conducted by a team of individuals, the PI is the responsible leader of that team. ***NOTE:*** *The Food and Drug Administration (FDA) considers Investigator and Principal Investigator to be synonymous.*

(2) Within VA, a PI must hold an official VA appointment from HRM.

x. **Prospective Research.** Prospective research is a research methodology that requires the generating of new data over time after approval and initiation of the protocol.

y. **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.*

z. **Research and Development (R&D) Committee.** The R&D Committee is the committee responsible for oversight of a VA facility's research program.

aa. **Research Data Repository.** The term "research data repository" means a data repository created from data obtained either to conduct a research protocol(s) or gathered in the course of conducting a research protocol and is maintained after the completion of the research protocol. The protocol may be a primary research project designed to prove or disprove a specific hypothesis or it may be a protocol specifically designed to collect data (either a one-time-only collection of data or an ongoing collection) that will be placed in a research data repository for future use.

bb. **Research Protocol.** As used in this Handbook, "research protocol" means the formal written plan for conducting a research investigation, including but not limited to biomedical, behavioral, social, health service, or educational research investigations, as well as clinical trials.

(1) The research protocol typically includes the background and rationale for conducting the research, the research hypotheses, the objectives or specific aims, and the research methods to be used.

(2) The protocol also includes a discussion of ethical issues, involvement of human subjects, privacy, confidentiality, data storage, and data security.

cc. **Research Team Member.** The phrase research team member(s) includes all investigators and research staff who directly support the research, including research assistants, statisticians, protocol coordinators, collaborators, and any other individuals who have roles in the development, implementation, conduct, analysis, or authorship of publications, presentations, or reports of the research.

dd. **Retrospective Research.** Retrospective research is research that utilizes only data already existing at the time the proposed protocol has been submitted for approval by the IRB and the R&D Committee.

ee. **Remote.** An adjective used to describe the use, processing, access to, transmission, or storage of VA information from locations other than sites in VA facilities.

ff. **VA-approved Research.** The phrase VA approved research means research that has been approved by a VA R&D Committee.

gg. **VA Investigator.** A VA investigator is any individual who conducts research while acting under a VA appointment, including full and part-time employees, without compensation (WOC) employees, and employees under the Intergovernmental Personnel Act (IPA) of 1970.

hh. **VA Protected Health Information (VAPI).** As defined by VA policy including VA Handbook 6500 and VHA Handbook 1605.1, protected health information (PHI) is individually-identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended; Title 20 United States Code (U.S.C.) 1232g, records described at 20 U.S.C. 132g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

ii. **VA Sensitive Information or Data.** As defined in VA Directive 6500, VA sensitive information or data means 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. This term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, propriety information, records about individuals requiring protection under various confidentiality provisions, such as the Privacy Act and HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include:

(1) Individually-identifiable medical, benefits, and personnel information.

(2) Financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information.

(3) Information that is confidential and privileged in litigation such as:

(a) Information protected by the deliberative process privilege;

(b) Attorney work-product privilege; and

(c) Attorney-client privilege.

(4) Other information, which released could:

(a) Result in violation of law or harm, or unfairness to any individual or group; or

(b) Adversely affect the national interest or the conduct of Federal programs.

jj. **VA Research.** The term VA research means the research that has been reviewed and approved by a VA R&D Committee.

4. SCOPE

a. VHA research activities include activities in support of VHA research or VHA's mission. This Handbook applies to all VHA research activities involving data or data repositories. VHA data repositories may be maintained within VA or external to VA, with appropriate prior permissions. Use of VA data repositories by non-VA investigators or non-VA entities may occur only in compliance with all applicable Federal laws, including the Privacy Act of 1974; regulations, including the HIPAA Privacy Rule; and VA and VHA policies.

b. This Handbook provides mandatory requirements that investigators, review committees, and others must follow in developing and implementing sound procedures for the use of data including data from VA and non-VA data repositories, in a manner that is both beneficial for science and protective of the rights and welfare of those who are the subjects of the data.

5. SOURCES OF DATA IN DATA REPOSITORIES

a. Data used for research purposes within VA may come from many different sources, and those sources may be internal or external to VA. Within VA, the data may come from individual research subjects during the conduct of a research protocol or may come from existing research or non-research data repositories. There are numerous external sources including registries, Medicare data, publicly available data, or private sources.

b. VA and VHA non-research data repositories are created to assist VA and VHA in its operations. These data repositories contain information gathered and used for a variety of non-research purposes, such as the ongoing treatment of Veterans, documentation of treatment provided, issues related to co-payments and collections from insurance companies, health care operations, personnel records, Veterans benefits, and statistical analyses to produce various management tracking tools, evaluations, or follow-up reports. Some examples of these non-research data repositories include:

(1) Veterans Integrated Service Network (VISN) data warehouses.

(2) National Databases Systems (vaww.va.gov/nds). ***NOTE:*** *This is an internal VA link not available to the public.*

(3) VA registries, data centers.

(4) Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System (CPRS).

(5) Pharmacy Benefits Management.

(6) The Emerging Pathogens Initiative.

(7) Center for Medicare and Medicaid Services (CMS) data.

6. DETERMINING IF DATA ARE IDENTIFIABLE OR DE-IDENTIFIED

For the purposes of this Handbook, data, including data contained within data repositories, are classified into two types: identifiable and de-identified.

a. **Identifiable Data.** For the purposes of this Handbook the definition of identifiable data is based on both the Common Rule (38 CFR Part 16) and the HIPAA Privacy Rule.

(1) If either condition in following subparagraphs 6a(1) or 6a(2), is met, the data are identifiable.

(a) The identity of the subject is or may be readily ascertained by the investigator or research team member or others from the information contained with in the data. The information is considered private information as defined in 38 CFR 16.102(f)(2) if it 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 (for example, a medical record or information about specific beliefs) or

(b) The subject is identifiable by HIPAA Privacy regulations because:

1. The data contain one or more of the eighteen types of identifiers listed in the HIPAA Privacy Rule in 45 CFR. 164.514(b) (2) (see App. B),

2. The covered entity has actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information; (i.e., there are other data that when combined with the dataset will allow the identification of any individual) (45 CFR 164(b)(2)(ii)), or

3. The data have not met the criteria for de-identification by statistical means as outlined in 45 CFR 164.514(b)(1).

NOTE: *The HIPAA Privacy Rule states that for data to be statistically de-identified the data must be statistically verified by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. This person must give an assurance in writing that there is a "very small" risk that the information could be used to identify the individual and must document the methods and results of the analysis that justify such determination. Statistical verification should be used only when it is determined that this method is necessary for the research and that the person doing the statistical verification has the appropriate experience and expertise.*

(2) Social Security Numbers (SSNs), real or scrambled, are considered identifiers. ***NOTE:*** *Scrambled SSNs are considered identifiers by the HIPAA Privacy Rule because they are unique to the individual and are derived from the SSN. In addition, this rule prohibits re-identification codes from being based on an identifier such as SSN (in whole or in part), name, or other direct identifier.*

(a) Real SSNs may be obtained only when required to meet the specific aims of the research protocol and their collection and use is approved by the IRB and the R&D Committee. To obtain access to real SSNs, the procedures defined by the VHA Privacy Office must be followed.

(b) When a research protocol calls for use of scrambled SSNs, the SSNs cannot be unscrambled by research staff or other individuals without an amendment to the research protocol and approval by the appropriate review committees. All required approvals from VHA Privacy Officer must also be obtained.

b. **De-identified Data.** De-indentified data is health information or other information on human subjects that:

(1) Does not meet the common rule definition of human subjects, and

(2) Meets the HIPAA de-identification requirements:

(a) No longer contains any of the eighteen types of identifiers listed in Appendix B, or

(b) Meets the criteria for de-identification by statistical means as outline in 45 CFR 164(b)(1).

c. **Re-identification of De-identified Data.** Re-identification of de-identified data must be approved in advance by an IRB(s) and R&D Committee(s).

(1) Approval may be given only if the research could not be conducted without re-identification of the data.

(2) Re-identification is necessary to validate the results of the research.

(3) The data being re-identified are contained in a data repository.

(a) If the data repository's policies state that the data repository may contain only de-identified data, then the re-identification of the data may not be done by the repository staff nor can the re-identified data be placed in the repository.

(b) If a research data repository contains only de-identified data by policy, the individual or body responsible for administering the data repository must amend the policies and the protocol governing the research repository before placing re-identified data in the data repository. The new policies permitting storage of re-identified data in the data repository must be approved by the IRB and R&D Committee of record for the facility where the research data repository resides. Only after these approvals have been obtained may the repository contain identifiable data.

(c) If the facility where the research data repository resides does not have a Federal-wide Assurance (FWA) or IRB of record, identifiable data may not be entered into the research repository.

7. SPECIAL CONCERNS FOR USE OF IDENTIFIABLE DATA

a. **Human Subjects Protection.** Research involving the use of identifiable data meeting the criteria for human subjects research must be in compliance with the Common Rule (38 CFR Part 16), all VHA policies related to protections of human subjects in research (e.g., VHA Handbook 1200.5), VHA Handbook 1605.1, and VA Handbook 6500.

(1) Determining if the research involves human subjects is critical because VHA must ensure that there are appropriate protections for the individuals from whom the data are collected and that research complies with applicable ethical standards. This determination dictates which review committees (e.g., the IRB) must approve the research prior to its initiation and if the requirements found in the Common Rule (38 CFR Part 16) apply to the research (see App. A).

(2) Research that involves human subjects is defined in the Common Rule (38 CFR 16.102f). A human subject is a living individual about whom an investigator conducting research obtains data through:

(a) Intervention or interaction with the individual, or

(b) Identifiable private information. This includes research that involves the use of identifiable information or data about human subjects.

(3) Research that does not involve interaction or intervention with human subjects and involves only the use of de-identified data (as defined in pars 3 and 6) is not considered to be human subjects research.

b. **Compliance with all Confidentiality Requirements.** The collection, use, and release of PHI from a data repository must comply with all applicable confidentiality and information security provisions, including the Privacy Act of 1974, the HIPAA Privacy Rule, and 38 U.S.C. 7332 (confidentiality of medical records related to drug abuse, alcoholism, alcohol abuse, infection with the human immunodeficiency virus, and sickle cell anemia), and the information security provisions of 38 U.S.C.

c. **Recruitment of Research Subjects.** Identifiable information must not be used to recruit subjects for research protocols unless approved by the IRB(s) and the R&D Committee(s). In addition to the IRB's approval of the protocol, the IRB must include an approval of a waiver of HIPAA authorization in such instances. The initial contact with the potential human subject needs to be in person or by mail, not by telephone. Additionally, the contact must follow the most recent VA and VHA memoranda or guidance regarding this issue. ***NOTE:*** *These may be found on the Office of Research and Development (ORD) website at:* www.research.va.gov .

d. **Re-contacting Research Subjects.** Identifiable information must not be used to re-contact individuals to obtain additional information unless approved by the IRB(s) and the R&D Committee(s). Re-contacting individuals without previous permission of the individual must meet the same requirements as those set forth by the IRB(s) and R&D Committee(s) for recruitment.

e. **Decedent's Data.** VHA must protect the individually identifiable health information about a deceased individual. A decedent's individually identifiable health information may be used for research purposes without obtaining HIPAA authorization from the decedent's personal representative and without IRB or Privacy Board (PB) approval. ***NOTE:*** *For further requirements including the representations that must be made and information on the use of decedent's data see VHA Handbook 1605.1.*

NOTE: *If the investigator must access a data repository containing individually-identifiable information of living and deceased individuals to identify the deceased individuals and obtain their information, the protocol must then be reviewed by an IRB. The IRB may waive the requirement for informed consent or HIPAA authorization if the applicable criteria are met.*

f. **Use of Data that Contain Coded Private Information.** Use of data that contains coded private information from data repositories requires IRB approval if the data are considered "identifiable" under the human subject protection regulations.

(1) Data that contain coded private information are considered "identifiable" under the human subject protection regulations (38 CFR Part 16) if any member of the research team can access the identities of the source persons from whom the data were obtained. In such cases, review and approval by the IRB(s) and the R&D Committee(s) is required for the research.

(2) Data that contain coded private information are considered "not identifiable" under the human subject protection regulations (38 CFR Part 16) and guidance from the Office for Human Research Protections (OHRP) if there is a written agreement preventing all members of the research team from accessing, or otherwise attempting to ascertain, identities or any identifiers of source persons.

g. **Use of Centers for Medicare and Medicaid (CMS) data.** All requests for use, transmission, distribution, storage, and disposition of CMS data must follow all VA and VHA policies, as well as all CMS requirements and other applicable Federal regulations.

8. PRIVACY AND CONFIDENTIALITY

a. **Privacy and Confidentiality.** Privacy of research subjects and confidentiality of their data are critically important and must be addressed carefully to protect the rights of individual research participants, their families, and their communities. A number of laws, VA and other Federal regulations and policies control how a research subject's private information may be used and when that data can be shared with non-VA investigators or institutions. The laws, regulations, and policies also address use of individually identifiable information even when it does not contain any health data. ***NOTE:*** *Individually Identifiable Health Information is a subset of Individually Identifiable Information*. Privacy laws, regulations, and policies that are applicable to data repository research include, but are not limited to:

(1) HIPAA, Standards for Privacy of Individually Identifiable Health Information (45 CFR Part 160 and Subparts A and E of Part 164).

(2) The Privacy Act (5 U.S.C. 552a) and implementing regulations at 38 CFR 1.575-1.584 and the associated Systems of Records. ***NOTE:*** *The Privacy Act requires agencies to publish a notice of the existence and character of their System of Records in the Federal Register. The System of Records, in part, states what records can be released outside of VA and who may grant permission to release the data.*

(3) The VA Claims Confidentiality Statutes (38 U.S.C. 5701) and implementing regulations 38 CFR 1.500-1.527.

(4) Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records (38 U.S.C. 7332), and implementing regulations at 38 CFR 1.460-1.496.

(5) Confidentiality of Healthcare Quality Assurance Review Records (38 U.S.C. 5705) and implementing regulations at 38 CFR 17.500-17.511.

(6) VHA Handbook 1605.1, Privacy and Release of Information. ***NOTE:*** *VHA Handbook 1605.1, Privacy and Release of Information, addresses many of the issues related to the preceding regulations.*

b. **Local Institutional Policies and Procedures.** Each VA facility conducting research using data covered by the preceding regulations and requirements must develop policies and procedures that ensure compliance with all of the applicable privacy and security regulations and policies.

(1) The policies and procedures should involve review by a knowledgeable person(s) designated to verify that there is compliance with all applicable statutes, regulations, and policies related to privacy and security of data prior to obtaining access to the data. A committee, an IRB, or R&D Committee or subcommittee may be set up to be responsible for the review of privacy and security issues related to the collection, use, storage, transmission, and retention of the data.

(2) Persons with the required knowledge include, but are not limited to: the facility Privacy Officer, the facility Information Security Officer (ISO), a research compliance officer, IRB administrator, a research administrator, IRB members, or others. These persons may need to obtain additional training in HIPAA and the Privacy Act of 1974.

9. STORAGE AND SECURITY

a. All applicable Federal statutes and regulations and VA and VHA policies governing storage and security of data and information must be followed (see VA Handbook 6500). ***NOTE:*** *Links to VA policies may be found at: www.va.gov/vhapublications.*

b. All identifiable data used and maintained as part of a research protocol must be retained or stored for the period of time stated in the applicable Privacy Act System of Records notice, Records Control Schedule (RCS) 10-1, and VA policy. Identifiable information may not be destroyed except with appropriate destruction authority. ***NOTE:*** *If the IRB-approved protocol, the HIPAA authorization, or the waiver of authorization state that identifiers will be destroyed as soon as they are no longer needed for the research, then they must be destroyed in accordance with the protocol, the HIPAA authorization, and/or the wavier of HIPAA authorization.*

c. Each research data repository must have a security plan for all data maintained that is consistent with VA requirements. The ISO needs to be consulted for any questions or to assist in the development of this plan.

d. Transmission and transfer of identifiable data must be performed in accordance with VA security policies.

e. Electronic access to identifiable data in a research data repository must be controlled through appropriate access controls, such as usernames and passwords, in accordance with VA security policies.

10. USE OF DATA REPOSITORIES FOR RESEARCH PURPOSES

VA investigators may use VA and VHA data, including data from existing treatment, payment, operations, or research data repositories, to prepare a VA research protocol, conduct VA-approved research, or to create or maintain a VA research data repository.

NOTE: *Individual investigators or VA employees (compensated by VA or persons appointed under a without compensation (WOC) or 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, III, original notes, documents, and records produced by VA in the course of the protocol are the property of VA.*

a. **Use Preparatory to Research.** Data repositories may be used by VA investigators for activities that are preparatory to VA research without the requirement to obtain either a HIPAA authorization from the subject or waiver of HIPAA authorization by an IRB or a PB. This includes use of PHI for the preparation of a research protocol prior to submission to the IRB(s) or R&D Committee(s). "Preparatory to Research" activity is the only instance of access for research purposes allowed in VHA without a written HIPAA authorization signed by the individual, a waiver of HIPAA authorization by an IRB or PB, or approval by the R&D Committee(s) and the IRB(s). This access is granted only to VHA researchers. Non-VHA researchers may not access VHA data for reviews preparatory to research. Additionally, the following holds true:

(1) The investigator must make the representations necessary for preparatory access as required by the HIPAA Privacy Rule and document it in the investigator's research files. The representations required by the HIPAA Privacy Rule are:

(a) The access to PHI is only to prepare a protocol;

(b) No PHI will be removed from the covered entity (i.e., VHA); and

(c) The PHI accessed is necessary for preparation of the research proposed.

(2) Only aggregate data may be recorded in the researcher’s files and these aggregate data may be used only for background information, to justify the research, or to show that there are adequate numbers of potential subjects that allow the investigator to meet sample size requirements.

(3) Individually identifiable health information will not be recorded.

(4) Data or information reviewed will not be used for contacting or recruiting subjects.

(5) Investigators must comply with all other access requirements set by the repository of interest.

(6) A Data Use Agreement (DUA)-Data Transfer Agreement (DTA) is required if the data are transferred from a data repository to the investigator. The data transferred from the data repository must be destroyed or returned to the data owner or administrator after the data are aggregated. ***NOTE:*** *If the investigator or the investigator's research staff directly accesses a data repository, the investigator must submit the HIPAA representation, described in subparagraph 9a(1), to the data repository owner or administrator with the additional statement that only aggregate data will be recorded for the preparatory to research activity and no individually identifiable information will be recorded*.

(7) ***NOTE:*** *Pilot studies are not considered to be "activities preparatory to research," but are full-fledged research projects that must be approved by the IRB(s), when human subjects are involved, and the R&D Committee(s).*

b. **Use of Data for Research Purposes**

(1) **Minimum Necessary Data.** VA investigators may obtain only the minimum amount of data that are necessary to conduct the research (i.e., minimum necessary data).

(2) **Approved Use.** VA investigators may use identified and de-identified data from data repositories only in accordance with the VA-approved protocol and not for any other purpose.

NOTE: *VA-approved research protocols are defined as those protocols that have been reviewed and approved by a VA R&D Committee(s). If IRB approval(s) is required, the protocol must be approved by the IRB prior to R&D Committee approving the protocol.*

(3) **Required Approvals.** The PI and each co-investigator or investigator, when stationed at different VA facilities or institutions, must obtain the following approvals:

(a) IRB. If the research meets the Common Rule definition of human subjects research, IRB approval must be obtained from the IRB(s) of record for the PI's facility and each co-investigator's facility. IRB approvals of a waiver of HIPAA authorization must be obtained as required.

(b) R&D Committee. All VA research must be approved by the R&D Committee(s) of the PI's VA facility and each co-investigator's VA facility.

(c) Other approvals. Other approvals may include, but are not limited to: union approval (e.g., to perform research on employee data); Privacy Office approval (e.g., for direct access to patient medical records through CPRS); ISO approval; and approvals from the administrator or oversight committee of a specific data repository.

11. DATA IN RESEARCH DATA REPOSITORIES

A research data repository is created when data obtained from implementing a research protocol are placed in a data repository. The protocol may be a primary research project designed to prove or disprove a specific hypothesis, or it may be a protocol specifically designed

to collect data that will be placed in a research data repository for future use. A research data repository can be created only after a research repository protocol is developed and approved by the IRB (if human research is involved) and the R&D Committee.

a. **Collection of Data.** Data may be collected under the following circumstances:

(1) **Identifiable Data**

(a) The investigator has obtained an individual's informed consent approved by the IRB, and HIPAA authorization; or

(b) An IRB finds that all criteria are met under 38 CFR 16.116(d) to waive the requirement for a research informed consent. In addition, the IRB or Privacy Board waives the requirement for a HIPAA authorization and documents that all criteria under 45 CFR 164.512(i)(2) are met.

(2) **De-identified Data**

(a) De-identified data (as defined in paragraphs 3 and 6 of this Handbook) may be collected without informed consent or HIPAA authorization after the protocol has received the appropriate approvals. ***NOTE:*** *Someone other than the investigator must verify that the data are de-identified. This individual may be the facility Privacy Officer, a member of the IRB, or other knowledgeable person as defined in the facility's Standard Operating Procedures (SOPs).*

(b) A protocol involving de-identified data needs to be approved only by the R&D Committee. The R&D Committee must confirm the data are de-identified.

NOTE: *If the investigator must review identifiable data prior to the data being de-identified, then an informed consent and HIPAA authorization must be obtained from the individual or the IRB must waive the informed consent and HIPAA authorization. If exempt from IRB review under the Common Rule (an informed consent or waiver of informed consent is not required), a HIPAA authorization or waiver of authorization by an IRB or PB may still be required.*

b. **Sources of Data.** Sources of data include:

(1) **Data Obtained Directly from Research Subjects**. Data may be collected from research subjects directly through such means as medical tests, interventions, questionnaires, or surveys.

(2) **Data Obtained from Sources other than Directly from the Subject.** Data may be collected from indirect sources such other research projects or research data repositories if appropriate approval has been obtained for such re-use of the data. Data also may be collected from non-research sources such as from a third party, or from review of the subject's administrative, medical, or other records. ***NOTE:*** *Use or reuse for research of data obtained from indirect sources, including other research projects, must obtain the same IRB or R&D Committee approvals as any other research project.*

(3) **Research Data Repository.** Research data are not considered to constitute a "research data repository" and are not subject to the requirements of this Handbook, if the data are:

(a) Collected for a specific research protocol;

(b) Never used for any other research purpose while retained for the research project for which the data were collected; and

(c) Destroyed after the required record retention period.

NOTE: *These data may not be used for other research purposes unless allowed by the informed consent under which they were collected, approved by the IRB, and placed in a research data repository.*

12. RESPONSIBILITIES OF VA FACILITIES RELEASING IDENTIFIABLE OR DE-IDENTIFIED INFORMATION FROM THEIR RECORDS TO ANOTHER VA SITE FOR RESEARCH PURPOSES

VA facilities that release identifiable or de-identified information for use in a VA-approved research protocol to a VA investigator or to a VA research repository are not considered to be engaged in research if the releasing facilities do not have any other role in the research, i.e., the VA facility will not be considered "engaged" in research solely on the basis of this transfer of data. The releasing VA facility does not need to hold a FWA, but if it does, the releasing VA facility's IRB and R&D Committee is not responsible for reviewing specific individual research protocols, unless an investigator or other member of the protocol's research team are at the same facility as the research data repository. Prior to the release of information the following steps must occur:

a. A Combined DUA-DTA must be implemented between the releasing facility and the receiving VA investigator. The Combined DUA-DTA must meet all VHA requirements.

b. The release of the information may occur only after the releasing facility's Privacy Officer and ISO have reviewed the request to ensure that all privacy and security procedures governing transfer of the data have been met. ***NOTE:*** *The releasing facility may require other facility specific procedures*.

c. The request, to the facility with the research data repository, for release of data must include the following for all sites engaged in the protocol:

(1) Documentation of IRB(s) approval(s) of the protocol if the project is considered human subjects research. If the request is for identifiable data that will be placed in a research repository, documentation that the research repository operations are defined in a VA-approved repository protocol for which the IRB approval is current.

(2) Documentation of the IRB's waiver of informed consent and waiver of HIPAA authorization if the subject of the information has not signed an informed consent and HIPAA authorization for the new protocol prior to the release of identifiable information.

(3) Documentation of R&D Committee approval of the research protocol or the research repository.

(4) If the request is for information that will be placed in a research repository, the request for data must include a copy of the repository protocol that includes a justification for the

information request, a summary of the research data repository's objectives, and a copy of its privacy and security plan.

NOTE: *The transfer of the data must be in compliance with all VA privacy and information security requirements.*

13. ADMINISTRATION OF RESEARCH DATA REPOSITORIES

A VHA research data repository is a resource for VA investigators, and it must remain under the control of VA. The repository may contain either identifiable or de-identified data. The data may be released to non-VA personnel or non-VA entities only in accordance with VHA Handbook 1605.1. Data repositories must be maintained and operated in accordance with the requirements of this Handbook and all other applicable VA and VHA policies and regulations.

a. **Administrative Structure.** The administrative structure of the research data repository must always include a VA investigator who is responsible for all activities of the data repository. ***NOTE:*** *An investigator under a WOC or IPA appointment may not serve as the sole administrator of a VA data repository.* Its oversight may involve a number of persons and committees including, but not limited to: a repository administrator, information technology specialist, data repository specialist, and various oversight committees (e.g., scientific, ethical, compliance, or security).

b. **Oversight Responsibilities.** The functions that must be carried out by an administrator of a research data repository include:

(1) Developing policies and procedures that include requirements for releasing data from the repository and mechanisms for verifying approval of the research by the IRB(s), if the request is for identifiable data, and R&D Committee(s) of record for the investigator(s) who is requesting the data;

(2) Reviewing requests to access data;

(3) Keeping records;

(4) Maintaining the privacy of subjects and the confidentiality of the data in the repository; and

(5) Ensuring data in the repository are stored and secured according to VA requirements.

c. **Oversight Committee.** One or more committees are to be established to provide scientific and ethical advice for repositories that contain a number of different databases or provide data broker services. The composition and charge of the committee(s) needs to be based on the size and complexity of the data repository. ORD is to be consulted for specific guidance on the need for separate scientific and ethics oversight committee versus a combined scientific and ethics oversight committee.

(1) **Scientific Oversight Committee**

(a) This Committee is composed of investigators with scientific expertise and experience with data from databases or data repositories, health systems research, epidemiology, statistics, and any disease areas related to the intended uses of the data.

(b) This committee is responsible for assisting the data repository administrator in developing policy on the use of the data and for providing technical and scientific recommendations to the research repository administrator and investigators wishing to access data in the data repository.

(c) Depending on the data repository's written procedures, the committee may approve or disapprove data use requests or make recommendation to the administrators of the data repository to approve or disapprove data use requests.

(2) **Ethics Oversight Committee**

(a) This Committee is composed of experts in the ethical and legal implications of research involving human subjects, use of large data bases or data from data repositories, as well as experts in the relevant scientific disciplines.

(b) This Committee is responsible for:

1. Reviewing requests for data for the protection of human research subjects and advising the database owner or administrator on possible actions related to the requests; and

2. Providing a disinterested review of the repository's activities, including policies, procedures, and proposals for use of stored data.

d. **Stable administrative oversight.** A concerted effort must be made to ensure that the administrative oversight of the research data repository remains stable. Measures to ensure stable administrative oversight include:

(1) Obtaining approval from the IRB, if applicable, and R&D Committee responsible for oversight of the research data repository for any proposed changes in administrative oversight.

(2) Ensuring continued control of the data and compliance with current VA and VHA requirements if administrative oversight is transferred to another qualified VA-compensated investigator or administrator.

(3) Combining the research data repository with another VA research data repository.

(4) The IRB, if applicable, and the R&D Committee must approve the appointment of a new administrator of a research data repository, and combining research data repositories.

e. **Termination.** A research data repository may be terminated only under the direction of the IRB or R&D Committee responsible for the oversight of the repository.

f. **Destruction of the data.** If the data are collected under an informed consent, the informed consent under which the data were collected must include the possible options for disposition of the data.

(1) Data may need to be destroyed if appropriate control of the data and compliance with VA and VHA requirements cannot be maintained. Destruction of data in a data repository must be done in accordance with all VA and VHA records disposition requirements, including the Privacy Act Research System of Records "Veterans, Employee, Research Records-VA" (34VA12). Decisions regarding disposal or disposition of the data must be made by the responsible oversight committee(s) (i.e., IRB or R&D Committee).

(2) After the data or record retention period has ended, the data is either to be destroyed or, if appropriate approvals have been obtained for such re-use of the data, placed in another research data repository.

NOTE: *VHA policy requires that all research records must be retained for a minimum of 5 years after the completion of a protocol and in accordance with VHA's Records Control Schedule (RCS 10-1), applicable FDA and HHS regulations, or as required by outside sponsors and then destroyed in accordance with VHA's RCS 10-1 requirements. Any documentation that is required in writing by the HIPAA Privacy Rule (e.g., the authorization or data use agreement) must be retained for 6 years from the date of its creation or the date when it was last in effect, whichever is later (45 CFR 164.530(j)). For example, VHA must be able to account for any disclosures outside the VA for research purposes for a period of 6 years or the life of the record (see VHA Handbook 1605.1).*

g. **Location of VA Research Data Repositories.** All VA research data repositories must be physically located within space owned or leased by VA. The local ISO and VA Police Service must determine that the security for the data repository and the location where the data repository is to be located meet applicable VA security requirements prior to data being placed in the space.

h. **Access to Research Repository Data and use of Data.** A VA investigator may access data from a research data repository only through a specific protocol approved by the investigator's own facility's IRB (if the protocol involves human subjects), and R&D Committee. The request for access must then be approved by the repository's administration in accordance with the repository's written procedures.

(1) The protocol must include sufficient safeguards to prevent compromising the confidentiality of research subjects' data and must address all other issues found in Paragraph 16, "Responsibilities of Investigators."

(2) The use of the data must be clearly described and consistent with the informed consent (when applicable) and HIPAA authorization (when applicable), under which the data were collected. Data may be reused for other purposes only if:

(a) The use is "preparatory to research" (see par. 10); or

(b) A new or amended protocol is developed and approved by the investigator's IRB (if human subjects research) and R&D Committee, and the data repository administrator.

(3) A Combined DUA-DTA must be completed by the requesting investigator prior to the data being released. The Combined DUA-DTA defines the terms and conditions of the agreement to access the data or to transfer the data to other facilities (see App. C).

(4) Subjects whose information is contained in the data repository may be contacted for additional data or to recruit them for a protocol only in accordance with current VA and VHA policies. In addition, the approved protocol must address re-contacting the subjects.

i. **Records.** Regardless of applicable administrative controls, adequate records of activities and operations of the research data repository must be maintained. The standard operating procedures (SOPs) for the data repository determine who is responsible for maintaining records and how the records must be maintained. Data and record retention requirements apply to data repository records. Records include, but are not limited to:

(1) Records of all sources of data deposited in the research data repository, including type of data; the date the data were deposited; and copies of the protocols, including the approved consent form template and HIPAA authorization template under which original data were collected. ***NOTE:*** *If the data are derived from an administrative data repository, the research repository's IRB or R&D Committee may require evidence that informed consent and HIPAA authorization were not required for its protection*.

(2) Records regarding any new use of the data. These records must include: a copy of the new use protocol, the protocol's PI, and official IRB and R&D Committee approval notifications, including: initial and continuing review, documentation of waivers of informed consent and HIPAA Privacy Rule authorization (where appropriate), Access Agreement, Combined DUA-DTAs, and all records of disposition of data after termination of the protocol.

(3) Record of data distribution including the location where the data will be stored and the name(s) and location(s) of the individual receiving the data.

(4) Records of all communication with investigators requesting and receiving permission to use data.

(5) Records of research data disclosure to a subject, a subject's family, a subject's physician, or a third party, where legally permitted.

(6) Minutes of meetings of the Scientific Oversight Committee, the Ethics Oversight Committee, when applicable, including attendance, discussion, and votes.

(7) Records of all IRB and R&D Committee actions relevant to the research data repository.

j. **Maintaining written procedures for operations.** The research data repository must use written SOPs. The SOPs must address, at least, the following subjects:

(1) Administrative activities;

(2) Conflict of interest (COI);

(3) Tracking of data;

(4) Reuse of data including who may approve the reuse;

(5) Disclosure to subjects and conditions under which disclosure is or is not allowed;

(6) Destruction of data due to the repository's termination;

(7) Access agreements (i.e., Combined DUA-DTA);

(8) Requiring and maintaining protocols and IRB and R&D Committee approvals; and

(9) Security and oversight.

k. **Reporting requirements**

(1) A report on the research data repository's status must be made to the IRB and the R&D Committee at the VA facility housing the research data repository, at an interval determined by the IRB or the R&D Committee, but at least annually. This report must include, but not be limited to, a description of the following:

(a) The sources of data being added to the research repository and the protocol(s) under which they were collected.

(b) The type of data released to others for use, the protocol(s) under which they were used, and the planned disposition of the data once the protocol is terminated.

(c) Any events involving risk to subjects or others, such as a breach of privacy or confidentiality. ***NOTE:*** *Problems may need to be reported promptly depending on the nature of the risk, the incident, and current applicable reporting requirements.*

(d) Findings linking a negative impact on the health status of individuals in the data repository with identified causal factors, including whether there may be a clinical intervention.

(e) All reporting requirements for active protocols (see VHA Handbook 1200.5). The reporting requirements include those for continuing review, unanticipated problems involving risks to subjects or others, protocol violations, and termination of protocols. Risks to institutions may also be appropriate for reporting.

(2) All privacy and security incidents regarding the VA research data repository must be reported in accordance with VA Incident Response policies and requirements. ***NOTE:*** *The facility ISO must be contacted for the current requirements.*

l. **Conflict of interest (COI).** All COI must be identified and managed in compliance with applicable COI regulations and policies including those of VHA, criminal COI statutes at 18 U.S.C. 11,and the Executive Branch Standards of Conduct at 5 CFR Part 2635. The investigator, research repository administrator, and any other key personnel associated with the repository must disclose any COI as provided in VA and VHA policies on COI; and they must seek advice on resolving identified conflicts from a VA ethics official at the Office of General Counsel or Regional Counsel.

(1) **Financial COI.** The IRB may determine that direct commercial ties must be discussed during the informed consent process. In addition, the IRB may require that a mechanism for appropriately managing such COI must be developed in consultation with a VA ethics official.

(2) **Role conflict and conflict of responsibilities.** If the investigator or repository administrator is both the medical caregiver and the investigator, the investigator must be aware of the potential conflicts created by functioning in dual roles (caregiver and researcher) and ensure that they are appropriately managed. This management of the COI may require such actions by the IRB or others that may include reassignment of responsibilities of an investigator to another qualified individual who does not have a COI. Investigators need to be mindful of potential conflicts created by their own unique personal or professional relationships, roles, and responsibilities. In determining if a COI exists and in resolving any such conflict identified, investigators must seek the advice of the ACOS for R&D, VA regional counsel or the VA-designated ethics officer, as appropriate.

14. ROLE AND RESPONSIBILITIES OF THE IRB

a. **VA facility housing the research data repository.** The IRB of record for the VA facility that houses the research data repository is the IRB responsible for the research data repository.

(1) This IRB is responsible for:

(a) Complying with all requirements in VHA Handbook 1200.05 and all COI policies, especially those related to commercial ties of the investigator and conflict of role, as well as the suggested strategies to manage conflicts. These strategies may include, but are not limited to; discussions with the potential research subjects about the conflicts, or requiring another qualified individual to conduct the informed consent discussion, a discussion the includes information on the COI;

(b) Reviewing and approving the creation and operations of the research data repository; and

(c) Conducting reviews of the research repository's activities at least once a year. As part of the review, the IRB must receive the information cited in subparagraph 13k. ***NOTE:*** *Unanticipated problems may need to be reported promptly depending on the nature of the risk, the type of incident, and current applicable reporting requirements (e.g., requirements of Office of Information and Technology (OI&T), OHRP, ORO).*

(2) This IRB is not responsible for approving individual research protocols that propose to use data from the research data repository unless:

(a) One or more of the investigators is from the same VA facility that houses the research data repository, or

(b) Written procedures of the research data repository require such approval.

b. **VHA Facility(ies) from which data originated.** Once data (identifiable or de-identified) have been transferred from a local VHA facility, that facility's IRB is no longer responsible for reviewing and approving research protocols accessing those data, if no part of the

research is to be conducted at the facility or with that facility's resources (e.g., staff, equipment) (see par. 12).

NOTE: *The transfer of the data must be in compliance with all VA privacy and information security requirements.*

c. **VA facility(ies) of the investigator(s) for individual research protocols.** The IRB(s) of record for the VA facility of each PI or co-investigator must approve the individual research protocol before the individual can access any data. Other responsibilities include, but are not limited to:

(1) Complying with all requirements of VHA Handbook 1200.5, including provisions for initial and continuing review of the research protocol. In considering the proposed research, the IRB(s) must review:

(a) Sufficient information from the investigator to adequately assess the request including if the data to be used are reasonable and necessary to conduct the research.

(b) The source of the data and the purpose for which the data were originally collected, including whether they were collected for research purposes.

1. If the data were collected for other research projects, whether the reuse is consistent with the consent under which they were collected.

2. If the data were collected for administrative or clinical reasons whether the guidelines under which they were collected allow for storage in a specific data repository and reuse for research purposes.

3. If the data is to be obtained from an administrative or clinical data repository, whether the administrative policies and procedures for the data repository allow for use of the data for research purposes, and if so, whether they allow for it as identified, de-identified, or coded. ***NOTE:*** *Although some data obtained from an administrative or clinical data repository may be used for a research protocol, the administrative policies for the administrative or clinical repository may not allow the data to be placed in a research data repository for reuse, and use in any other research projects would require requesting the data from the original source repository.*

(c) A description of the data including if they are identified, de-identified, or coded. If the data are identified or coded, a justification for use of this type of data is required (see par. 7).

(d) A justification for the use of real SSNs, if they are requested.

(e) Information on data storage and security including:

1. All locations where the data is to be stored, accessed, or used including servers, desktop personal computers, laptops, non-VA locations, or portable media. ***NOTE:*** *The subject's contact information including name, address, SSN, and phone number need to be maintained in a separate file at the VA and be linked with the remainder of the subject's data only when it is necessary to conduct the research.*

2. Information on the need and mechanism for copying data from a secure VA server and transmitting or transporting data to other locations.

3. Plans for the destruction of data if they are not to be placed in a data repository after the protocol is completed and the retention period has expired.

(f) Information on any plans to contact, re-contact, or recruit the patients or individuals for further information, or to recruit them for any other research project.

(g) How the privacy and confidentiality of subjects associated with the data is to be maintained.

(h) Information on any plans to use the current data and the data obtained from the proposed project for future research. If data is to be retained for future research, the protocol must describe the repository in which they are to be maintained, its location, and its security measures. ***NOTE:*** *If the data are retained for future research, the data repository must be established and maintained in accordance with this Handbook.*

(i) If any data is going to be released outside VA. If this is the case, a discussion regarding why this release is consistent with the VHA policy, the Privacy Act, and HIPAA must occur.

(j) Information on the PI's ability to finish the protocol.

(k) Documentation that all research team members are to be working within their scope of practice, privileges, or functional statements.

(2) Determining whether or not the project is research as defined by the Common Rule as found in 38 CFR 16.102(d). If the VA facility does not have a FWA and an IRB of record, this determination is to be the responsibility of the R&D Committee of record for the investigator's facility. The R&D Committee may consult with another VA facility's IRB or a person with expertise in this area.

(3) Determining, if the research activity is human subjects research, if it is exempt from review by the IRB in accordance with 38 CFR 16.101(b). If the facility does not have an FWA or IRB of record, non-exempt human subjects research cannot be conducted at the facility.

(4) Approving or exempting the protocol from IRB review. If an IRB review is required, the review may be either by the full board, or if all criteria found in 38 CFR 16.110 are met, by an expedited review process. The protocol must be approved in the same form by each investigator's IRB, and therefore, any differences in the conditions for the IRB approval must be reconciled before the research is initiated.

(5) Waiving informed consent and HIPAA authorization if the appropriate criteria are met. If the research does not meet the criteria, the IRB must approve a written informed consent form, and the investigator must obtain informed consent from each subject. If the requirements for waiver of the HIPAA authorization have not been met, the investigator must obtain a written authorization from each subject. The authorization must meet all criteria for a HIPAA authorization that are found in VHA Handbook 1605.1.

(6) Ensuring that if the data were collected during the conduct of a previous research protocol, the reuse in the new protocol is consistent with the original informed consent. If it is not, or the original informed consent did not address the reuse of the data, the IRB must specifically approve the proposed reuse. ***NOTE:*** *If the informed consent states specifically that the data will not be used for other purposes, it cannot be reused.* Reuse may be approved where:

(a) The subjects must again provide consent and a new HIPAA authorization obtained; or

(b) The subject's name SSN, scrambled SSN or date of birth are not used plus all criteria are met to waive informed consent and waive HIPAA authorization; or

(c) The research is exempt from IRB review (38 CFR 16.101), and the criteria for waiver of HIPAA authorization have been met; or

(d) The data are de-identified prior to use (see definitions in pars. 3 and 5).

(7) Performing continuing review, unless the protocol is determined to be exempt. ***NOTE:*** *If it is exempt, the R&D Committee is still required to complete both the initial review and annual review of the research.*

(8) Ensuring the data accessed from the data repository are required by the approved protocol and used only for the purposes defined in the approved protocol. Reuse of the data may not occur without approval of a new protocol, unless the use is preparatory to research as defined in paragraphs 3 and 10.

(9) Approving research. To approve the research, the IRB must make all determinations required by 38 CFR 16.111. In addition, the IRB must determine if the use of the data is allowed by and is consistent with both the Privacy Act of 1974 and the HIPAA Privacy Rule.

(10) When acting as a PB, ensuring that all HIPAA Privacy Rule requirements have been fulfilled.

(11) Obtaining, at its discretion, the assistance of ad hoc reviewers or consultants including the facility's Privacy Officer and ISO. ***NOTE:*** *Current VHA policy requires appointment of the Privacy Officer and ISO to the IRB or the R&D Committee.*

NOTE: *IRB approval is not required if the research is determined to not involve human subjects. The VA facility's policies must state which committee is responsible for making the determination that the research does not involve human subjects, the criteria for this determination, and if the chair or the chair's designee may make the determination. The R&D Committee may make this determination only when the facility does not hold an FWA.*

15. ROLE AND RESPONSIBILITIES OF THE R&D COMMITTEE

a. **VA facility housing the research data repository.** The R&D Committee of record for the VA facility that houses the research data repository is responsible for oversight of the research data repository.

(1) The R&D Committee is responsible for:

(a) Complying with all requirements in VHA Handbook 1200.1.

(b) Reviewing and approving creation and operation of the research data repository, including the research repository SOPs. ***NOTE:*** *If the data repository contains identifiable data, IRB approval must first be obtained*.

(c) Conducting reviews of the research repository's activities at least once a year. As part of the review, the R&D Committee must receive the information cited in subparagraph 13k. ***NOTE:*** *Unanticipated problems may need to be reported promptly depending on the nature of the risk, the type of incident, and current applicable reporting requirements (e.g., requirements of OI&T, OHRP, ORO).*

(2) The R&D Committee is not responsible for approving individual research protocols that propose to use data from the research data repository unless:

(a) One or more of the investigators is from the same VA facility that houses the research data repository, or

(b) Written procedures of the research data repository require such approval.

b. **VHA facility(ies) from which data originated.** Once data (identifiable or de-identified) have been transferred from a local VHA facility, that facility's R&D Committee is no longer responsible for reviewing and approving research protocols accessing those data if no part of the research will be conducted at the facility or with that facility's resources (e.g., staff, equipment) (see par.12). ***NOTE:*** *The transfer of the data must be in compliance with all VA privacy and security requirements.*

c. **VA facility(ies) of the investigator(s) for individual research protocols that will use data from a data repository (research or non-research).** The R&D Committee(s) of record for the facility of each principal investigator and for each co-investigator (if they are not at the PI's facility) must review and approve the individual research protocol before the data can be accessed. It also must comply with all the requirements of VHA Handbook 1200.1, including provisions for initial and continuing review of the research protocol. In reviewing the proposed research, the R&D Committee:

(1) Must receive sufficient information from the investigator to adequately assess the request including:

(a) The source of the data and the purpose for which the data were originally collected, including whether they were collected for research purposes.

(b) If the data were collected for other research projects, whether the reuse is consistent with the research informed consent under which they were collected.

(c) If the data were collected for administrative or clinical reasons, whether the guidelines under which they were collected allow for storage in a specific data repository and reuse for research purposes.

(d) If the data is to be obtained from an administrative or clinical data repository, whether the administrative policies and procedures for the data repository allow for use of the data for research purposes, and if so, whether they allow for it as identified, de-identified, or coded. ***NOTE:*** *Although some data obtained from an administrative or clinical data repository may be used for a research protocol, the administrative policies for the administrative or clinical repository may not allow the data to be placed in a research data repository for reuse, and use in any other research projects requires requesting the data from the original source repository.*

(e) A description of the data including if they are identified, de-identified, or coded. If the data are identified or coded, a justification for use of this type of data is required.

(f) A justification for the use of real SSNs, if they are requested.

(g) Information on data storage and security including:

1. All locations where the data is to be stored, accessed, or used including servers, desktop personal computers (PCs), laptops, non-VA locations, or portable media. ***NOTE:*** *The subject's contact information including name, address, SSN, and phone number should be maintained in a separate file at the VA and be linked with the remainder of the subject's data only when it is necessary to conduct the research.*

2. Information on the need and mechanism for copying data from a secure VA server and transmitting or transporting data to other locations.

3. Plans for the destruction of data if they will not be placed in a research data repository after the protocol is completed and the retention period has expired.

(h) Information on any plans to contact, recontact, or recruit the patients or individuals for further information or to recruit them for any research project (see par. 7).

(i) How the privacy of subjects associated with the data and data confidentiality will be maintained.

(j) Information on any plans to use the current data and the data obtained from the proposed project for future research. If data will be retained for future research, the protocol must describe the repository in which they are to be maintained, its location, and its security measures. ***NOTE:*** *If the data are retained for future research, the research data repository must be established and maintained in accordance with this Handbook.*

(k) If any data is to be released outside VA, a discussion regarding why this release is consistent with the VHA policy, the Privacy Act, and HIPAA must occur.

(l) Information on the PI's ability to finish the protocol.

(m) Documentation that all research team members are to be working within their scope of practice, privileges, or functional statements.

(2) If the VA facility does not have a FWA and an IRB of record, it must be determined whether or not the project is human subjects research, as defined by the Common Rule as found

in 38 CFR 16.102(d) and (f). ***NOTE:*** *The R&D Committee may consult with another VA facility's IRB or a person with expertise in this area.* If it is determined that the activity is human subjects research, the R&D Committee(s) may not approve the research unless the VA facility has an FWA and the research is first approved by the facility's IRB(s) of record or exempted from IRB review by the facility's IRB(s) of record.

(3) Must ensure that, if the data were collected during the conduct of a previous research protocol, the reuse in the new protocol is consistent with the original informed consent. If it is not, or the original informed consent did not address the reuse of the data, the R&D Committee must receive documentation that the IRB specifically-approved the proposed reuse. ***NOTE:*** *If the informed consent states specifically the data will not be reused for other purposes, it cannot be reused*. Reuse may be approved where:

(a) The subjects must again provide consent and a new HIPAA authorization must be obtained;

(b) The subject's name, SSN, scrambled SSN, or date of birth are not used, plus all criteria are met to waive informed consent and waive HIPAA authorization;

(c) The research is exempt from IRB review (38 CFR 16.101), and the criteria for waiver of HIPAA authorization have been met; or

(d) The data are de-identified, as defined in paragraphs 3 and 6 of this Handbook, prior to use.

(4) Must perform a continuing review of the protocol.

(5) Must ensure the data accessed from the data repository are required by the approved protocol and used only for the purposes defined in the approved protocol. Reuse of the data may not occur without approval of a new protocol unless the use is preparatory to research as defined in Paragraphs 3 and 10.

d. **VA facilities with no IRB of record and no FWA.** The R&D Committees for VA facilities with no IRBs of record and no FWA, must comply with all the requirements of VHA Handbook 1200.1, and they must make determinations regarding whether the project is research, and if the project is research, whether it is human subjects research as defined by the Common Rule (38 CFR 16.102) ***NOTE:*** *The R&D Committee may delegate these determinations to the Chair or other voting member. The VA facility's policies must state who makes this determination and the criteria that is used for this determination. The R&D Committee may consult with a VA IRB or a person with the appropriate expertise in this area*.

(1) If the R&D Committee or designated voting members of the committee. determines that the project is human subjects research, the research may not be conducted at that facility unless the facility obtains an FWA, identifies an IRB of record according to VHA policies, and the designated IRB and R&D Committee approve the research.

(2) The R&D Committee may, at its discretion, obtain the assistance of ad hoc reviewers or consultants including the facility's Privacy Officer and ISO.

16. RESPONSIBILITIES OF THE INVESTIGATORS

a. **Protocol design and conduct.** The investigator's primary responsibilities for designing and conducting research involving the use of data repositories are similar to those for other types of studies. If the protocol involves human subjects then all policies related to human subjects research, including those in VHA Handbooks 1200.5 and 1605.1, are applicable. In addition, the protocol must incorporate all information required by the review committees including the following:

(1) The type of data (identified or de-identified) including what PHI elements are to be obtained. ***NOTE:*** *The data that will be requested for or obtained for the research must be reasonable and necessary to conduct the research*.

(2) The source of data (e.g., subjects, non-research data repositories, research data repositories, publicly available, VA source, non-VA source).

(3) How and where the data will be stored (e.g., electronic, paper records, approved VA-owned or VA-leased space), how the data will be transmitted, and how the data will be secured during storage, use, and transmission both during the conduct of the research protocol and after the protocol is completed. The discussion is to address how the planned storage meets all applicable requirements. ***NOTE:*** *The investigator is encouraged to consult the facility's ISO and VA Police Service during the development of the protocol to ensure compliance with all information security requirements and physical security requirements.*

(4) Plans to store data for future research. If the data is stored for future research, there must be a description of research data repository, its location, and its security measures. ***NOTE:*** *If the data are retained for future research and placed in a research data repository, if not pre-existing, the research data repository must be established and maintained in accordance with the provisions of this Handbook.*

(5) Plans to share with others including other researchers (VA and non-VA). If the data were collected through a research project, discussion of whether or not the original informed consent allowed for such reuse of the data and if the reuse is consistent with the HIPAA authorization that was obtained.

(6) Justification for the use of any identifiers.

(7) Justification that the data requested represent the minimum necessary to conduct the research.

(8) A discussion of plans for obtaining informed consent and HIPAA Authorization, or for requesting the IRB to waive these requirements. If the investigator requests that the requirement for a HIPAA Authorization be waived, justification for this request must be included in information submitted to the IRB or PB.

b. **Approvals.** No research involving data repositories can be initiated before the investigator(s) obtains all required approvals in writing. These approvals include, but are not

limited to the relevant IRB(s) (if the protocol involves human subjects) and the R&D Committee(s).

c. **Maintaining the privacy and confidentiality of all PHI and sensitive data.** The investigator is responsible for maintaining the privacy and confidentiality of all PHI and sensitive data in accordance with applicable VA and VHA information confidentiality and security requirements. ***NOTE:*** *The investigator is encouraged to consult with the facility's Privacy Officer and VA Police Service during the development of the protocol to ensure compliance with all privacy laws, regulations, and policies.*

d. **If the investigator leaves VA.** If the investigator no longer holds an appointment as an employee (compensated or uncompensated) or an IPA, all research records, data, and data in repositories must remain at VA and under VA control. All data and records are the property of VA. The data may not be copied or removed unless all requirements for use of VA data by non-VA investigators are met. ***NOTE:*** *The Privacy Officer must be consulted if an investigator receives a request for data from a non-VA investigator.*

17. RESPONSIBILITIES OF THE OWNER OR ADMINISTRATOR OF NON-RESEARCH DATA REPOSITORIES

a. The owner or administrator of each data repository or data warehouse must develop policies and procedures for responding to requests for data. Responsibilities of the owner or administrator of research data repositories are to be found in Paragraph 12 of this Handbook. ***NOTE:*** *Although the term owner or administer is used within this Handbook, VA information is owned by the Administration, Staff Office, or other Agency component that generates or gathers the information to perform statutory responsibilities. The information system itself is owned by VA Office of Information and Technology.* These policies and procedures need to address:

(1) The use of the data for research purposes. This requires:

(a) Documentation from all co-investigators' facilities if the co-investigators are not from the same facility as the principal investigator, and

(b) The following documentation from the investigator:

1. IRB approval(s) if human subjects research.

2. R&D Committee(s) approval.

3. HIPAA authorization or waiver of HIPAA authorization if human subjects research.

4. Research informed consent or waivers of consent if human subjects research.

5. Summary of protocol or full protocol to include:

a. Why access is needed.

b. What databases are to be accessed.

c. The specific data needed including a justification for the use of identifiers, especially if real SSNs are to be used.

d. Where data is to be stored (VA and non-VA locations) and where copies are to be stored (server, PC, laptop, memory sticks).

e. How data is to be secured (physical security, encryption, passwords etc.)

f. Who will have access to the data, VA employees (compensated or WOC), non-VA investigators, contractors, etc.

g. Disposition of data at end of the protocol and the required retention time period, e.g., placed in another VA repository, destroyed, or de-identified (if data are identifiable).

6. Documentation that the investigators and research staff have completed the relevant human subjects, cyber security, and privacy training and the training is up to date.

(2) The roles of the Privacy Officer and ISO at the facility were the data repository resides including their role(s) in ensuring the transfer of data is in compliance with all applicable VA policies.

(3) If the data may be reused for other research projects conducted by the same investigator and if the projects are approved for such reuse by the IRB and R&D Committee.

(4) Whether the data are permitted to be placed in a research repository for use by other VA investigators and if the projects using the data are approved by the IRB(s) and R&D Committee(s).

(5) If the original protocol is amended to allow other uses of the data and the amendment is approved by the IRB(s) and R&D Committee(s):

(a) Must the Combined DUA-DTA be re-negotiated by the database owner or administrator and the investigator, or

(b) Will the database owner or administrator require a new IRB and R&D Committee approved protocol instead of an approved amendment if additional data are required.

(6) The specific logistics of how the data are requested, what steps to be taken by each person such as approving officials, etc., what must be done for the data to be transferred.

b. Other potential issues that may be addressed in the policies include:

(1) Requiring submission of all manuscripts resulting from the use of the data to the database owner or administrator for review to ensure appropriate interpretation.

(2) Requiring review and written approval from the Privacy Officer and ISO at the releasing facility.

(3) Disposition of any data beyond the minimum necessary data to conduct the research. The data owner or administrator must develop policies that address what must be done when the PI receives more data than the minimal necessary data. This may occur when:

(a) The database administrator does not have the resources to develop project specific data,

(b) The data extract is technically complex and best done by the research team, or

(c) The investigator does not know if a given database contains all required data fields or if some data within the data fields are missing.

(4) Requiring that all reports of serious adverse events and unanticipated problems associated with the project for which data were released, be sent to the database owner or administrator, including privacy or security breaches.

NOTE: *The research data repository owner may contact ORD for assistance in developing appropriate policies and procedures that would be applicable to research requests.*

18. TRAINING

a. **Personnel to be trained.** All research data repository personnel (including trainees, clerks, secretarial support, and oversight committee members), investigators and members of the research teams, research office staff, members of the IRB(s) and R&D Committee(s), and others who deal with issues related to a research data repository must complete the training required by ORD.

b. **Training requirements.** Currently, Cyber Security and Privacy Training are required; other required training courses may include: material on human subjects protection, Good Clinical Practice, Privacy, Ethics, and VA Research Data Security and Privacy. ***NOTE:*** *Although specific training requirements can be found on the ORD web-site, all specific requirements have not been included in this Handbook because the requirements may change.*

19. REFERENCES

a. Title 5 U.S.C. 552.

b. Title 45 CFR Parts 160 and 164.

c. Title 38 CFR Part 1.

d. Title 38 CFR Part 16.

e. Title 38 CFR Part 17.

f. Title 38 U.S.C. 7332.

g. VA Directive and Handbook 6500.

h. VA Directive and Handbook 6102.

i. VA Directive 06-2.

j. VA Directive 6212.

k. VA Directive and Handbook 6502.

l. VA Handbook 6502.1.

m. VA Handbook 6502.2.

n. VA Handbook 5011/5.

o. VA Directive 6601.

p. VHA Handbook 1605.1.

q. VHA Handbook 1605.2 .

r. VHA Handbook 1200.1.

s. VHA Handbook 1200.5.

CRITICAL QUESTIONS FOR THE INSTITUTIONAL REVIEW BOARD (IRB) AND RESEARCH AND DEVELOPMENT (R&D) COMMITTEE TO ASK ABOUT ALL RESEARCH PROJECTS

1. IS THE PROJECT RESEARCH?

The Common Rule (Title 38 Code of Federal Regulations (CFR) Part 16) defines research as a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalized knowledge.

2. IS IT HUMAN SUBJECTS RESEARCH?

A human subject is a living individual about whom an investigator conducting research obtains data through intervention or interaction with the individual or through identifiable private information (38 CFR 16.102(f)). The definition provided in the Common Rule (38 CFR Part 16) includes Department of Veterans Affairs (VA) employees, as well as investigators, technicians, and others assisting investigators, when they serve in a "subject" role by being observed, manipulated, or sampled. As required by 38 CFR 16.102(f) an intervention includes all physical procedures by which data are gathered and all physical, psychological, or environmental manipulations that are performed for research purposes.

3. IF IT IS HUMAN SUBJECTS RESEARCH, IS IT EXEMPT FROM INSTITUTIONAL REVIEW BOARD (IRB) REVIEW?

Criteria to identify research that involves human subjects, but is exempt from the requirements of the Common Rule, and therefore exempt from IRB review, are found in 38 CFR 16.101(b). ***NOTE:*** *The exempt status may only be determined by the IRB Chair or IRB member designated by the Chair. If the VA facility does not have an IRB or Federal-wide Assurance (FWA), the R&D Committee may delegate these determinations to the Chair or other voting member who has sufficient expertise. It may also consult with a VA IRB or a person with the appropriate expertise in this area.*

4. MUST ANY HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) REQUIREMENTS BE MET?

In addition, if the research uses individually identifiable information, either a HIPAA authorization must be obtained or an IRB or Privacy Board may waive the requirement if the applicable criteria are meet.

5. ARE ALL DATA STORAGE AND SECURITY REQUIREMENTS MET?

Data storage and security requirements may be found in VA Handbook 6500.

THE EIGHTEEN HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) IDENTIFIERS

The removal of the following eighteen identifiers from data meets Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements for de-identification of data (Title 45 Code of Federal Regulations (CFR) 164.514).

1. Names;

2. All geographic subdivisions smaller than a state, except for the initial three digits of the zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people;

3. All elements of dates except year and all ages over 89;

4. Telephone numbers;

5. Fax numbers;

6. E-mail addresses;

7. Social Security Number (SSN);

8. Medical record numbers;

9. Health plan beneficiary numbers;

10. Account numbers;

11. Certificate or license numbers

12. Vehicle identifiers and license plate numbers;

13. Device identifiers and serial numbers;

14. Uniform Resource Locator (URLs);

15. Internet Protocol (IP) addresses;

16. Biometric identifiers;

17. Full-face photographs and any comparable images; and

18. Any other unique, identifying characteristic or code, except as permitted for re-identification in the Privacy Rule.

NOTE: *a) HIPAA states that the entity does not have actual knowledge that the [remaining] information could be used alone or in combination with other information to identify an individual who is the subject of the information. b) Codes for re-identifying de-identified*

information may not be derived from, or related to, information about the individual, and may not otherwise be capable of being translated to identify the individual. Scrambled SSNs may not be used as codes and de-identified data may not include scrambled SSNs. c) Scrambled SSNs are considered identifiers.

COMBINED DATA USE DATA TRANSFER AGREEMENT REQUIREMENTS

1. When a combined Data Use Agreement (DUA)-Data Transfer Agreement (DTA) is required. A Combined DUA-DTA is required when data are transferred for research from:

a. One Department of Veterans Affairs (VA) facility to another VA facility

b. One VA investigator or data owner or administrator (e.g., administrator of a Veterans Integrated Service Network (VISN) data warehouse, a national database, or a research data repository) to a VA investigator for a VA-approved research project. ***NOTE:*** *This is applicable when a data extract or the data are actually transferred by the data owner or administrator to the investigator. If the investigator or the investigator's research staff perform the data extract, the data owner or administrator must approve this activity in writing and must define what data may be extracted, how they may be used, who may use them, if they can be disclosed to others, how they must be secured, and if they may be reused for other research.*

c. A VA investigator or Principal Investigator (PI) to a non-VA person or entity who is serving as a contractor or collaborator on the PI's VA-approved protocol

d. Preparatory to research when data are transferred from a data repository for review by the investigator or the investigator's research staff. ***NOTE:*** *Subparagraph 9a of the Handbook contains requirements for when the investigator or the investigator's research staff directly access a database.*

NOTE: *Although VHA Handbook 1605.1 does not require the use of a DUA for transferring of data for research purposes within VHA, this Handbook has added the requirement for a DUA-DTA when data are transferred for research purposes.*

2. When a combined DUA-DTA is not required. A Combined DUA-DTA is not required when:

a. Data are transferred (disclosed) to a research sponsor in accordance with the VA-approved protocol and signed research informed consent documents and Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorizations.

b. Data are transferred from one VA facility or VA investigator to another VA facility or VA investigator when this transfer is required to conduct a VA-approved protocol, the transfer is described within the protocol, and the protocol is approved by each site's IRB and the protocol is then active at each site. For example: When data from a multi-site VA-approved clinical trial must be transferred to a VA coordinating center or to another VA site involved in the protocol.

c. Data are disclosed to a non-VA individual or entity for research purposes and:

(1) A signed research informed consent and signed HIPAA authorization has been obtained from each research subject, or

(2) A written request for the data has been sent to the Privacy Office and the Privacy Officer has determined that:

(a) The release of the data meets all requirements of the Privacy Act, HIPAA, and other applicable regulations,

(b) The Privacy Officer has approved the release, and

(c) All other applicable approvals have been obtained.

NOTE: *The actual release of the data must be coordinated with the facility's Privacy Officer. All requirements in VHA Handbook 1605.1 must be met.*

3. Developing a combined DUA-DTA. When a Combined DUA-DTA is required it must be developed in accordance with this appendix, and it must be signed by an official of the releasing facility and an official of the receiving facility or entity prior to data being transferred. The officials signing the Combined DUA-DTA may vary depending on the specific information that is being transferred, how it will be used, and on the location to which the data are being transferred. ***NOTE:*** *One of the signing officials at the releasing facility and one of the signing officials at the receiving facility must have the authority to enforce the requirements in the DUA-DTA such as the Associate Chief of Staff (ACOS) for Research and Development (R&D), the Chief Information Officer, or the medical center Director*.

4. Identifying the signing officials for combined DUA-DTAs

a. Data being transferred within a VA facility. The data or database owner or designee and the receiving investigator are the signatory officials for the Combined DUA-DTA. The ACOS for R&D of the recipient must also sign the Combined DUA-DTA.

b. Data being transferred to another VA facility. The data or database owner or designee must be the signatory official for the releasing facility. The ACOS for R&D of the releasing facility must also sign the Combined DUA-DTA if the data being released are from a research data repository. In addition, the releasing facility and other VA policies may require the signature of other officials such as the Chief Information Officer, the Privacy Officer, the ISO, or the database owner's or the administrator's supervisor.

5. Elements that must be incorporated into all combined DUA-DTAs. These include:

a. A description of all specific uses of the data including the name of the research protocol in which they will be used. If the use is preparatory to research, a description of the intended preparatory activity and the potential research project must be included.

b. Names of all persons who will have access to or use the data.

c. Name and description of any entities to which the data will be disclosed as required by the protocol.

d. Disposition of the data after the research is completed. Include both the initial data received, any new data that were generated based on the data that were originally transferred, and any data repositories created from the original data.

6. <u>Stipulations that must be included in all combined DUA-DTAs.</u> These include that:

a. The data will not be disclosed within the VA or outside the VA other than as permitted by this agreement and permitted within the protocol for which the data have been requested.

b. Data must be used, stored, and secured according to the requirements of the VHA series 1200 Handbooks, other applicable VA and VHA requirements, and as described in the approved research protocol.

c. Any non-compliance with the applicable VA and VHA requirements, other applicable Federal regulations, or the research protocol as approved by the IRB and R&D Committee(s), must be reported according to the facility's policies and procedures and by VHA requirements. It must also be reported to the investigator or VA employee who allowed the data to be transferred. If data are from a VA data repository, the data repository administrator or owner must notify the IRB(s) having oversight responsibilities for the repository in accordance with the repositories procedures.

d. Any theft, loss, or compromise of the data must be immediately reported to the investigator's facility's ISO, Privacy Officer, the investigator's supervisor, and others as stipulated in VA, VHA, and local facility's requirements. It must be reported to the Privacy Officer and ISO of the facility from which the data were transferred, in addition to the investigator or VA employee who allowed the transfer of the data. If data are from a VA research data repository, the research data repository administrator must notify the IRB having oversight responsibilities for the repository in accordance with the research data repositories procedures

e. No effort will be made to re-identify data that are de-identified.

f. Scrambled social security numbers (SSNs) will not be "unscrambled" to reveal the real SSNs.

NOTE: *A combined DUA-DTA is not required if data is to be transferred from one VA facility to another VA facility in accordance with the VA-approved protocol. The same protocol must be approved by each facility's IRB for each facility engaged in that research. Examples include: a. Data from a VA Cooperative Studies Program (CSP) protocol are transferred from one of the VA sites to a CSP coordinating center, or b. If a VA-approved research protocol is open at more than one site, the data may be transferred to one of the other sites that is conducting the same research <u>if this data transfer is described in the protocol</u>.*