USE OF DATA AND DATA REPOSITORIES

1. POLICY

The Birmingham Veterans Affairs Medical Center (BVAMC) Human Research Protection Program (HRPP) is committed to protecting the safety and welfare of veterans participating in VA research. This policy ensures the BVAMC has authorized adequate provisions to protect research repositories and adheres to all applicable policies and regulations. This policy applies to all BVAMC human subject research repositories established for the purpose of storing data and/or human biological specimens for future research purposes. This policy does not apply to data and/or human biological specimens collected and stored solely as part of routine clinical care or hospital procedures, such as blood banks, pathology, surveillance, or quality assurance.

2. BACKGROUND

VA must exercise prudent stewardship of public resources, including public funds that support research programs. This Standard Operating Procedure (SOP) establishes procedures to ensure data and/or human biological specimens to be used for research are responsibly obtained, stored and distributed, and to protect the rights of individuals who have donated bio-specimens and/or data to support VA research.

3. SOURCES OF DATA IN DATA REPOSITORIES

A. Data used for research purposes within VA may come from 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:

- Veterans Integrated Service Network (VISN) data warehouses
- National Databases Systems (vwww.va.gov/nds). NOTE: This is an internal VA link not available to the public.
- VA registries, data centers.
• Veterans Health Information Systems and Technology Architecture (VistA)
  computerized Patient Record System (CPRS).
• Pharmacy Benefits Management.
• The Emerging Pathogens Initiative.
• Center for Medicare and Medicaid Services (CMS) data.

4. DETERMINING IF DATA ARE IDENTIFIABLE OR DE-IDENTIFIED

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

A. Identifiable Data: For the purposes of this SOP, the definition of identifiable data is based on both the Common Rule (38 CFR Part 16) and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

1) If either condition in the following subparagraphs 4.A.1) or 4.A.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 within 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 Appendix A.
   2. The covered entity has actual knowledge 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) or
   3. The data have not met the criteria for de-identification by statistical means as outlined in 45 CFR 164.514(b)(1)

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 are approved by the Institutional Review Board (IRB) and the Research and Development Committee (R&DC). To obtain access to real SSNs, the procedures defined by the VHA Privacy Office must be followed.
b) When a research protocol calls for the 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 amendments must be reviewed by the local Privacy Officer (PO) to ensure Privacy regulations have been met.

B. **De-identified Data:** De-identified 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 A, or
   b) Meets the criteria for de-identification by statistical means as outlined 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 the IRB and R&DC

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 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&DC of record for the facility where the research data repository resides. Only after these approvals have been obtained may the repository contain identifiable data.

5. PRIVACY AND CONFIDENTIALITY

A. 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. Review HRPP SOP #10, Research Data Security, Confidentiality and Privacy.

B. Contact the facility PO, Information Security Officer (ISO), and/or the Research Compliance Officer (RCO) for guidance on policies relating to privacy and confidentiality.

6. 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 per VA Handbook 6500 Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program.

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.

C. The data repository must have a security plan for all data maintained that is consistent with VA requirements. Consult the ISO for any questions or assistance 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.

7. 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, Individual Identifiable Information (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 the IRB. This access is granted only to VHA researchers.

1) The investigator must document the following in the research files:

   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 protocol

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 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 requirements set by the repository of interest.

6) A Data Use Agreement (DUA) is required if the data are transferred from a data repository to the investigator for the purpose of preparatory for review by the investigator or the investigator’s research staff. See Appendix B.

B. Use of Data for Research Purposes

1) VA investigators may obtain only the minimum amount of data necessary to conduct the research.

2) 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.

3) 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 subject’s research, IRB approval must be obtained from the IRB(s) of record for the PI’s facility and each co-investigator’s facility. IRB approval 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 not limited to: union approval (to perform research on employee data); PO and ISO approval; and approvals from the administrator or oversight committee of a specific data repository.

8. 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 to be used to prove or disprove a specific hypothesis, or it may be a protocol specifically designed to collect data to be used for future use.

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 criteria are met to waive the requirement for a research informed consent and HIPAA authorization and documents all criteria are met.

2) De-identified Data
   a) De-identified data may be collected without informed consent or HIPAA authorization after the protocol has received the appropriate approval. NOTE: The
facility Privacy Officer must verify the data are de-identified.
b) A protocol involving de-identified data needs to be presented to the IRB who makes the determination if the criteria for Exempt status are met.

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

1) Data may be collected from research subjects directly through such means as medical tests, interventions, questionnaires, or surveys.

2) Data may be collected from indirect sources such as other research projects or research data repositories if appropriate approval has been obtained for such re-use of the data.

3) Research data are not considered to constitute a “research data repository” and are not subject to the requirements of VHA Handbook 1200.12 *Use of Data and Data Repositories in VHA Research*, 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 require 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.*

9. **CREATING A RESEARCH DATA REPOSITORY**

Principal Investigators are the “owners” or “administrators” of the research data repository and are responsible for developing an SOP for each research data repository they create and must utilize the guidance set forth in 11.C in developing the SOP.

A. The **Research & Development Committee (R&DC)** will:

1) Comply with all requirements in VHA Handbook 1200.01.

2) Review and provide final approval for the establishment and operations of all BVAMC research repositories to include the administrative structure and standard operating procedures.

3) Approve research protocols for local investigators that propose to use data from any research or non-research repository housed at the BVAMC before data can be accessed.

B. The **Institutional Review Board (IRB)** of record will:

1) Comply with all requirements in VHA Handbook 1200.05 and all conflict of interest policies.

2) Review and approve the establishment and operations of all BVAMC research repositories to include the administrative structure and standard operating procedures.

3) Approve research protocols for local investigators that propose to use data from any
research or non-research repository housed at the VA/BVAMC before data can be accessed.

C. The **Repository Administrator** will:

1) Adhere to all applicable policies and procedures associated with conducting research involving the use of research repositories. Adherence to VHA Handbooks 1200.05 and 1605.1, and BVAMC HRPP SOPs are also required if the protocol involves human subjects.

2) Develop standard operating procedures to include the repository’s administrative structure and mechanisms for verifying committee approvals and releasing data from the repository. The administrative structure must always include a VA investigator who is responsible for all the activities of the data repository. Completing the DATA REPOSITORY REQUEST FORM will constitute the administrative SOP. **NOTE: An investigator under a WOC or IPA may not serve as the sole administrator of a VA data repository.**

3) Ensure the repository’s standard operating procedures at minimum addresses each of the following:

   a) Administrative activities (e.g., Administrative structure, approval verification...);
   b) Conflict of Interest (COI);
   c) Tracking of data (e.g., data source, data type...);
   d) Reuse of data;
   e) Disclosure to subjects and conditions under which disclosure is or is not allowed;
   f) Data disposition plan due to repository termination;
   g) Access agreements (i.e., combined DUA-DTA);
   h) Original protocol, amendments, IRB and R&DC approvals;
   i) Security and oversight plan

4) Relinquish access to all research records, data, and data in repositories if the investigator no longer holds an appointment as a VA employee or IPA. All data and records are the property of the VA. The data may not be copied or removed unless all requirements for use of VA data by a non-VA investigator are met.

5) Will review the request for access and verify the required approvals are granted prior to approving and providing access to the repository data. The approval verification can be accomplished by reviewing the project/protocol file(s) in the Research Administrative Office. The PO will be consulted if a request is received from a non-VA investigator.

6) Maintain records to include requests for access and disclosure logs.

7) Provide an annual status report of the research data repository to the IRB and R&DC at continuing review. The 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 privacy and security incidents.
   d) Findings linking a negative impact on the health 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 according to VHA Handbook 1200.05.

D. The Privacy & Information Security Officers will:

1) Serve as resources and subject matter experts in areas of privacy & confidentiality and information security in research. The PO and ISO will provide consultation and assistance to the BVAMC research oversight committees and research community.

2) Will review data repository security plans to include repository location, access controls, and standard operating procedures.

3) Will review request for access from non-VA investigators and in other instances when a combined DUA-DTA may be required.

E. The Investigators will:

1) Adhere to all applicable policies and procedures in designing and conducting research involving the use of data repositories.

2) Obtain all of the required approvals in writing before initiating research involving data repositories.

3) Maintain the privacy and confidentiality of all PHI and sensitive data in accordance with all applicable VA and VHA policies and procedures.

4) Notify the Research Administrative Office and relevant research oversight committees of any intention to leave VA employment, so administrative structure of any repositories may be properly transferred. Other situations may include investigators that no longer hold an appointment as an employee or IPA. Any investigator that is no longer an employee must relinquish all access to research records, data, and data in repositories. All data and records are the property of the VA and must remain at the VA under VA control. This data may not be copied or removed unless all requirements for the use of VA data by a non-VA investigator are met.

5) Submit a request as part of the Initial Review Application to the IRB to create the repository data (complete the attached Appendix C: DATA REPOSITORY REQUEST FORM).

10. RELEASING BVAMC RESEARCH REPOSITORY DATA TO A BVAMC INVESTIGATOR

A BVAMC Investigator may request data from an established BVAMC IRB approved research data repository.

A. The standard IRB Initial Review Application must be utilized.

B. The Repository Administrator may have additional requirements for requesting access to the Data Repository.
11. **RELEASING IDENTIFIABLE OR DE-IDENTIFIED INFORMATION TO ANOTHER VA SITE FOR RESEARCH PURPOSES**

VA facilities releasing 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. 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. See Appendix B

B) The release of the information may occur only after the BVAMC’s PO and ISO have reviewed the request to ensure all privacy and security procedures governing transfer of the data have been met.

C) The request to a BVAMC’s research data repository for release of data must include the following for all sites engaged in the protocol:

1) Documentation of the receiving site’s IRB approval of the protocol if the project is considered human subjects research. If the request is for identifiable data to be placed in a research repository, documentation must be received indicating IRB approval for such repository.

2) Documentation of the IRB’s waiver of informed consent and waiver of HIPAA authorization as applicable.

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

4) If the request is for information which will be placed in a research repository, the request for data must include a copy of the repository protocol including 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.*

12. **DEFINITIONS**

See HRPP SOP #24 – HRPP Definitions
13. REFERENCES

VHA Handbook 1200.12 Use of Data and Data Repositories in VHA Research
VHA Handbook 1200.01 Research and Development (R&D) Committee
VHA Handbook 1200.05 Requirements for the Protection of Human Subjects in Research
VHA Handbook 1605.1 Privacy and Release of Information
VA Handbook 6500 Risk Management Framework for VA Information Systems - Tier 3:
   VA Information Security Program
Common Rule (38 CFR Part 16)
Health Insurance Portability and Accountability Act (HIPAA)

14. ATTACHMENTS

None

15. RESECISSIONS

January 24, 2014, Reviewed October 2018

16. REVIEW DATE

November 1, 2021

[Signature]

Louis Dell'Italia, MD
ACOS, Research and Development
THE EIGHTEEN HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY
ACT OF 1996 (HIPAA) IDENTIFIERS

1. Name;

2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
   (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

4. Phone numbers;

5. Fax numbers

6. Electronic mail addresses;

7. Social Security numbers;

8. Medical record numbers;

9. Health plan beneficiary numbers;

10. Account numbers

11. Certificate/license numbers;

12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers

16. Biometric identifiers, including finger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).
COMBINED DATA USE-DATA TRANSFER AGREEMENT REQUIREMENTS

1. When a combine 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 when the receiving facility is not engaged in the VA-approved protocol.

   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 equally 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.

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 document and 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 facility Privacy Officer who 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.

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 may have the authority to enforce the requirements in the DUA-
DTA such as the Associate Chief of Staff for Research and Development (ACOS/R&D), the Chief
Information Office (CIO), 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/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/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 CIO, PO, 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 descriptions 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 generated based on the data originally transferred, and any data
repositories created from the original data.

6. Stipulations that must be included in all combined DUA-DTAs. 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 must be reported according to the facility's policies and procedures. 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.

D. Any theft, loss, or compromise of the data must be immediately reported to the investigator's facility's ISO, PO, the investigator's supervisor and other as stipulated by HRPP SOP #10. If data are from a BVAMC research data repository, the research data repository administrator must notify the IRB.

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 combine 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 conducting the same research if this data transfer is described in the protocol.
REQUEST FORM
To CREATE a BVAMC Research Data Repository

Date:
Principal Investigator:
Data Repository/Protocol Title:

There are two types of data repositories: Non-research and Research

**Research Data Repository – Definition**
The term "research data repository" means a data repository created from data obtained either to

<table>
<thead>
<tr>
<th>NON-RESEARCH</th>
<th>RESEARCH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CREATION:</strong></td>
<td><strong>CREATION:</strong></td>
</tr>
<tr>
<td>&quot;Created&quot; for non-research activities</td>
<td>&quot;Created&quot; solely for research</td>
</tr>
<tr>
<td>Examples: Clinical databases, CPRS, QA databases, Cancer Registries, etc.</td>
<td>To be used for future research</td>
</tr>
<tr>
<td>IRB approval not required.</td>
<td>IRB approval required to &quot;CREATE&quot;</td>
</tr>
<tr>
<td>Complete a Research Data Repository SOP submission form AND a standard Initial Review Submission Form</td>
<td></td>
</tr>
</tbody>
</table>

**USE:**

<table>
<thead>
<tr>
<th>NON-RESEARCH</th>
<th>RESEARCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRB approval required for each &quot;USE&quot; of data obtained from a non-research database.</td>
<td>IRB approval required for each use of data obtained from a Research Data Repository.</td>
</tr>
<tr>
<td>Complete a standard IRB submission form.</td>
<td>Complete a standard IRB submission form.</td>
</tr>
</tbody>
</table>

conduct a research protocol(s) or gathered in a 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.

**Creating a Research Data Repository**
Principal Investigators are the “owners” or “administrators” of the research data repository and are responsible for developing an SOP for each research data repository that they create. The Principal Investigator provides answers to the questions below and this is the administrative SOP for a research data repository. The IRB and the R&D Committee must approve the creation of and administrative SOP for each research data repository, as well as comply with VHA Handbook 1200.05 (IRB) and VHA Handbook 1200.01 (R&D Committee).
IRB and R&D Approval is Required
The IRB and R&D Committees are required to review and approve the creation and operation of all research repositories if one or more of the investigators are from the BVAMC (i.e., the VA facility that houses the research data repository) and the data are housed at the BVAMC. Continuing Review of each research data repository must occur at an interval determined by the IRB or the R&D Committee, but at least annually.

Accessing Data in a Research Data Repository
All VA investigators 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.

Combined Data Use – Data Transfer Agreement - Definition
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.

Combined Data Use-Data Transfer Agreement- Use of

(1) A Combined Data Use-Data Transfer Agreement is not required if data are 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. (e.g., when data from a VA Cooperative Studies Program (CSP) protocol are transferred from one of the VA sites to a CSP coordinating center). All transfers of data for other purposes require a combined Data Use-Data Transfer Agreement and must follow requirements in VHA Handbook 1200.12 entitled, “Use of Data and Data Repositories in VHA Research.” Privacy Officer and Information Security Officer approval are required. A DUA/DTA IS NOT NEEDED if there are signed HIPAA authorizations and informed consent documents, applicable to the protocol, that clearly address the transfer of data to a non-VA facility or to a VA facility that is not engaged in conducting the protocol under which the consent and authorization were obtained.

(2) A DUA/DTA IS NOT NEEDED if two or more VA facilities are engaged in conducting the protocol, and the protocol has been approved by each facility’s IRB of record, and the transfer of the data is required to conduct the research.

(3) A DUA/DTA IS NEEDED if the recipient facility is engaged in the conduct of the protocol, but the sending facility is not engaged in the conduct of the protocol. Of course, prior approval of the protocol by the recipient facility’s IRB of record is required.

INITIAL REVIEW

Additional Initial Review Requirements for a Research Data Repository
Please complete and append to the Initial Review Submission Form

Is this data repository being “created” solely for research purposes and will be used for future research? □ YES □ NO
If NO, it is not a research data repository and completion of this form is not required. If you want to use a non-research data repository (e.g., clinical, CPRS, QA, Medicare, etc.) for research purposes, complete the standard IRB Initial Review Submission Form.

If YES, complete this application.

An Administrative SOP is required for the creation of a Research Data Repository. Addressing the following will create the required SOP.

1. Administrative and regulatory activities (e.g., Administrative structure, approval verification, etc.) to include maintenance of original documents, amendments, IRB, R&DC and ACOS/R approvals. An annual report must include, but not 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 privacy and security incidents.
   d. Findings linking a negative impact on the health 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 according to VHA Handbook 1200.05.

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

3. Conflict of Interest – state Conflict of Interest will be addressed with the Research Service Conflict of Interest Committee prior to releasing data from the research data repository.

4. Describe plans to store data in this repository for future research. If the data are stored for future research, there must be a description of research data repository, its location, and its security measures.

5. Ensure documentation is in place of the local ISO’s and VA Police Service’s determination the security for the data repository and the location where the data repository is to be located meets applicable VA security requirements. This must be completed prior to data being placed in the space.
   **NOTE:** All VA research data repositories must be physically located within space owned or leased by VA.

6. Confirm you understand you may only store data for future research in an IRB/R&D approved data repository.

7. Describe plans to share with others including other researchers (VA and non-VA), if any and include procedures you will use to document/track who you share data with. If the data were collected through a research project, discuss whether or not the original informed consent allowed for such reuse of the data and if the reuse/sharing is consistent with the HIPAA authorization that was obtained. If you plan to share research repository data with other sites or investigators a Combined
Data Use-Data Transfer Agreement may be required. Privacy and Information Security approval is required.

8. Provide conditions under which disclosure to subjects is or is not allowed.

9. Confirm that no research involving data repositories will be initiated without first obtaining IRB and R&D Approval of individual research projects. Note: The repository's administrator (i.e. the investigator who created the database) must then approve or disapprove.

10. Confirm that you will be responsible for maintaining the privacy and confidentiality of subject’s protected health information (PHI) and sensitive data in accordance with applicable VA and VHA information confidentiality and security requirements.

11. Confirm that if you leave VA, all research records, data, and data in repositories must remain at VA and under VA control and that the data may not be copied or removed unless all requirements for use of VA data by non-VA investigators are met. All data and records are the property of the VA.

12. Confirm that you will consult the Privacy Officer if you receive a request for information from a non-VA investigator. Special additional requirements apply.

13. Confirm records will be maintained to include requests for access and disclosure logs.

14. If the data you plan to use were collected for administrative or clinical reasons, discuss whether the guidelines under which they were collected allow for storage in a specific data repository and reuse for research purposes. For example, there may be administrative policies that may not allow the administrative and or clinical data to be placed in a research data repository for reuse.

15. Confirm that you will terminate a research data repository only under the direction of the IRB or R&D Committee responsible for the oversight of the repository. NOTE: Current VA Requirements do not allow destruction of research data.

Investigator Signature

Date
DATA USE AGREEMENT

AGREEMENT FOR EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), BIRMINGHAM VETERANS AFFAIRS MEDICAL CENTER (BVAMC) AND <INSERT OUTSIDE AGENCY NAME>

Purpose:
This Agreement establishes the terms and conditions under which the <insert name> will provide, and <insert name> will use the data to <be very specific in why data is being shared, and state the method of transfer and how that will be accomplished>

Any other uses will be subject to prior approval by the <transferring agency Director>.

TERMS OF THE AGREEMENT:

1. This Agreement is by and between the <INSERT NAME> and BVAMC (Owner), a component of the U.S. Department of Veterans Affairs.

2. This data transfer agreement covers the transfer and use of data by the <INSERT NAME> and BVAMC, for the project specified in this agreement. This Agreement supersedes any and all previous data.

3. The terms of this Agreement can be changed only by a written modification of the agreement by the agency signatories (or their designated representatives) to this Agreement or by the parties adopting a new agreement in place of this Agreement.

4. The BVAMC retains all ownership rights to the data file(s) and VHA retains all ownership rights to the VHA data file(s) provided to you under this Agreement.

5. The <Insert user name> will be designed as custodians of the VA data for the <user name> and will be responsible for complying with all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use and disclosure of the Owner’s data provided under this agreement. The User agrees to notify the Owner within fifteen (15) days of any change of custodianship.

Technical Representative for BVAMC

Insert Name and Phone Number

Custodian for <User Agency>

Insert Name and Phone Number
 ADMINISTRATION (VHA), BIRMINGHAM VETERANS AFFAIRS MEDICAL CENTER (BVAMC) AND <INSERT OUTSIDE AGENCY NAME>

6. The following named individuals are designated as their agencies’ Points of Contact for performance of the terms of the Agreement.

**Point-of-contact on behalf of BVAMC**

Insert Name and Phone Number

**Point-of-contact on behalf of <User Agency>**

Insert Name and Phone Number

7. Except as VHA shall authorize in writing, the User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the VHA data covered by this Agreement to any person outside the <User Agency>. The User agrees that, access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to Owner’s data to perform this Agreement.

8. The parties mutually agree that any derivative data or file(s) that is created from the original data may be retained by the User until the project specified in this DTA has been completed. The use of the data will be for the time period covered by the <Insert MOU or Proposal Name> (Insert Time Frame). At the end of this period <insert terms of agreement for return or data, destruction of data or renewing agreement> you are authorized to keep the data on your system in a secure encrypted partition in accordance with FIPS 140-2 validation.

9. The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the Owner will notify the User to destroy or return such data at Users expense using the same procedures stated in the above paragraph of this section.

10. The User will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the Owner’s data and to prevent unauthorized use or access to it. VA sensitive information must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be validated by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140 (See http://csrc.nist.gov/cryptval/140-1/1401val.htm for a complete list of validated cryptographic modules). Only approved encryption solutions using validated modules may be used when protecting data during transmission. Additional security

**DATA USE AGREEMENT**

AGREEMENT FOR EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), BIRMINGHAM VETERANS AFFAIRS MEDICAL CENTER (BVAMC) AND <INSERT OUTSIDE AGENCY NAME>
controls are required to guard VA sensitive information stored on computers used outside VA facilities. All VA data must be stored in an encrypted partition on the hard drive and must be encrypted with FIPS 140 validated software. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. Further, the User agrees that the data must not be physically moved or transmitted in any way from the site indicated in item number 5 without first being encrypted and obtaining prior written approval from the data owner.

a. If the data user becomes aware of the theft, loss or compromise of any device used to transport, access or store VA information, or of the theft, loss or compromise of any VA data, the user must immediately report the incident to his or her supervisor. That supervisor must within one hour inform the <Fill in VA Information Security Officer and/or VA Privacy Officer and the Director names and phone numbers>. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements for responding to security incidents.

11. The authorized representatives of VHA and the Inspector General will be granted access to premises where the data are kept by the User for the purpose of confirming that the User is in compliance with the security requirements.

12. No findings, listing, or information derived from the data, with or without identifiers, may be released if such findings, listing, or information contain any combination of data elements that might allow the deduction of a veteran without first obtaining written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement.
Examples of such data elements include but are not limited to social security number, geographic indicator, age, sex, diagnosis, procedure, admission/discharge date(s), or date of death. The Owner shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from its files provided under this Agreement identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual. The Owners’ review of the findings is for the sole purpose of assuring that data confidentiality is maintained and that individuals cannot be identified from the findings. The Owner agrees to make this determination about approval and to notify the User within two weeks after receipt of findings. The Owner may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual.

DATA USE AGREEMENT

AGREEMENT FOR EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), BIRMINGHAM VETERANS AFFAIRS MEDICAL CENTER (BVAMC) AND <INSERT OUTSIDE AGENCY NAME>

13. The User may not reuse the Owner’s original or work file(s) for any other purpose.
14. In the event that the Owner determines or has a reasonable cause to believe that the User disclosed or may have used or disclosed any part of the data other than as authorized by this Agreement or other written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement, the Owner in its sole discretion may require the User to: (a) promptly investigate and report to the Owner the User’s determinations regarding any alleged or actual unauthorized use or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by the Owner, submit a formal response to an allegation of unauthorized disclosure; and (d) if requested, return the Owner’s data files to the Owner. If the Owner reasonably determines or believes that unauthorized disclosures of Owner’s data in the possession of User have taken place, the Owner may refuse to release further data to the User for a period of time to be determined by the Owner, or may terminate this Agreement.

15. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. §1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by §1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. §552a(i)(1)) may apply if it is determined that the User, or any individual employed or affiliated therewith, knowingly and willfully discloses Owner’s data. Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. §641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted.

16. All questions of interpretation or compliance with the terms of this Agreement should be referred to the VHA official name in item 18 (or his or her successor).

17. Authority for VHA to share this data for the purpose indicated is under the HIPAA Privacy Rule, is 45 CFR 164.512(k)(6)(ii), under the Privacy Act is routine use 30 in VA system of records, 121VA19, entitled National Patient Databases-VA and under 38 USC 5701(b)(3) and (e).

DATA USE AGREEMENT

AGREEMENT FOR EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), BIRMINGHAM VETERANS AFFAIRS MEDICAL CENTER (BVAMC) AND <INSERT OUTSIDE AGENCY NAME>

18. On behalf of both parties the undersigned individuals hereby attest that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.
<table>
<thead>
<tr>
<th>Transferring Responsible Official</th>
<th>Date</th>
<th>User Responsible Official</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thomas C. Smith, III, FACHE</td>
<td></td>
<td>&lt;Printed Name&gt;,</td>
<td></td>
</tr>
<tr>
<td>Medical Center Director</td>
<td></td>
<td>&lt;Title&gt;</td>
<td></td>
</tr>
<tr>
<td>Organization Transferring Data</td>
<td></td>
<td>Organization Receiving Data</td>
<td></td>
</tr>
</tbody>
</table>

Concur/Non-Concur:

<table>
<thead>
<tr>
<th>Transferring Agency</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ISO Name&gt;</td>
<td></td>
</tr>
<tr>
<td>Information Security Officer</td>
<td></td>
</tr>
<tr>
<td>Organization Transferring Data</td>
<td></td>
</tr>
</tbody>
</table>

Concur/Non-Concur:

<table>
<thead>
<tr>
<th>Transferring Agency</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PO Name&gt;</td>
<td></td>
</tr>
<tr>
<td>Privacy Officer</td>
<td></td>
</tr>
<tr>
<td>Organization Transferring Data</td>
<td></td>
</tr>
</tbody>
</table>