DATA USE AGREEMENTS

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) Handbook establishes guidance and uniform procedures for the creation and use of Data Use Agreements (DUA).

2. SUMMARY OF CHANGES: This is a new Handbook.

3. RELATED ISSUES: VHA Directive 1080, Access to Individually Identifiable Information in Information Technology Systems.

4. RESPONSIBLE OFFICE: The VHA Office of Informatics & Analytics (10P2) is responsible for the contents of this Handbook. Questions may be referred to the VHA Office of Informatics & Analytics (OIA), Health Information Governance (HIG), National Data Systems (NDS) Office at (202) 461-1581 or sent to the following email address: hia@va.gov.

5. RESCISSIONS: None.

6. RECERTIFICATION: This VHA Handbook is scheduled for recertification on or before the last working day of November 2018.

Robert A. Petzel, M.D.
Under Secretary for Health

DISTRIBUTION: E-mailed to the VHA Publications Distribution List on 11/22/13.

TABLE OF CONTENTS
DATA USE AGREEMENTS

PARAGRAPH: **PAGE:**

1. Purpose 1

2. Background 1

3. Definitions 2

4. Scope 5

5. Responsibilities 6

6. Determining when a DUA is Required or Prohibited 7

7. Special Circumstances and Exceptions 10

8. Establishing DUAs 10

9. Processing and Monitoring DUAs 10

10. References 11

APPENDICES:

A. DUA Decision Tree A-1

B. Case Use Examples B-1

C. DUA Templates C-1

D. DUA Process Flow D-1

E. Data Use Agreement with Federal Entities E-1

F. Data Use Agreement with Non-Federal Entities F-1

G. Data Use Agreement with Limited Data Sets with Federal Entities G-1

H. Data Elements to be Provided to Federal Entity H-1

I. Data Use Agreement with Limited Data Sets with Non-Federal Entities I-1

J. Data Elements to be Provided to Non-Federal Entity J-1

DATA USE AGREEMENTS

1. PURPOSE: This Veterans Health Administration (VHA) Handbook establishes guidance for determining when a Data Use Agreement (DUA) is required by Federal laws, regulations, or U.S. Department of Veterans Affairs (VA) and VHA policies, for formulating a DUA based upon an established template, and for processing and monitoring DUAs. This Handbook also establishes new policy which precludes the use of DUAs, per VHA policy, in certain circumstances. **AUTHORITY:** 38 U.S.C. 7301(b).

2. BACKGROUND:

a. VHA, as a component of a government agency and as a health plan with health care provider functions, must comply with all applicable Federal privacy laws and regulations. As a covered entity under the Health Insurance Portability and Accountability Act (HIPAA) and in accordance with VHA privacy policy, VHA is required to enter into a DUA under certain data-sharing circumstances such as when a limited data set (LDS) is used or disclosed and as described in this Handbook.

b. Previously, in those cases where the use of a DUA was not mandated by Federal law or regulation, the decision to use a DUA was made by the Data Owner. This led to inconsistent practices when determining the need for a DUA and the level of detail required in the DUA. The Under Secretary for Health formed the Managing Data Workgroup in December 2010 to recommend solutions to VHA's most pressing data management challenges. The Workgroup made several recommendations and one of those recommendations focused on making data more accessible to those whose VA job duties required such access. The term Data Transfer Agreement (DTA) had been adopted within VHA in an attempt to distinguish between legally required agreements and agreements made as a best practice to protect the organization and the data, but not otherwise required by law. While different terms were used to describe different purposes, the same templates were being used for both DUAs and DTAs. This has led to confusion throughout VHA.

c. VHA Directive 1080, Access to Individually Identifiable Information in Information Technology Systems charges VHA Office of Informatics and Analytics (OIA), Health Information Governance (HIG), National Data Systems (NDS), and its Health Information Access (HIA) program, with the responsibility for developing policy and processes for accessing VHA individually identifiable information (III) including protected health information (PHI). This Handbook fulfills that responsibility by establishing policy and procedures related to DUAs.

NOTE: *"DUA" as used in this Handbook is not solely limited to the agreement as defined and required by the HIPAA Privacy Rule to disclose a limited data set of protected health information, but instead is meant to more broadly encompass data sharing agreements of other types of data and in other circumstances.*

3. DEFINITIONS:

a. **Access.** Access is the viewing, inspecting or obtaining a copy, of III or PHI electronically, on paper or other medium.

b. **Authorized User.** An Authorized user is:

(1) An individual permitted by:

(a) Federal law and regulation to have access to or obtain a copy of VHA III or PHI;

(b) VA to have access to one or more VA IT systems; and

(c) VHA, in accordance with all applicable VHA policies and with a need to know to have access to VHA III/PHI.

(2) Authorized users may request access to VHA III or PHI at the local level from a VA medical facility or Veterans Integrated Service Network (VISN) or at a national level from a VHA Data Owner (e.g., Decision Support System).

(3) Authorized users may include, but are not limited to, VA employees, VA contractors (including External Peer Review Program), VA Business Associates (including The Joint Commission), volunteers, trainees, students, and accredited Veteran Service Officer (VSO) representatives, and Department of Defense (DoD) health care staff.

c. **Business Associate.** A business associate is an entity, including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of PHI, or that provides to or for VHA certain services as specified in the Privacy Rule that involve the disclosure of PHI by VHA. The term "Business Associate" also includes a Subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

d. **Business Associate Agreement.** A Business Associate Agreement (BAA) is an agreement between VHA and a Business Associate documenting a Business Associate's responsibility to safeguard PHI used by or disclosed to the business associate by VHA according to the HIPAA Security, Privacy and Data Breach Notification Rules.

e. **Data Owner.** For the purposes of this Handbook, a Data Owner is an agency official with statutory or operational authority over specified information, and responsibility for establishing the criteria for its creation, collection, maintenance, processing, dissemination, or disposal. A Data Owner, or designee, is also an agency official who has been identified as having the responsibility and the accountability for the use or disclosure of the VHA data contained in a VA Information Technology (IT) system. These responsibilities may extend to interconnected systems or groups of interconnected systems. As determined by the Office of General Counsel (OGC), the official owner of data within VHA is the Under Secretary for Health. It is VHA practice to delegate responsibility and accountability for business functions and the data related

to those functions to designated VHA Program Offices. Identification of a data owner should generally begin with the program office which sponsored the creation of the data.

f. **Data Use Agreement.** A Data Use Agreement (DUA) is an agreement that:

(1) Governs the sharing of data between a Data Owner and Requestor;

(2) Defines ownership as related to the data exchange;

(3) Establishes the specific terms of use and disclosure for the Requestor;

(4) Provides a means to transfer liability for the protection of the data to the Requestor;

(5) Is considered "internal' if the Requestor is within VA, and "external" if Requestor is outside VA;

(6) Serves as a means to establish criteria for using, disclosing, storing, processing, and disposing of data; and

(7) Satisfies HIPAA requirements when providing information within an LDS.

g. **De-identified Information.** De-identified information is health information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual because the 18 Patient Identifiers described in the HIPAA Privacy Rule have been removed. De-identified information is no longer covered by the Privacy Act, 38 U.S.C. §§ 5701, 7332, or the HIPAA Privacy Rule. SOURCE: 45 CFR § 164.514 (b)(2)(i).

h. **Designated Signatory Official.** For the purposes of this Handbook, the Designated Signatory Official is the individual authorized to enter into and sign a DUA on behalf of the Requestor.

i. **Derivative Data.** For the purposes of this Handbook, Derivative Data are data which have been derived from other data by mathematical techniques, or data which are used or taken from other sources (not original).

j. **Disclosure**. Disclosure is the release, transfer, provision of access to, or divulging in any other manner III or PHI from VHA to either another VA component or another entity outside of VA. In some cases once information is disclosed, VHA relinquishes ownership of the information.

k. **Freedom of Information Act.** The Freedom of Information Act (FOIA) is a Federal law that compels the disclosure of agency records to any person upon written request, unless one or more of nine exemptions apply to the records (see Title 38 Code of Federal Regulations (CFR) 1.554(a) (1)-(9)) and Title 5 United States Code (U.S.C.) 552, implemented by 38 CFR §§ 1.550-1.559).

l. **Health Information.** Health Information is any information, whether oral or recorded in any form or medium, created or received by a health care provider, health plan, public health authority, employer, life insurers, school or university, or health care clearinghouse or health plan that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual. This encompasses information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions. Source: 45 CFR § 160.103

m. **Individually Identifiable Health Information.** Individually Identifiable Health Information (IIHI) is a subset of Health Information, including demographic information collected from an individual, that: (1) is created or received by a health care provider, health plan, or health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA); (2) relates to the past, present, or future physical or mental condition of an individual, or provision of or payment for health care to an individual; and (3) identifies the individual or where a reasonable basis exists to believe the information can be used to identify the individual. ***NOTE****: VHA uses the term IIHI to define information covered by the Privacy Act and the Title 38 confidentiality statutes in addition to HIPAA.*

n. **Individually Identifiable Information.** Individually Identifiable Information (III) is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as IIHI regardless of how it is retrieved. III is a subset of personally identifiable information and is protected by the Privacy Act.

o. **Limited Data Set.** A Limited Data Set (LDS) is protected health information which excludes certain specified direct identifiers of the individual, his relatives, household members, or employers. These excluded identifiers include the following: 1) names; 2) address (other than town or city, state, or zip code); 3) phone number; 4) fax number; 5) e-mail address; 6) Social security numbers (SSN); 7) medical record numbers; 8) health plan numbers; 9) account numbers; 10) certificate and/or license numbers; 11) vehicle identification; 12) device identifiers; 13) web universal resource locators (URL); 13) internet protocol (IP) address numbers; 14) biometric identifiers; and 15) full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, state, or zip code. Thus, an LDS is not de-identified information, and it is covered by the HIPAA Privacy Rule. An LDS may be used and disclosed for research, health care operations, and public health purposes pursuant to a DUA. Source: 45 CFR § 164.514(e)(2)(i).

p. **Memorandum of Understanding.** A Memorandum of Understanding (MOU) is a document which defines the responsibilities of the parties entering into the agreement. MOUs are generally recognized as binding, even if no legal claim could be based on the rights and obligations laid down in them.

q. **Non-VA User.** A non-VA user is any individual who accesses VA IT Systems for the purpose of conducting activities other than for an official VA purpose. Non-VA users include VSOs, some researchers, employees of other government agencies, and others. Access to data

by a non-VA user may be given only within the appropriate authorities of Federal laws, regulations and VA and VHA policies.

r. **Patient Identifiers.** Patient identifiers are the 18 data elements attributed to an individual under the HIPAA Privacy Rule that must be removed from health information for it to be de-identified and no longer covered by the Rule. Please see VHA Handbook 1605.1, Privacy and Release of Information, Appendix B, De-identification of Data, for more detail.

s. **Protected Health Information.** The HIPAA Privacy Rule defines Protected Health Information (PHI) as III transmitted or maintained in any form or medium by a covered entity, such as VHA. ***NOTE****: VHA uses the term protected health information to define information that is covered by HIPAA but, unlike III, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer.*

t. **Requestor.** For the purposes of this Handbook, the Requestor is the person, program office, or entity generating applications to receive VHA III or PHI.

u. **VA Information Technology Systems.** For the purposes of this Handbook, VA Information Technology Systems (VA IT Systems) are any electronic systems containing III or PHI belonging to VHA and that are maintained by either VA or VHA.

v. **VA User.** A VA user is any individual who accesses VA IT Systems for the purpose of conducting official activities on VA's behalf. VA users include all staff, contractors, students, interns, VA researchers, volunteers, and others in an officially supervised capacity performing a sanctioned function for VA.

w. **VHA Data**. For the purposes of this directive, VHA data are factual information related to the VA organizational component responsible for coordinating and providing health care for enrolled Veterans; this information is contained in multiple system levels, including local data residing in Veterans Health Information Systems Architecture (VistA); multiple-source VistA data combined into Network data warehouses; databases constructed from rolled-up local facility data housed in central locations.

4. SCOPE:

a. The goal of this Handbook is to provide guidance to Requestors seeking access to VHA PHI and III, and to VHA Data Owners and/or officials with operational authority and responsibility for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination or disposal. This Handbook defines standard procedures for managing and monitoring DUAs, describes when DUAs are required or prohibited, and applies to VHA data shared with Authorized Users.

b. This Handbook does not apply to the sharing or transmission of VHA research data in research data repositories or in the possession of VHA research investigators. Requirements

related to the use of DUAs in these circumstances can be found in VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research.

5. RESPONSIBILITIES:

a. **VHA Health Information Access.** As a component under NDS, the VHA Health Information Access (HIA) program is responsible for establishing and distributing policies and procedures for access to VHA III and PHI, including the utilization of DUAs, and for development and maintenance of processes and mechanisms for collecting, storing, managing, and reporting DUAs on behalf of VHA.

b. **VHA Privacy Office.** The VHA Privacy Office will review DUAs when they are related to disclosures outside VA of national level VHA data requiring national level permissions. The VHA Privacy Office will determine if a DUA is required and if there is legal authority for the release of VHA data. The VHA Privacy Office will draft an approval letter for the signature of the Under Secretary for Health, should one be required to accompany a DUA.

c. **VHA FOIA Office.** VHA FOIA Office is responsible for determining whether the requested information is releasable under the provisions of the FOIA.

d. **VHA Privacy Compliance Assurance Office.** VHA Privacy Compliance Assurance (PCA) Office will monitor compliance with this Handbook in accordance with VHA Handbook, 1605.03 Privacy Compliance Assurance Program and Privacy Compliance Monitoring, and will report its findings to HIA on an annual basis, utilizing its current methodologies and 3-year review cycle.

e. **VHA Health Care Security Requirements Office.** VHA Health Care Security Requirements (HCSR) Office will review DUAs in instances of disclosures of national VHA data outside VA, when such DUAs are required, to ensure security requirements and responsibilities are properly documented.

f. **VISN Directors, Chief Officers, Program Officers, and Medical Facility Directors.** VISN Directors, Chief Officers, program officers, and medical facility Directors are responsible for ensuring that all personnel under their direction comply with the requirements of this policy.

g. **VHA Data Owners.** VHA Data Owners must enter into a DUA before transferring or sharing VHA data, as required by this Handbook and other VHA policy. The Data Owner must determine whether ownership is retained or relinquished when sharing VHA data with non-Federal entities. The Data Owner must consult with the Privacy Officer and others as appropriate, to determine if the data can and should be shared, and if relinquishing ownership is appropriate. The Data Owner is accountable for the release of the data and for monitoring any DUA the Data Owner generates as defined by this Handbook.

h. **VHA Data Owner's Information Security Officers.** The VHA Data Owner's Information Security Officer (ISO) will review and provide concurrence or non-concurrence for all DUAs generated by that Data Owner based on compliance with VA security policies.

i. **VHA Data Owner's Privacy Officers and/or VHA Program Office Privacy Liaison.** The VHA Data Owner's Privacy Officers and/or the VHA Program Office Privacy Liaison will review and provide concurrence or non-concurrence for all DUAs generated by that Data Owner based on whether privacy legal authority exists for sharing VHA data. VHA facility Privacy Officers will annually review their facility's compliance with this Handbook and report these findings to PCA as a part of the facility self-assessment survey to ensure that an annual review of compliance is maintained.

6. DETERMINING WHEN A DUA IS REQUIRED OR PROHIBITED:

a. Determining if a DUA is required or prohibited is based upon who is requesting the information, and how, and for what purpose the Requestor will use the data. Please refer to Appendix A, *DUA Decision Tree*, and Appendix B, *Case Use Examples,* for further detail.

b. A DUA is:

(1) Used to document the transfer of liability to an external entity if ownership of the data transfers.

(2) Used to bind the behavior of the Requestor to specific uses or limitations of the data if ownership is retained by VHA.

(3) Used to document ownership status and establishes appropriate rules based on this status and establishes criteria to use, disclose, store, process, make copies, transfer and dispose of data, and identifies who will have access to and control of the information at both origination and Requestor locations.

(4) Used only in situations where VHA may condition the use, release or disclosure of VHA data on the signing of the DUA as VHA has discretion in deciding to provide the data.

(5) Not used in situations where VHA is mandated by policy, or required by law or regulation, to release or disclose the data.

c. Whether a DUA is required or prohibited, the Data Owner still has the responsibility to account for the data and to protect data under their ownership. At a minimum, the following data elements must be captured for aggregate reporting purposes:

(1) Name of the Requestor;

(2) The nature of the data shared;

(3) The stated use of the data;

(4) The authority under which the data was shared;

(5) Final disposition of the data; and

(6) The ownership status of the data provided to the requestor.

d. A DUA is required in the following instances:

(1) When sharing an LDS as defined in this Handbook in accordance with Federal laws or regulations. The HIPAA Privacy Rule requires that, when a covered entity uses or discloses an LDS, the covered entity shall use a DUA to ensure the Requestor of the LDS will only use or disclose the PHI for specific purposes. This requirement applies whether the LDS is being shared inside VHA, with other VA entities, or outside VA.

(2) When VHA III or PHI is to be shared with a non-VA entity, a DUA is required prior to the disclosure unless prohibited in sub-section 6e of this Handbook. VHA must be able to identify the specific legal authority that would allow for such a disclosure. The VHA Privacy Office can provide guidance on legal authorities by contacting VHAPrivIssues@va.gov.

(3) When it is the intention to retain ownership, control of its use, and liability when sharing VHA data pursuant to written authorization. The DUA, or some other document acting as a DUA as outlined in this Handbook, must explicitly state retention of ownership of the data.

(4) In special circumstances such as when a signed agreement is in place (see paragraph 7 of this Handbook).

e. Under certain circumstances a DUA is prohibited by Federal laws, regulations, and VA and VHA policies. These requirements preclude VHA from putting any further conditions upon the release or disclosure of the data. DUAs are prohibited in the following circumstances, except as otherwise required under paragraph 6d, or paragraphs 7a or 7c:

(1) When sharing VHA data within VA unless noted in Paragraph 7 of this Handbook. ***NOTE:*** *This does not prohibit Veterans Benefits Administration (VBA) or National Cemetery Administration (NCA) from creating DUAs to share VBA III or NCA III with VHA.*

(2) When VHA receives a properly completed FOIA request;

(3) When VHA data are requested by an entity that is charged with health care oversight of VA specifically for their oversight activities, including but not limited to:

(a) The White House;

(b) The Office of Management and Budget (OMB);

(c) A Member of Congress;

(d) The House Veterans' Affairs Committee (HVAC) and/or Senate Veterans' Affairs Committee (SVAC);

(e) The Government Accountability Office (GAO);

(f) The Department of Health and Human Services, Office for Civil Rights;

(g) VHA Office of Research Oversight (ORO);

(h) VA Office of the Inspector General; and

(i) The Office of the Secretary of Veterans Affairs for purposes of health care oversight.

(4) When VHA data are requested by a law enforcement entity for a specific criminal activity pursuant to a Privacy Act (b)(7) letter and for law enforcement reporting pursuant to a standing written request letter.

(5) When VHA data are requested by a State Public Health Authority pursuant to a standing written request letter or when VHA initiates release to the State Public Health Authority for the purpose of promoting public health and patient safety with the exception of a State Cancer Registry.

(6) When VHA data are disclosed to a State Abuse Hotline in order to report suspected or alleged abuse.

(7) When VHA data are disclosed for the purpose of treatment or payment.

(8) When VHA data are requested by a Member of Congress in response to an inquiry from a Veteran for assistance in a VA matter. This is not considered health care oversight. *NOTE: A written authorization or a copy of the original correspondence from the Veteran requesting the Member's assistance must be provided.*

(9) When VHA data are disclosed to the Veteran or his/her legal representative (e.g., a VSO), or to a family member or friend involved in the Veteran's care or payment for care.

(10) When an agreement is in place that expressly and wholly binds specific behavior related to data sharing, such as certain MOUs.

(11) When a BAA is in place that governs the business relationship between VHA and the entity except for otherwise permitted in this Handbook.

NOTE: *This Handbook eliminates the use of the term DTA within VHA. Any DTA created prior to this Handbook, or used as a term in other VHA policy will be considered a DUA until it is replaced as outlined in Paragraph 8b. Some organizations outside VHA utilize the term Data Sharing Agreement. This Handbook does not address the use of this term by those organizations.*

7. SPECIAL CIRCUMSTANCES & EXCEPTIONS:

a. In some circumstances internal DUAs are required by agreement with external entities, such as the Centers for Medicare and Medicaid Services (CMS), when those external entities' data are subsequently shared within VHA. These mandates specify particular handling and processing requirements in order to track internal redistribution of the information (see Appendix B, *Case Use Examples,* for further detail).

b. A DUA is not needed if there is some other document, such as an Memorandum of Agreement (MOU) that cites the authority to disclose data and which expressly documents the limitations, if any, of the data sharing. Depending on the reason for the data sharing, any such agreement may have to include the content contained in the appropriate DUA template.

c. When data are being obtained from research data repositories or data are already in possession of VHA research investigators, all requirements for DUAs found in VHA Handbook 1200.12, *Use of Data and Data Repositories in VHA Research,* must be followed. If a VHA researcher is requesting data for research purposes, and the data are from a non-research source, such as the Corporate Data Warehouse, VHA researchers must follow the requirements of this DUA Handbook.

8. ESTABLISHING DUAS:

a. When a DUA is required by regulation or VHA policy, the DUA template(s) referenced in this policy or any subsequent version released by HIA must be used. These templates facilitate Administration-wide reporting capabilities and ensure that required language is used as well as fostering the ease of data sharing. These templates are tailored for sharing VHA III or PHI with other Federal and non-Federal entities, and the sharing of information based on an LDS. The differences between these templates relate to the ownership of the data and the rules that are in place based on that ownership status (see Appendix C, *DUA Templates). **NOTE:** For situations that do not fall into the above scenarios please contact the HIA program within NDS.*

b. Any existing DUAs utilizing older templates created prior to publication of this Handbook are to be replaced with the new template within one year of this Handbook's publication, regardless of the expiration date of the existing DUA.

9. PROCESSING AND MONITORING DUAS

a. When the Data Owner has determined a DUA is required and the appropriate template has been completed, the DUA is reviewed and processed in accordance with Appendix D, DUA Process Flow. This process is outlined as follows:

(1) The appropriate DUA is generated by the VHA Data Owner and completed by the Requestor;

(2) The Data Owner's ISO and Privacy Officer/VHA Program Office Privacy Liaison must review the DUA to determine if the terms of the agreement comply with all applicable Federal

laws, regulations, and VA and VHA policies. The Data Owner's ISO and Privacy Officer written concurrence must be obtained prior to final signatures;

(3) The DUA is signed by the VHA Data Owner and the Designated Signatory Official of the Requestor;

(4) The VHA Data Owner determines whether a national review by VHA HCSR Office and VHA Privacy Office is appropriate. This includes situations where the data being disclosed is either of a national-level (such as data stored within national data warehouses or registries and which contains patient or beneficiary information) and/or is released on a recurring basis; and

(5) A signed copy of the completed DUA must be forwarded to NDS for tracking purposes. Instructions for submission are provided on the DUA Page on the VHA Data Portal (http://vaww.vhadataportal.med.va.gov/DataAccess/DUA.aspx). This is considered the official Federal Record. ***NOTE:*** *This is a VA internal Web site, not available to the public.*

b. In circumstances wherein guidance to prohibit or permit disclosure of the data are not defined in law, regulation, or VHA policies; the DUA must be reviewed and approved by the OGC.

c. If there is an approval letter that must be signed by the Under Secretary for Health, OGC must review and concur prior to gaining the signature of the Under Secretary for Health.

d. VHA Data Owners are accountable for ensuring the terms of the DUA are being met and shall confirm compliance with the Requestor on an annual basis, if ownership is retained by VHA. If the VHA Data Owner, facility Privacy Officer, or facility ISO suspects the terms of a DUA are not being met, the VHA PCA Office must be notified to schedule an assessment to determine if the Requestor is compliant with the DUA. If it is determined that the terms of the agreement are not being met, PCA will provide a written report specifying the details. PCA will develop a remediation strategy that must be satisfied by the Requestor.

e. VHA facility Privacy Officers, in collaboration with facility ISOs, will annually review their facility's compliance with this Handbook and report these findings to PCA as part of the facility self-assessment survey to ensure an annual compliance review is maintained. HIA and PCA will collaborate to define the assessment scope, questions to be asked and observations to be made during PCA and facility self-assessment surveys.

10. REFERENCES:

a. Freedom of Information Act (FOIA), 5 U.S.C. 552.

b. Privacy Act of 1974, 5 U.S.C. 552a.

c. HIPAA Privacy Rule 45 CFR Parts 160 and 164.

d. VA Directive 6066, Protected Health Information (PHI).

e. VA Handbook 6500, Managing Information Security Risk : VA Information Security Program.

f. VA Handbook 6500.6, Contract Security.

g. VHA Directive 1605, VHA Privacy Program.

h. VHA Handbook 1605.1, Privacy and Release of Information .

i. VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information.

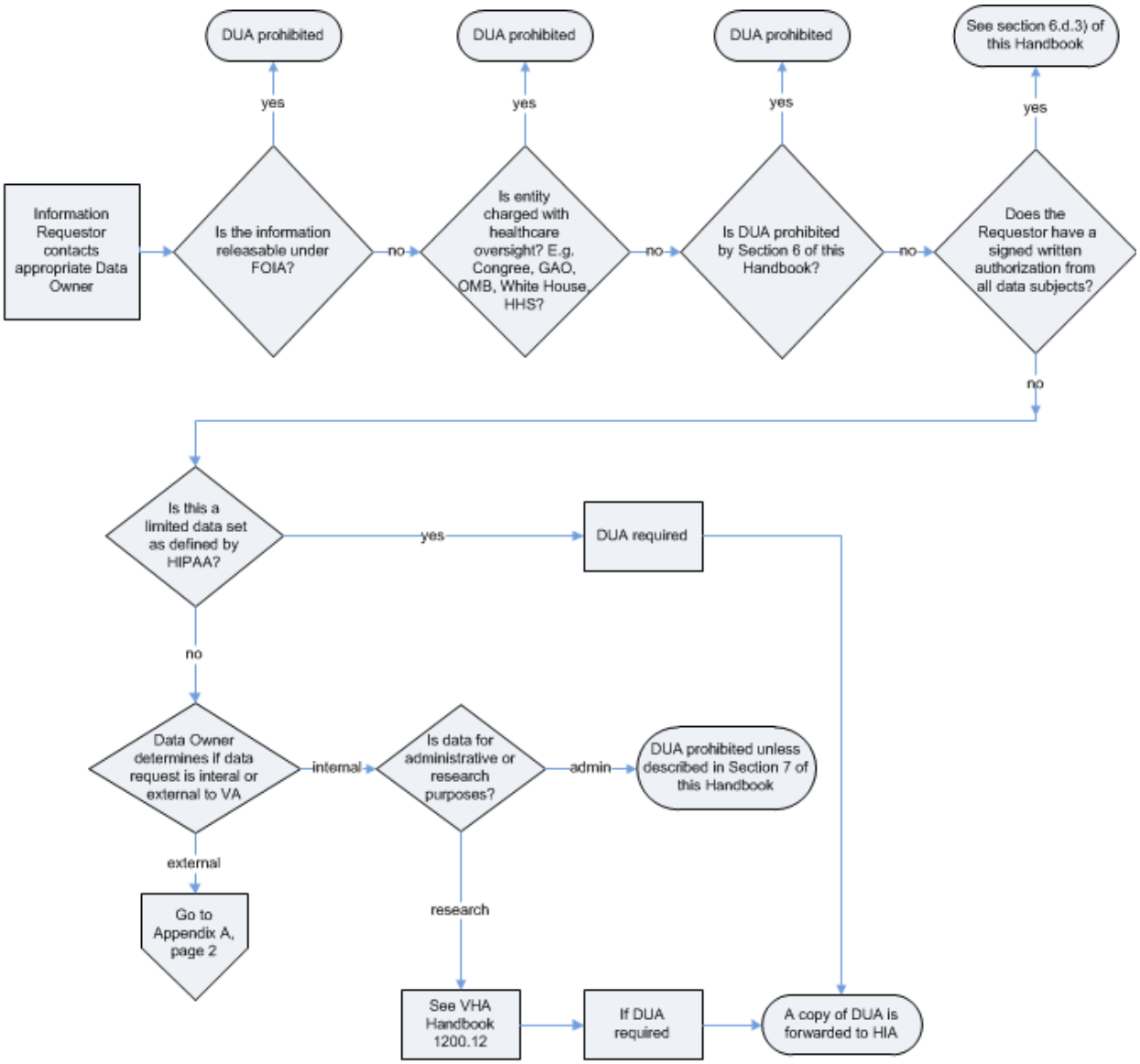
j. VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research.

k. VHA Directive 2010-019, Access to Centers for Medicare and Medicaid Services (CMS) Data for VHA Users Within the VA Information Technology (IT) Systems.

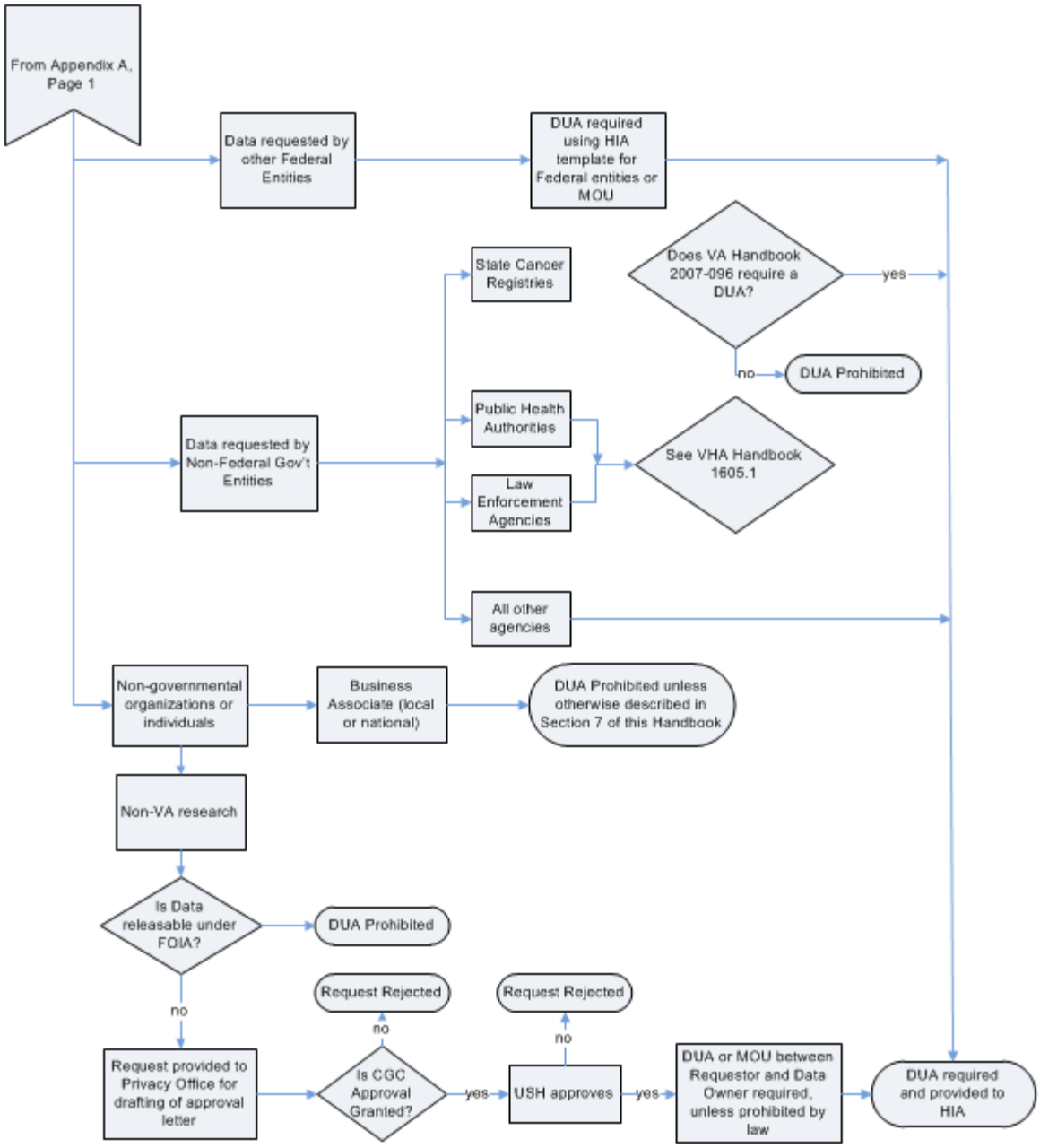
l. VHA Directive 2009-046, Release of VA Data to State Cancer Registries.

DUA DECISION TREE

Page 1



Page 2


From Appendix A, Page 1
Data requested by other Federal Entities
DUA required using HIA template for Federal entities or MOU
State Cancer Registries
Does VA Handbook 2007-096 require a DUA?
yes
no
DUA Prohibited
Public Health Authorities
Data requested by Non-Federal Gov't Entities
See VHA Handbook 1605.1
Law Enforcement Agencies
All other agencies
Non-governmental organizations or individuals
Business Associate (local or national)
DUA Prohibited unless otherwise described in Section 7 of this Handbook
Non-VA research
Is Data releasable under FOIA?
DUA Prohibited
no
Request Rejected
Request Rejected
no
no
Request provided to Privacy Office for drafting of approval letter
Is CGC Approval Granted?
yes
USH approves
yes
DUA or MOU between Requestor and Data Owner required, unless prohibited by law
DUA required and provided to HIA

CASE USE EXAMPLES

Section 6 of this Handbook provides overall guidance when Data Use Agreements (DUA) are required or prohibited. Generally speaking, DUAs are prohibited when sharing Veteran Health Administration (VHA) individually identifiable information (III) and VHA protected health information (PHI) internally to Veterans Affairs (VA), and required when sharing VHA III/PHI outside VA. There are exceptions to this statement. This Appendix provides additional guidance on, and exceptions to, these rules, as well as identifies other sources of governance.

1. CENTERS FOR MEDICARE AND MEDICAID SERVICES (CMS) DATA: In compliance with the Information Exchange Agreement between VHA and CMS, and VHA Directive 2010-019, *Access to Centers of Medicare and Medicaid Services (CMS) Data for VHA Users within VA Information Technology (IT) Systems*, VHA is required to create internal DUAs when redistributing CMS raw and merged data (VA/CMS data) to internal VHA users.

a. Guidance for providing VA/CMS data for administrative purposes is provided by VHA Medicare and Medicaid Analysis Center (MAC). MAC policy for obtaining VA/CMS data, including the requirement for a DUA can be found under the "How to Request CMS Data" tab on the MAC homepage (http://vaww.va.gov/medicareanalysis/). ***NOTE:*** *This is a VA internal Web site, not available to the public.*

b. Guidance for providing VA/CMS data for research purposes is provided by VA Information Resource Center (VIReC). VIReC policy for obtaining VA/CMS data can be found in the document "VIReC's VA/CMS Data for Research Projects Policies (http://vaww.virec.research.va.gov/Index-VACMS.htm)." ***NOTE:*** *This is a VA internal Web site, not available to the public.*

2. LIMITED DATA SETS (LDS): A DUA is required whenever sharing data that meets the definition of an LDS under the Health Insurance Portability and Accountability Act (HIPAA). (For guidance on LDS please refer to VHA Handbook 1605.1, Privacy and Release of Information.) This is a circumstance wherein an internal DUA is required.

3. NON-FEDERAL GOVERNMENT ENTITIES:

a. **State Cancer Registries.** (see VHA Handbook 1605.1, Privacy and Release of Information, and VHA Directive 2009-046, Release of VA Data to State Cancer Registries for guidance.)

b. **Public Health Authorities.** (see VHA Handbook 1605.1 Privacy and Release of Information 1605.1 for guidance.)

c. **State, Local or Municipal Courts.** VHA IIIand PHI may be released for use in proceedings of a state, local or municipal court upon receipt of a court order or a subpoena issued or approved by a judge. In the presence of a court order, or for discovery proceedings, a DUA is prohibited. Please reference VHA Handbook 1605.1, Privacy and Release of Information for more information. ***NOTE:*** *If the data are from a research project that is covered by a*

Certificate of Confidentiality issued by the National Institutes of Health the VHA Office of Research and Development should be contacted. A Certificate of Confidentiality is issued to protect identifiable research information from forced disclosure. See http://grants.nih.gov/grants/policy/coc/ for more information.

d. **All Other Non-Federal Government Entities.** VHA Data Owners may authorize disclosure of VHA data to other non-Federal government agencies in accordance with Federal law, the HIPAA Privacy Rule, or VA and VHA policy. Absent a signed, written authorization from the data subject and those exceptions listed in Paragraph 7 of this Handbook, a DUA, or other documentation that contains the elements of a DUA is required, unless prohibited by law, regulation, or VA/VHA policies. If the data are to be used by a Business Associate, contractor, or other non-government agent on behalf of the Requestor, then this must be specified in the DUA. ***NOTE:*** *The Privacy Officer must identify the authority under which the data may be disclosed.*

4. NON-GOVERNMENTAL ORGANIZATIONS OR INDIVIDUALS:

a. **Business Associate.** A DUA is prohibited when sharing VHA III/PHI with entities operating under Business Associate Agreements (BAA) with VHA. There is an exception however when VHA is required by agreement to have a DUA when sharing data with a Business Associate, such as when sharing CMS data.

b. **FOIA Requests.** If the requested data are processed under the Freedom of Information Act (FOIA), a DUA is prohibited. The request must be processed by the VHA FOIA Officer in accordance with VHA policy.

c. **Non-VA Research.** VHA data will at times be requested by non-VA investigators for research projects that are not VA research projects. The definition of VA research is found in VHA Directive 1200 and VHA Handbook 1200.01. There are a number of ways data requests may be classified that affect handling of the request and may or may not require a DUA.

(1) A DUA is required when it is the intention to retain ownership, control of its use, and liability when sharing VHA data pursuant to written authorization.

(2) A DUA is required if written authorization from all data subjects is not obtained. A written request must be provided and accompanied with the following information:

(a) A copy of the research protocol;

(b) The approval letter from the Requestor's Institutional Review Board (IRB) of record;

(c) Documentation of a HIPAA waiver of authorization approved by the IRB; and

(d) Approval from the Under Secretary for Health or designee. This process is managed by the VHA Privacy Office and they should be contacted for questions about the approval process. Once the Under Secretary for Health's Approval Letter is obtained, that letter is cited in the

DUA as the authority to release the data and the DUA is processed in accordance with the standard procedures outlined in this document.

1. A DUA is prohibited if the requested data for non-VA research is processed under FOIA. The request must be processed by the appropriate VHA FOIA Officer in accordance with the FOIA statute and VHA policy.

2. A DUA is required if a LDS is disclosed under the HIPAA Privacy Rule and VHA Handbook 1605.1.

5. OTHER FEDERAL GOVERNMENT ENTITIES: VHA may share data with other Federal agencies provided a DUA is in place in order to ensure that the data will only be used for the purpose(s) for which it was requested. DUAs are prohibited in the following circumstances:

a. **Other VA Entities.** When sharing VHA III/PHI with other VA entities. If the other VA entity is providing a service for VHA under a BAA, VHA privacy policies apply to the data as outlined in VA Directive 6066, *Protected Health Information*. If VHA provides III or protected health information (PHI) to the other VA entity not pursuant to a BAA, VHA privacy policies would not apply to the data.

b. **Federal Entities Charged with Healthcare and/or Research Oversight.** When VHA data are requested for oversight activities by a Federal government agency charged with health care oversight. Examples of such agencies include but are not limited to: The Executive Office of the President, the Office of Management and Budget, a Member of Congress, the United States House of Representatives Committee on Veterans' Affairs or its respective sub-committees, the United States Senate Committee on Veterans' Affairs or its respective sub-committees, the United States Department of Health and Human Services, the United States Department of Veterans Affairs Office of the Inspector General, and the Governmental Accountability Office.

c. **Federal Courts.** VHA III/PHI will be disclosed for use in proceedings of a Federal court upon receipt of a court order or a subpoena issued or approved by a judge. (Please reference VHA Handbook 1605.1, *Privacy and Release of Information* for more information.) ***NOTE:*** *If the data are from a research project that is covered by a Certificate of Confidentiality issued by the National Institutes Health, the VHA Office of Research and Development should be contacted. A Certificate of Confidentiality is issued to protect identifiable research information from forced disclosure. See http://grants.nih.gov/grants/policy/coc/ for more information.*

6. VA CONTRACTORS: VHA prohibits a DUA to share data with VA contractors pursuant to a valid contract that includes a description of the use, the transfer, and all privacy and security requirements in VA Handbook 6500.6 are met. ***NOTE:*** *For more information on the security requirements in contracts reference VA Handbook 6500.6.*

7. VA RESEARCH: For additional information about VA Research please see VHA Handbooks 1200.01 and associated VHA 1200 series Handbooks.

a. For guidance on the requirements for DUAs for VA Research if the data are being obtained from a research data repository or for data which is in the possession of VHA research investigators, see VHA Handbook 1200.12, *Use of Data and Data Repositories in VHA Research*.

b. For guidance on use of data for activities preparatory to research see VHA Handbooks 1200.12 and 1200.05. ***NOTE*:** *Access to data for preparatory to research is only granted to VA investigators.*

DATA USE AGREEMENT (DUA) TEMPLATES

The DUA templates have been designed to contain the essential elements that describe the use and disclosure of Veterans Health Administration (VHA) individually identifiable information (III)/VHA protected health information (PHI) being shared. All templates describe what VHA III/PHI is being shared and with whom, and ensure the appropriate levels of security and privacy reviews are conducted. All templates cite the authorities under which VHA may share the data and describe the means of its transfer, storage and access. These templates vary from each other based on ownership status of the requested data, and the language associated with protecting the data based on that ownership status.

1. DUA FOR FEDERAL ENTITIES: In this circumstance, ownership of the copy of the data transfers to the other Federal entity. As a component of the Federal government, the entity is subject to much of the same information security laws and regulations, such as the Federal Information Security Management Act (FISMA) and Federal Information Processing Standards (FIPS) as VA.

When sharing VHA III/PHI with other Federal entities, the data may become part of those Federal entities' Privacy Act System of Records (SOR), contingent upon whether a personal identifier is used to retrieve information by the Federal entity. In other instances where information is not retrieved by a personal identifier, references to a Privacy Act System of Records will not be applicable and should not be included in the DUA. ***NOTE:*** *Information disclosed as part of an LDS cannot be retrieved by an individual identifier (i.e., name, account number, email address, picture, SSN, etc.) and therefore is not covered by the Privacy Act.*

NOTE: *See Appendix E for a DUA with Federal Entities.*

2. DUA FOR NON-FEDERAL ENTITIES: When sharing VHA III/PHI with non-Federal entities, VHA may choose to retain or relinquish ownership of the data. The DUA binds the behavior of the Requestor to specific uses or limitations of the data.

NOTE: *See Appendix F for a DUA with Non-Federal Entities.*

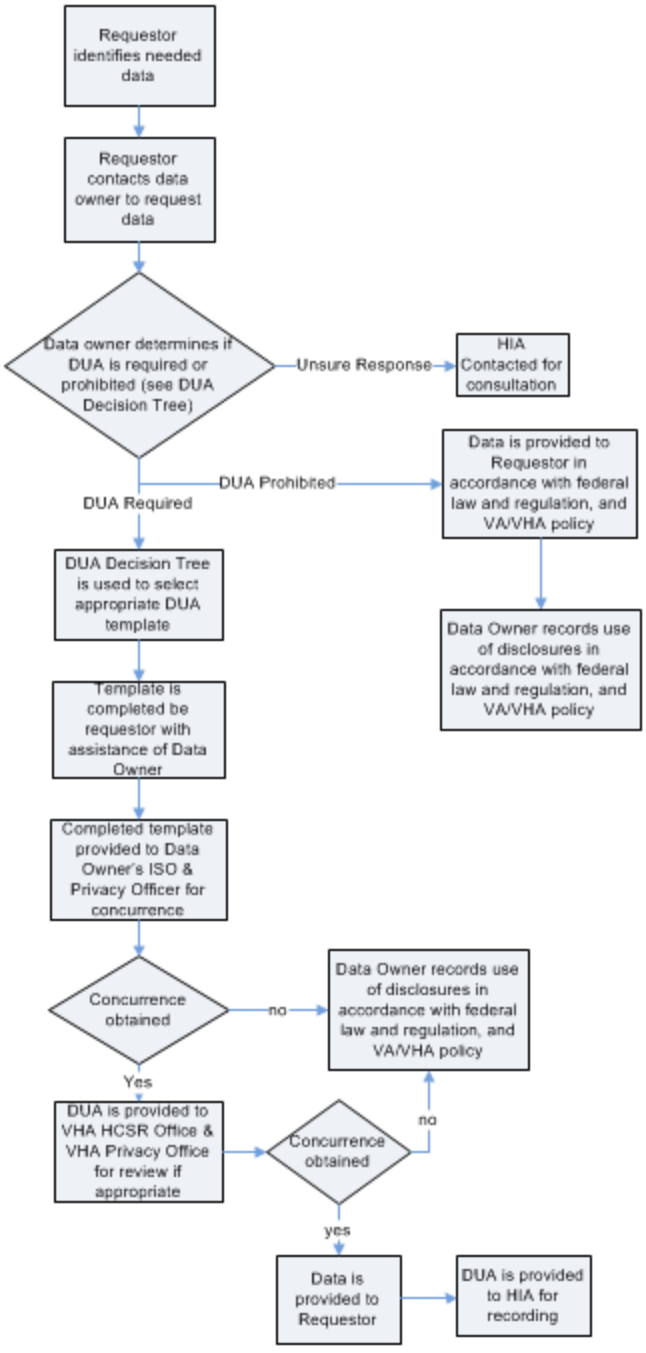
3. DUA FOR LDS WITH FEDERAL ENTITIES: This template has specific language to address requirements of the HIPAA Privacy Rule.

NOTE: *See Appendix G for a DUA for LDS with Federal Entities.*

4. DUA FOR LDS WITH NON-FEDERAL ENTITIES: This template has specific language to address requirements of the HIPAA Privacy Rule.

NOTE: *See Appendix I for a DUA for LDS with Non-Federal Entities.*

DUA PROCESS FLOW



DATA USE AGREEMENT WITH FEDERAL ENTITIES

FOR DATA FROM THE DEPARTMENT OF VETERANS AFFAIRS (VA), VETERANS HEALTH ADMINISTRATION (VHA) TO THE <INSERT NAME OF FEDERAL ENTITY> FOR <INSERT PROJECT NAME>

Purpose:
This Agreement establishes the terms and conditions under which the Department of Veterans Affairs, VHA <INSERT FACILITY/PROGRAM OFFICE> will provide, and <INSERT NAME OF FEDERAL ENTITY> will use VHA individually identified information/VHA protected health information (VHA III/PHI).

References and Authorities:
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- The Health Insurance Portability and Accountability Act of 1994, Pub. L. 104-191
- Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information (HIPAA Privacy and HIPAA Security Rules), 45 C. F. R. §§ 160, 164.
- Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001
- The HITECH Act, Pub. L. 109-1
- System of Records Notice (SORN) <INSERT VHA SORN NUMBER>, <INSERT NAME OF VHA DATABASE and (DATE and FEDERAL REGISTRY CITATION NUMBER)>
- System of Records Notice (SORN) <INSERT FEDERAL ENTITY SORN NUMBER>, <INSERT NAME OF FEDERAL ENTITY DATABASE and (DATE and FEDERAL REGISTRY CITATION NUMBER)>

TERMS OF THE AGREEMENT:

1. This Agreement is by and between VHA <INSERT FACILITY/PROGRAM OFFICE> and the <INSERT NAME OF FEDERAL ENTITY>

2. This Agreement supersedes any and all agreements between the parties with respect to the transfer and use of data for the purpose described in this agreement, and pre-empts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any other prior communication with respect to the data and activities covered by this Agreement.

3. The VHA <INSERT FACILITY/PROGRAM OFFICE NAME> will transfer to <INSERT NAME OF FEDERAL ENTITY PROGRAM OFFICE RECEIVING INFORMATION>, through <DESCRIBE SECURE MEANS OF TRANSFER>, any and all related data for:
- <INSERT PURPOSE>;
- <INSERT ADDITIONAL PURPOSE>.

VHA III/PHI to be transferred from VHA <INSERT VHA PROGRAM OFFICE> to the <INSERT NAME OF FEDERAL ENTITY> may include, but is not limited to:

- <NAME DATA ELEMENTS>

4. VHA will retain ownership of the original data and the Federal agency will receive a copy. Data transferred under this agreement becomes the property of <INSERT NAME OF FEDERAL ENTITY>. The data shall be treated by <INSERT NAME OF FEDERAL ENTITY> in the same manner as other individually identifiable information maintained under the Privacy Act by <INSERT NAME OF FEDERAL ENTITY>. The data will be incorporated into <INSERT NAME OF FEDERAL ENTITY> Privacy Act Systems of Records (SOR) "<INSERT NAME OF FEDERAL ENTITY DATABASE>" (<INSERT SORN NUMBER OF FEDERAL ENTITY DATABASE>).The following named individuals are designated as Technical Representatives of VHA, and the <INSERT NAME OF FEDERAL ENTITY>, who will arrange for transfer of the VHA III via <DESCRIBE SECURE MEANS OF TRANSFER> to the <INSERT NAME OF FEDERAL ENTITY> for their use. The <INSERT NAME OF FEDERAL ENTITY> Technical Representative will be responsible for complying with all conditions of use and for establishment and maintenance of security arrangements to prevent unauthorized use or disclosure of the data provided under this agreement. <INSERT NAME OF FEDERAL ENTITY> agrees to notify VHA within 15 days of any change of circumstances affecting the ability of the <INSERT NAME OF FEDERAL ENTITY> to comply with terms of this agreement.

Technical Representative for <INSERT NAME OF FEDERAL ENTITY>:
<INSERT NAME, PHONE NUMBER AND EMAIL OF FEDERAL ENTITY TECHNICAL REPRESENTATIVE>

Technical Representative for VHA:
<INSERT NAME, PHONE NUMBER AND EMAIL OF VHA TECHNICAL REPRESENTATIVE>

5. The following named individuals are designated as their agencies' Points of Contact for performance with the terms of the Agreement. All questions of interpretation or compliance with the terms of this Agreement should be referred to the officials named below.

Point-of-Contact on behalf of <INSERT NAME OF FEDERAL ENTITY>:

<INSERT NAME, PHONE NUMBER AND EMAIL OF FEDERAL ENTITY POC>
Point-of-Contact on behalf of VHA:

<INSERT NAME, PHONE NUMBER AND EMAIL OF VHA POC>

6. The VHA III provided to <INSERT NAME OF FEDERAL ENTITY> under this Agreement will be covered by the Privacy Act SOR "INSERT SOR NAME Although <INSERT NAME OF FEDERAL ENTITY> will own the copy of VHA III/ PHI transferred under this Agreement, it agrees not to disclose the VHA III/ PHI to any person outside the <INSERT NAME OF FEDERAL ENTITY> except as required by law. pursuant to a Freedom of Information Act (FOIA) request, as authorized by Federal statute or regulation, <INSERT VHA SORN NAME AND NUMBER> or pursuant to a court order from a court of competent jurisdiction.

7. <INSERT NAME OF FEDERAL ENTITY PROGRAM OFFICE> will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the data covered by this Agreement and to prevent unauthorized use or access to it. As a component of a federal agency, <INSERT NAME OF FEDERAL ENTITY PROGRAM OFFICE> will conform to the applicable Federal Information Processing Standards (FIPS) and Special Publications developed by the National Institute of Standards and Technology and, the common information security laws and regulations, such as the Federal Information Security Management Act (FISMA). The use of unsecured telecommunications, including the Internet, to transmit individually-identifiable or deducible information derived from VHA III/ PHI covered by this Agreement is prohibited, unless VHA and <INSERT NAME OF FEDERAL ENTITY> agree to transmit any data in an encrypted form which meets the encryption requirements of FIPS 140-2.

8. In the event <INSERT NAME OF FEDERAL ENTITY> as the data owner determines or reasonably believes that an unauthorized disclosure of the data shared in this Agreement has occurred, <INSERT NAME OF FEDERAL ENTITY> will follow all appropriate breach protocols as required by Federal law. developed under FISMA and statutory protocols under <INSERT THE CORRECT AUTHORITY i.e., HIPAA, HITECH, and title 38 OR THE OMB REQUIREMENTS ON ALL FEDERAL AGENCIES\>, which include but are not limited to the following: (1) Immediately notifying its Privacy Officer/Chief Information Officer of the potential breach; (2) Working with its breach response program to investigate and assess the nature and scope of the breach and taking all appropriate actions; (3) Identifying all individuals involved who are the subject of the breach; and (4) Providing all necessary notifications to the individuals involved as required by <INSERT APPROPRIATE LANGUAGE FROM ABOVE> and [INSERT NAME OF FEDERAL ENTITY] policy. [INSERT NAME OF FEDERAL ENTITY] will immediately notify VHA of any identified potential breaches and will share findings of the breach investigation and remediation activities with VHA in a timely manner. After notification of a breach, VHA may request [INSERT NAME OF FEDERAL ENTITY] perform a security and privacy compliance assessment to ensure adequate processes are in place for the protection of the data. [INSERT NAME OF FEDERAL ENTITY] agrees to share all findings from the security and privacy compliance assessment with VHA.

9. Authority for <INSERT PROGRAM OFFICE> to share this data for the purpose indicated is under this Agreement are as follows: HIPAA Privacy Rule provision <45 CFR INSERT LEGAL CITATION>, the Privacy Act is [INSERT LEGAL CITATION OR ROUTINE USE FROM THE APPLICABLE PRIVACY ACT SYTEM OF RECORD] and 38 USC 5701(b)(3) <IF THIS STATUTE IS APPLICABLE> and 38 USC 7332 <INSERT LEGAL CITATION, IF THIS STATUTE IS APPLICABLE>.

10. 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.

11. This Agreement may be terminated by either party, at any time, and for any reason upon 30 days written notice from the terminating party to the other party.

12. On behalf of VHA and <INSERT NAME OF FEDERAL ENTITY>, each undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____ _____
<INSERT NAME OF FEDERAL ENTITY SIGNER> Date
<INSERT TITLE OF FEDERAL ENTITY SIGNER>
<INSERT PROGRAM OFFICE OF FEDERAL ENTITY>
<INSERT NAME OF FEDERAL ENTITY>

_____ _____
<INSERT NAME OF VHA SIGNER> Date
<INSERT TITLE OF VHA SIGNER>
<INSERT VHA PROGRAM OFFICE>
Veterans Health Administration

Concur/Non-Concur:

_____
<INSERT NAME OF VHA FACILITY/PROGRAM OFFICE ISO>

_____
Signature and Date

Concur/Non-Concur:

_____
<INSERT NAME OF VHA FACILITY/PROGRAM OFFICE PRIVACY OFFICER>

_____
Signature and Date

DATA USE AGREEMENT (DUA) WITH NON-FEDERAL ENTITIES

AGREEMENT FOR DATA EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), <INSERT FACILITY OR PROGRAM OFFICE NAME> AND <INSERT NON-FEDERAL ENTITY NAME>

Purpose:
This Agreement establishes the terms and conditions under which the VHA <INSERT FACILITY/PROGRAM OFFICE NAME> will provide, and <INSERT ENTITY NAME>, its contractors and agents, will use VHA data <PROVIDE DESCRIPTION OF PROJECT INCLUDING TYPE OF DATA AND HOW IT WILL BE USED>.

TERMS OF THE AGREEMENT:

1. This Agreement is by and between <INSERT ENTITY NAME>, its contractors and agents (hereafter the "Requestor") and the VHA <INSERT FACILITY OR PROGRAM OFFICE NAME> (hereafter the "VHA"), a component of the U.S. Department of Veterans Affairs.

2. This Agreement supersedes any and all agreements between the parties with respect to the transfer and use of data for the purpose described in this agreement, and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any other prior communication with respect to the data and activities covered by this Agreement.

3. <SELECT ONE > VHA retains all ownership rights and responsibilities to the original and derivative data file(s) provided to the Requestor under this Agreement. <OR> VHA will retain ownership of the original data and <INSERT ENTITY NAME> will receive a copy. Data transferred under this agreement becomes the property of <INSERT ENTITY NAME>.

4. Upon completion of the project, or at the request of VHA after making an ownership decision, the Requestor will securely return or destroy, at VHA option, all data gathered, created, received or processed.

5. <INSERT NAME OF OFFICIAL AND ENTITY> will be responsible for the observance of all conditions of use and for establishment and maintenance of appropriate administrative, technical and physical security safeguards to prevent unauthorized use and to protect the confidentiality of the data. The Requestor agrees to notify the VHA within fifteen (15) days of any change in the named Requestor.

6. VHA will ensure the secure transfer of the data to <INSERT NAME OF OFFICIAL AND ENTITY>. The method of transfer will be: <INSERT METHOD OF TRANSFER.>
The following named individuals are designated as their agencies' Points of Contact for performance of the terms of the Agreement. All questions of interpretation or compliance with the terms of this Agreement should be referred to the VHA official named below.

VHA's Point-of-Contact on behalf of <INSERT FACILITY/PROGRAM OFFICE NAME>

Name:
Title:
Telephone:

Other Points-of-Contact on behalf of <INSERT FACILITY/PROGRAM OFFICE NAME>

Name:
Title:
Telephone:

Points-of-Contact on behalf of <INSERT NON-FEDERAL ENTITY NAME>

Name:
Title:
Telephone:

7. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA], the requesting entity must provide the following information:

<DESCRIBE WHERE THE DATA WILL BE STORED:>

<DESCRIBE MEANS OF ACCESSING DATA AND ACCESS AUDIT METHODS:>

<PROVIDE DATE OF PROJECT COMPLETION:>

8. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] Except as VHA shall authorize in writing, <insert requesting entity name>, its contractors and agents, 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 or entity outside the Requestor and its team of subcontractors performing the Project. Without limitation to any other provision of this Agreement, the Requestor agrees not to disclose, display or otherwise make available any company proprietary information to any third party, in any form, except to public health officials or as required by law. VHA will clearly indicate in writing any information that is considered to be trade secret or confidential business information.

9. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] <INSERT ENTITY NAME>, its contractors and agents, shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with VA Handbook 6500, to protect VA data confidentiality and to prevent unauthorized access to the data provided by VHA. If co-mingling must be allowed to meet the requirements of the business/research need, the Requestor must ensure that VHA's information is returned to the VHA or destroyed in accordance with VA's sanitization requirements. VHA reserves the right to conduct onsite inspections of Requestor's IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA requirements.

All VHA data and derivative data must be stored in an encrypted partition on the Requestor's or its contractors'/subcontractors' information system hard drive using FIPS 140-2 validated software. (See http://csrc.nist.gov/groups/STM/cmvp/validation.html for a complete list of validated cryptographic modules). The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. FIPS 140-2 (or current version) compliant / NIST validated encryption will be used to secure VHA data stored on any portable drives, IT components, disks, CDs / DVDs.

Data must not be physically moved or transmitted from the site without first obtaining prior written approval from the information owner and the data being encrypted prior to said move or transmission.

10. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] All electronic storage media used on non-VA leased or owned IT equipment that is used to store, process, or access VA sensitive information must have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with VA policies and procedures upon the earlier of: (1) completion or termination of the agreement, or (2) disposal or return of the IT equipment by the Requestor or any person acting on behalf of the Requestor.

11. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] VHA reserves the right to allow authorized representatives of VHA and the VA Inspector General to be granted access to premises where the data are kept by the Requestor for the purpose of confirming that the Requestor is in compliance with all requirements associated with this agreement.

12. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] If a Requestor's employee, contractor, or agent becomes aware of the theft, loss or compromise of any device used to transport, access or store VHA information or data, such employee, agent, or contractor must immediately report the incident to his or her supervisor. Should any security incident or event involve VHA data (i.e. the theft, loss, compromise, or destruction of any device used to transport, access, or store VHA data) covered by this agreement, or the incident places VHA data at risk of loss, unauthorized access, misuse or compromise, the Requestor will notify the VHA Point-of-Contact by phone or in writing within one hour of detection. The Requestor will provide details of the security event, the potential risk to VHA data, and the actions that have been or are being taken to remediate the issue. The Requestor will also provide VHA with a written closing action report once the security event or incident has been resolved. VHA will follow this same notification process should a security event occur within the VHA's boundary involving Requestor provided data. Designated points of contact will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirement for responding to security incidents.

13. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] The Requestor's employees, contractors and agents must provide evidence of completion (or initiation) of background investigation prior to granting access to VA or VHA information systems.

14. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] The Requestor's employees, contractors and agents must complete VA's Security and Privacy Awareness training and sign VA's National Rules of Behavior.

15. In the event VHA determines or has a reasonable cause to believe that the Requestor 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 person designated in item number 5 of this Agreement, VHA in its sole discretion may require the Requestor to: (a) promptly investigate and report to /VHA the Requestor's determinations regarding any alleged or actual unauthorized use or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by VHA, submit a formal response to an allegation of unauthorized disclosure; and (d) if requested, return VHA's data files to the Data Owner. If VHA reasonably determines or believes that unauthorized disclosures of Data Owner's data in the possession of Requestor have taken place, the VHA may refuse to release further data to the Requestor for a period of time to be determined by VHA, or may terminate this Agreement.

16. Access to the VHA data shall be restricted to authorized <insert Entity name> employees, contractors, agents and officials who require access to perform their official duties in accordance with the uses of the information as authorized in this Agreement. Such personnel shall be advised of: (1) the confidential nature of the information; (2) safeguards required protecting the information; and (3) the administrative, civil and criminal penalties for noncompliance contained in applicable Federal laws. The Requestor agrees to limit access to, disclosure of and use of all data provided under this Agreement. The Requestor agrees that access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to the Information Owner's data to perform this Agreement.

17. <INSERT ENTITY NAME>, its contractors or agents, will protect the privacy and confidentiality of any individually identifiable information contained in the data consistent with the Privacy Act of 1974, and, to the extent applicable, standards promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 38 U.S.C. 5701(f),and other applicable laws, regulations, and policies. The Requestor may provide data access to appropriate employees, contractors, and other authorized Requestors. Except as may be required in a public health emergency to protect life and health of individuals and populations, and for authorized follow-up activities described herein, the Requestor will not attempt to identify the individuals whose records are contained in the data provided under this agreement or link these data with other data sources for identification purposes.

18. The information provided may not be disclosed or used for any purpose other than as outlined in this Agreement. If the Requestor wishes to use the data and information provided by VHA under this Agreement for any purpose other than those outlined in this Agreement, the Requestor shall make a written request to VHA describing the additional purposes for which it seeks to use the data. If VHA determines that the Requestor's request to use the data and information provided hereunder is acceptable, VHA shall provide the Requestor with written approval of the additional use of the data.

19. The Requestor hereby acknowledges that criminal penalties under § 1106(a) of the Social Security Act (42 U.S.C. § 1306(a)) may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The Requestor further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i)(1)) may apply if it is determined that the Requestor, or any individual employed or affiliated therewith, knowingly and willfully discloses VHA's data. Finally, the Requestor acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the Requestor, 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.

20. Authority for <INSERT PROGRAM OFFICE> to share this data for the purpose indicated is under the HIPAA Privacy Rule, is <INSERT LEGAL CITATION>, under the Privacy Act is <INSERT LEGAL CITATION OR ROUTINE USE FROM THE APPLICABLE PRIVACY ACT SYTEM OF RECORD> and under 38 USC 5701 <INSERT LEGAL CITATION> and 38 USC 7332 <INSERT LEGAL CITATION, IF THIS STATUTE IS APPLICABLE>.

21. <INSERT ENTITY NAME> will ensure that its contractors and agents abide by the terms and conditions of this agreement. The VA or VHA may request verification of compliance.

22. The terms of this Agreement can be changed only by a written modification to 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.

23. This Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, VHA will notify the Requestor to destroy or securely return such data at Requestor's expense using the same procedures stated in the above paragraph of this section.

24. 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.

_____ _____
<INSERT NAME OF ENTITY SIGNER> Date
<INSERT TITLE OF ENTITY SIGNER>
<INSERT PROGRAM OFFICE OF ENTITY>
<INSERT NAME OF ENTITY>

_____ _____
<INSERT NAME OF VHA SIGNER> Date
<INSERT TITLE OF VHA SIGNER>
<INSERT VHA PROGRAM OFFICE>
Veterans Health Administration

Concur/Non-Concur:

_____
<INSERT NAME OF VHA PROGRAM OFFICE ISO>

_____
Signature and Date

Concur/Non-Concur:

_____
<INSERT NAME OF VHA PROGRAM OFFICE PRIVACY OFFICER>

_____
Signature and Date

DATA USE AGREEMENT FOR A LIMITED DATA SET WITH FEDERAL ENTITIES

AGREEMENT FOR DATA EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), <INSERT FACILITY OR PROGRAM OFFICE NAME> AND <INSERT FEDERAL ENTITY NAME>

This Data Use Agreement (Agreement) is entered into as of this ____ day of _____, <INSERT YEAR>, by and between the Department of Veterans Affairs (VA) Veterans Health Administration (VHA), <INSERT FACILITY OR PROGRAM OFFICE NAME> ("Covered Entity"), and <INSERT FEDERAL ENTITY NAME> ("Data Requestor").

WHEREAS, the Covered Entity and the Data Requestor are committed to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations of Title 45 Code of Federal Regulations (CFR) Parts 160 and 164 ("HIPAA Privacy Rule"); and

WHEREAS, the purpose of this Agreement is to satisfy the obligations of the Covered Entity under the HIPAA Privacy Rule, and to ensure the integrity and confidentiality of information disclosed by the Covered Entity to the Data Requestor under this Agreement ("Data") in the form of a Limited Data Set, as defined by the HIPAA Privacy Rule at 45 CFR § 164.514(e); and

WHEREAS, the parties acknowledge and recognize that the Data will not be disclosed to the Data Requestor until the parties execute this Agreement pursuant to 45 CFR § 164.514(e)(4)(ii).

TERMS OF THE AGREEMENT:

1. All provisions of this Agreement that apply to the Data Requestor also apply to any employee, contractor, subcontractor, or other agent of the Data Requestor. The Data Requestor will ensure that its employees, contractors, subcontractors and other agents abide by the terms and conditions of this Agreement. The Covered Entity may request verification of compliance.

2. The Data Requestor will use the Data provided by the Covered Entity under this Agreement to <PROVIDE BRIEF DESCRIPTION OF PROJECT INCLUDING TYPE OF DATA AND HOW IT WILL BE USED>. The specific VHA data-elements being provided to the Data Requestor to support these analyses, and specific data elements to be excluded from the limited data set are listed in Attachment A.

3. For the purpose described in paragraph 2, the Covered Entity will provide the Data Requestor with a Limited Data Set, defined by the HIPAA Privacy Rule as Protected Health Information (PHI) from which the following direct identifiers of the individual have been removed: names, addresses (other than town or city, state, or zip code), phone numbers, fax numbers, e-mail addresses, Social Security Numbers, medical record numbers, health plan numbers, account numbers, certificate and/or license numbers, vehicle identifiers or serial numbers, device identifiers or serial numbers, web universal resource locators, internet protocol address numbers, biometric identifiers, and full-face photographic images and any comparable images. The

Covered Entity and the Data Requestor acknowledge and affirm that a Limited Data Set does not meet the standard for de-identified information as provided by the HIPAA Privacy Rule and is therefore still subject to its requirements.

4. The following named individuals are designated as their agency's Point-of-Contact (POC) for performance of the terms of the Agreement. The Data Requestor agrees to notify the Covered Entity within fifteen (15) calendar days of any change in the named contact.

Point-of-Contact on behalf of <INSERT NAME OF FEDERAL ENTITY>:

<INSERT NAME, PHONE NUMBER AND EMAIL OF FEDERAL ENTITY POC>
Point-of-Contact on behalf of VHA:

<INSERT NAME, PHONE NUMBER AND EMAIL OF VHA POC>

5. The VHA PHI/III provided to <INSERT NAME OF FEDERAL ENTITY> under this Agreement will be covered by the Privacy Act SOR "INSERT SOR NAME>. Although <INSERT NAME OF FEDERAL ENTITY> will own the copy of VHA III/PHI transferred under this Agreement, it agrees not to disclose the VHA III/PHI to any person outside the <INSERT NAME OF FEDERAL ENTITY> except pursuant to a Freedom of Information Act (FOIA) request, as authorized by Federal statute or regulation, <INSERT VHA SORN NAME AND NUMBER> or pursuant to a court order from a court of competent jurisdiction.

6. [TO BE MODIFIED FOR SPECIFIC AGREEMENT] The parties mutually agree that any derivative data, analyses, or findings created from the Data may be retained by the Data Requestor. The Data Requestor agrees to share any findings or outcomes from the analysis of the Data with the Covered Entity at no charge and with no conditions.

7. The Data Requestor agrees that it will not identify, contact, or attempt to identify or contact the individuals whose information is contained in the Data. The Data Requestor also agrees that it will not link or attempt to link the Data with other data sources for such purposes.

8. The Data Requestor shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with the HIPAA Privacy Rule and the common information security laws and regulations, such as the Federal Information Security Management Act (FISMA) and Federal Information Processing Standards (FIPS), to protect VA data confidentiality and to prevent unauthorized access to, or use or disclosure of, the Data.

(a) Data will be <INSERT MEANS OF SECURE TRANSMISSION OF DATA> by the Covered Entity to <INSERT FEDERAL ENTITY POINT OF CONTACT> at <INSERT FEDERAL ENTITY NAME AND ADDRESS>. The Data Requestor agrees to store all data received from the Covered Entity in a physically secure space. Pursuant to the Covered Entity's requirements for information security, the data once received by the Data Requestor will reside on dedicated equipment isolated from all other information systems and will not be comingled with any other data. Access to the Data Requestor site in order to review the data will be made

available to predetermined VA staff for inspection/audit at all times during standard business hours.

(b) The Data Requestor agrees that the Data will be stored in an encrypted partition on the Data Requestor's information system hard drive using Federal Information Processing Standards (FIPS) 140-2 validated software. (See http://csrc.nist.gov/groups/STM/cmvp/validation.html for a complete list of validated cryptographic modules). The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. FIPS 140-2 (or current version) compliant / NIST validated encryption will be used to secure the Covered Entity's data stored on any portable drives, IT components, disks, compact disk (CDs) / optical disk storage (DVDs).

(c) The Data Requestor agrees that the Data provided under the Agreement will not be physically moved or transmitted from the Data Requestor's site without first obtaining prior written approval from the Covered Entity, and without the data being encrypted prior to said move or transmission.

9. The Data Requestor will grant authorized representatives of the Covered Entity, VA OI&T, and the VA Inspector General access to premises where the Data are kept by the Data Requestor for the purpose of confirming that the Data Requestor is in compliance with all security and data use requirements prescribed by this Agreement. The Data Requestor will be notified 60 days in advance of a need to review the premises where the Data are kept. If the review is in response to a data breach by the Data Requestor, the 60-day notice requirement will be waived.

10. If a Data Requestor's employee, contractor, subcontractor, or agent becomes aware of the theft, loss, or compromise of any device used to transport, access, or store the Data, or of the theft, loss, or other unauthorized access, use, or disclosure of any of the Data, such employee, contractor, subcontractor, or agent must immediately report the incident to his or her supervisor. Should any security incident or event involve the Data (i.e. the theft, loss, or other unauthorized access, use, or disclosure of any of the Covered Entity's data or the destruction of any device used to transport, access, or store such data), the Data Requestor will notify the VHA POC along with VA OI&T Information Security Officer (ISO) by phone or in writing within one (1) hour of detection. The VHA POC will contact VHA's Privacy Officer. The Data Requestor will provide details of the security event, the potential risk to the individuals whose information is contained in the Data, and the actions that have been or are being taken by the Data Requestor to remediate the incident or event. The Data Requestor will also provide the Covered Entity with status updates upon request and a written closing action report once the security event or incident has been resolved.

11. Access to the Data shall be restricted to authorized employees, contractors, subcontractor, and agents of the Data Requestor requiring access to perform their official duties as authorized by this Agreement. The Data Requestor shall inform such personnel of: (1) the confidential nature of the information; (2) safeguards required to protect the information; (3) the administrative, civil, and criminal penalties for noncompliance contained in applicable Federal laws; and (4) that their actions can lead to the immediate termination of this Agreement by the Covered Entity. The Data Requestor agrees to limit access to, disclosure of, and use of Data

provided under this Agreement to the minimum number of individuals needing access to the data provided by the Covered Entity to perform their duties as authorized by this Agreement.

12. In the event that the Covered Entity suspects or determines that the Data Requestor accessed, used, or disclosed any part of the Data other than as authorized by this Agreement or other written authorization from the person designated in Paragraph 4 of this Agreement, the Covered Entity in its sole discretion may require the Data Requestor to:

(a) Promptly investigate and report to the Covered Entity the Data Requestor's determinations regarding any alleged or actual unauthorized use or disclosure;

(b) Promptly resolve any problems identified by the investigation;

(c) Submit a formal response to an allegation of unauthorized disclosure; and

(d) Return the Data to the Covered Entity.

Further, if the Covered Entity suspects or determines that the Data in the possession of the Data Requestor has been accessed, used, or disclosed other than as authorized by this Agreement, the Covered Entity in its sole discretion may suspend further releases of the data to the Data Requestor or may terminate this Agreement in its entirety.

13. The Data Requestor hereby acknowledges that criminal penalties under § 1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fi imprisonment not exceeding 5 years, or both, may apply to disclosures of information covered by §1106 and not authorized by regulation or by Federal law. Finally, the Data Requestor acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the Data Requestor, or any individual employed or affiliated therewith, embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys, or disposes of any Data provided under this Agreement.

14. This Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Once this Agreement is terminated, the Data Requestor has no legal authority to access, use, disclose, or retain the Data. Upon termination of the Agreement, the Data Requestor must, at its own expense, destroy or return the limited data set in accordance with Paragraph 9.

15. All questions of interpretation or compliance with the terms of this Agreement should be referred to the Covered Entity's official named in Paragraph 4 (or his or her successor).

16. Authority for the Covered Entity to disclose this data to the Data Requestor for the purpose indicated is provided by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, 45 CFR 164.514(e). The Privacy Act and 38 USC §§ 5701 and 7332 do not apply, as a Limited Data Set is not considered individually identifiable under these statutes.

17. This Agreement supersedes any and all previous agreements related to this project. The terms of this Agreement can only be changed by written modification to this Agreement or adoption of a new agreement in place of this Agreement.

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 of the terms specified herein.

_____ _____
<INSERT NAME OF FEDERAL ENTITY SIGNER> Date
<INSERT TITLE OF FEDERAL ENTITY SIGNER>
<INSERT PROGRAM OFFICE OF FEDERAL ENTITY>
<INSERT NAME OF FEDERAL ENTITY>

_____ _____
<INSERT NAME OF VHA SIGNER> Date
<INSERT TITLE OF VHA SIGNER>
<INSERT VHA PROGRAM OFFICE>
Veterans Health Administration

Concur/Non-Concur:

_____
<INSERT NAME OF VHA PROGRAM OFFICE ISO>

_____
Signature and Date

Concur/Non-Concur:

_____
<INSERT NAME OF VHA PROGRAM OFFICE PRIVACY OFFICER>

_____
Signature and Date

DATA ELEMENTS TO BE PROVIDED TO <INSERT NON-FEDERAL ENTITY NAME> FOR < PROVIDE BRIEF DESCRIPTION OF PROJECT>

The following identifiers **must be removed** from health information if the data are to qualify as a limited data set:

1. Names
2. Postal address information, other than town or city, state and Zip Code
3. Telephone Numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web universal resource locators (URLs)
14. Internet protocol (IP) address numbers
15. Biometric identifiers, including fingerprints and voiceprints
16. Full-face photographic images and any comparable images

Note: The above data elements apply to the individual, the individual's relatives, employer, and household members.

<INSERT LIST OF DATA ELEMENTS TO BE PROVIDED>

DATA USE AGREEMENT FOR A LIMITED DATA SET WITH A NON-FEDERAL ENTITY

AGREEMENT FOR DATA EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), <INSERT FACILITY OR PROGRAM OFFICE NAME> AND <INSERT NON-FEDERAL ENTITY NAME>

This Data Use Agreement (Agreement) is entered into as of this ____ day of _____, <INSERT YEAR>, by and between the Department of Veterans Affairs (VA) Veterans Health Administration (VHA), <INSERT FACILITY OR PROGRAM OFFICE NAME ("Covered Entity"), and <INSERT NON-FEDERAL ENTITY NAME> ("Data Requestor").
WHEREAS, the Covered Entity and the Data Requestor are committed to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations of Title 45 Code of Federal Regulations (CFR) Parts 160 and 164 ("HIPAA Privacy Rule"); and

WHEREAS, the purpose of this Agreement is to satisfy the obligations of the Covered Entity under the HIPAA Privacy Rule, and to ensure the integrity and confidentiality of information disclosed by the Covered Entity to the Data Requestor under this Agreement ("Data") in the form of a Limited Data Set, as defined by the HIPAA Privacy Rule at 45 CFR § 164.514(e); and

WHEREAS, the parties acknowledge and recognize that the Data will not be disclosed to the Data Requestor until the parties execute this Agreement pursuant to45 CFR § 164.514(e)(4)(ii).

TERMS OF THE AGREEMENT:

1. All provisions of this Agreement that apply to the Data Requestor also apply to any employee, contractor, subcontractor, or other agent of the Data Requestor. The Data Requestor will ensure that its employees, contractors, subcontractors and other agents abide by the terms and conditions of this Agreement. The Covered Entity may request verification of compliance.

2. The Data Requestor will use the Data provided by the Covered Entity under this Agreement to <PROVIDE BRIEF DESCRIPTION OF PROJECT INCLUDING TYPE OF DATA AND HOW IT WILL BE USED>. The specific VHA data-elements being provided to the Data Requestor to support these analyses, and specific data elements to be excluded from the limited data set are listed in Attachment A.

3. For the purpose described in paragraph 2, the Covered Entity will provide the Data Requestor with a Limited Data Set, defined by the HIPAA Privacy Rule as Protected Health Information from which the following direct identifiers of the Veteran have been removed: names, addresses (other than town or city, state, or zip code), phone numbers, fax numbers, e-mail addresses, Social Security Numbers, medical record numbers, health plan numbers, account numbers, certificate and/or license numbers, vehicle identifiers or serial numbers, device identifiers or serial numbers, web universal resource locators, internet protocol address numbers, biometric identifiers, and full-face photographic images and any comparable images. The Covered Entity

and the Data Requestor acknowledge and affirm that a Limited Data Set does not meet the standard for de-identified information as provided by the HIPAA Privacy Rule and is therefore still subject to its requirements.

4. The following named individuals are designated as their agency's Point-of-Contact (POC) for performance of the terms of the Agreement. The Data Requestor agrees to notify the Covered Entity within fifteen (15) calendar days of any change in the named contact.

Point-of-Contact on behalf of <INSERT NAME OF NON-FEDERAL ENTITY>:

<INSERT NAME, PHONE NUMBER AND EMAIL OF NON-FEDERAL ENTITY POC>
Point-of-Contact on behalf of VHA:

<INSERT NAME, PHONE NUMBER AND EMAIL OF VHA POC>

5. <SELECT ONE > VHA retains all ownership rights and responsibilities to the original and derivative data file(s) provided to the Requestor under this Agreement. <OR> VHA will retain ownership of the original data and <INSERT ENTITY NAME> will receive a copy. Data transferred under this agreement becomes the property of <INSERT ENTITY NAME>.

The Data Requestor has no rights in the Data other than to use the Data for the purpose described in paragraph 2 for the duration of this Agreement and will not use the Data for any purpose other than as outlined in this Agreement, unless such use is required by law. If the Data Requestor wishes to use the Data for any purpose other than as specified in this Agreement, the Data Requestor shall first provide a written request to the Covered Entity describing the additional purpose for which it seeks to use the data. The Data Requestor may not use the information for the additional purpose unless the Covered Entity provides the Data Requestor with written approval of the additional use.

6. [TO BE MODIFIED FOR SPECIFIC AGREEMENT] The parties mutually agree that any derivative data, analyses, or findings created from the Data may be retained by the Data Requestor. The Data Requestor agrees to share any findings or outcomes from the analysis of the Data with the Covered Entity at no charge and with no conditions.

7. The Data Requestor agrees that it will not identify, contact, or attempt to identify or contact the individuals whose information is contained in the Data. The Data Requestor also agrees that it will not link or attempt to link the Data with other data sources for such purposes.

8. The Data provided may not be used or disclosed by the Data Requestor for any purpose other than as outlined in this Agreement or as otherwise required by law. If the Data Requestor wishes to use the Data provided by the Covered Entity under this Agreement for any purpose other than those outlined in this Agreement, the Data Requestor shall make a written request to the Covered Entity describing the additional purposes for which it seeks to use the data. If the Covered Entity determines that the Data Requestor's request to use the data and information provided hereunder is acceptable, the Covered Entity shall provide the Data Requestor with written approval of the additional use of the data.

Data will <INSERT MEANS OF SECURE TRANSMISSION OF DATA> by the Covered Entity to <INSERT NON-FEDERAL ENTITY POINT OF CONTACT> at <INSERT NON-FEDERAL ENTITY NAME AND ADDRESS>.

9. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA], the requesting entity must provide the following information:

<DESCRIBE WHERE THE DATA WILL BE STORED:>
<DESCRIBE MEANS OF ACCESSING DATA AND ACCESS AUDIT METHODS:>
<PROVIDE DATE OF PROJECT COMPLETION:>

10. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] Except as VHA shall authorize in writing, <insert requesting entity name>, its contractors and agents, 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 or entity outside the Requestor and its team of subcontractors performing the Project. Without limitation to any other provision of this Agreement, the Requestor agrees not to disclose, display or otherwise make available any company proprietary information to any third party, in any form, except to public health officials in connection with the purposes established herein or as otherwise required under the Freedom of Information Act (FOIA), or other Federal law. VHA will clearly indicate in writing any information that is considered to be trade secret or confidential business information.

11. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] <INSERT ENTITY NAME>, its contractors and agents, shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with VA Handbook 6500, to protect VA data confidentiality and to prevent unauthorized access to the data provided by VHA. If co-mingling must be allowed to meet the requirements of the business/research need, the Requestor must ensure that VHA's information is returned to the VHA or destroyed in accordance with VA's sanitization requirements. VHA reserves the right to conduct onsite inspections of Requestor's IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA requirements.

All VHA data and derivative data must be stored in an encrypted partition on the Requestor's or its contractors/subcontractors information system hard drive using FIPS 140-2 validated software. (See http://csrc.nist.gov/groups/STM/cmvp/validation.html for a complete list of validated cryptographic modules). The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. FIPS 140-2 (or current version) compliant / NIST validated encryption will be used to secure VHA data stored on any portable drives, IT components, disks, CDs / DVDs. Data must not be physically moved or transmitted from the site without first obtaining prior written approval from the information owner and the data being encrypted prior to said move or transmission.

12. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] All electronic storage media used on non-VA leased or owned IT equipment that is used to store, process, or access VA sensitive information must have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with VA policies and procedures upon the earlier of: (1) completion or

termination of the agreement, or (2) disposal or return of the IT equipment by the Requestor or any person acting on behalf of the Requestor.

13. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] VHA reserves the right to allow authorized representatives of VHA and VA's Inspector General to be granted access to premises where the data are kept by the Requestor for the purpose of confirming that the Requestor is in compliance with all requirements associated with this agreement.

14. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] If a Requestor's employee, contractor, or agent becomes aware of the theft, loss or compromise of any device used to transport, access or store VHA information or data, such employee, agent, or contractor must immediately report the incident to his or her supervisor. Should any security incident or event involve VHA data (i.e. the theft, loss, compromise, or destruction of any device used to transport, access, or store VHA data) covered by this agreement, or the incident places VHA data at risk of loss, unauthorized access, misuse or compromise, the Requestor will notify the VHA Point-of-Contact by phone or in writing within one hour of detection. The Requestor will provide details of the security event, the potential risk to VHA data, and the actions that have been or are being taken to remediate the issue. The Requestor will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within VA's boundary involving Requestor provided data. Designated points of contact will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirement for responding to security incidents.

15. [INSERT IF VHA RETAINS OWNERSHIP OF THE DATA] The Requestor's employees, contractors and agents must provide evidence of completion (or initiation) of background investigation prior to granting access to VA or VHA information systems.

16. [INSERT IF THE VHA RETAINS OWNERSHIP OF THE DATA] The Requestor's employees, contractors and agents must complete VA's Security and Privacy Awareness training and sign VA's National Rules of Behavior.

17. The Data Requestor shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with the HIPAA Privacy Rule, to protect VA data confidentiality and to prevent unauthorized access to, or use or disclosure of, the Data.

18. The Data Requestor will grant authorized representatives of the Covered Entity, VA OI&T, and the VA Inspector General access to premises where the Data are kept by the Data Requestor for the purpose of confirming that the Data Requestor is in compliance with all security and data use requirements prescribed by this Agreement. The Data Requestor will be notified 60 days in advance of a need to review the premises where the Data are kept. If the review is in response to a data breach by the Data Requestor, the 60-day notice requirement will be waived.

19. Access to the Data shall be restricted to authorized employees, contractors, subcontractor, and agents of the Data Requestor requiring access to perform their official duties as authorized by this Agreement. The Data Requestor shall inform such personnel of: (1) the confidential

nature of the information; (2) safeguards required to protect the information; (3) the administrative, civil, and criminal penalties for noncompliance contained in applicable Federal laws; and (4) that their actions can lead to the immediate termination of this Agreement by the Covered Entity. The Data Requestor agrees to limit access to, disclosure of, and use of Data provided under this Agreement to the minimum number of individuals needing access to the Covered Entity's data to perform their duties as authorized by this Agreement.

20. In the event that the Covered Entity suspects or determines that the Data Requestor accessed, used, or disclosed any part of the Data other than as authorized by this Agreement or other written authorization from the person designated in Paragraph 4 of this Agreement, the Covered Entity in its sole discretion may require the Data Requestor to:
(a) promptly investigate and report to the Covered Entity the Data Requestor's determinations regarding any alleged or actual unauthorized use or disclosure;
(b) promptly resolve any problems identified by the investigation;
(c) submit a formal response to an allegation of unauthorized disclosure; and
(d) return the Data to the Covered Entity.

Further, if the Covered Entity suspects or determines that the Data in the possession of the Data Requestor has been accessed, used, or disclosed other than as authorized by this Agreement, the Covered Entity in its sole discretion may suspend further releases of the data to the Data Requestor or may terminate this Agreement in its entirety.

21. The Data Requestor 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 covered by § 1106 and not authorized by regulation or by Federal law. Finally, the Data Requestor acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the Data Requestor, or any individual employed or affiliated therewith, embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys, or disposes of any Data provided under this Agreement.

22. This Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Once this Agreement is terminated, the Data Requestor has no legal authority to access, use, disclose, or retain the Data. Upon termination of the Agreement, the Data Requestor must, at its own expense, destroy or return the limited data set in accordance with paragraph 9.

23. All questions of interpretation or compliance with the terms of this Agreement should be referred to the Covered Entity's official named in Paragraph 7 (or his or her successor).

24. Authority for the Covered Entity to disclose this data to the Data Requestor for the purpose indicated is provided by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, 45 CFR 164.514(e). The Privacy Act and 38 USC §§ 5701 and 7332 do not apply, as a Limited Data Set is not considered individually identifiable under these statutes.

25. This Agreement supersedes any and all previous agreements related to this project. The terms of this Agreement can only be changed by written modification to this Agreement or adoption of a new agreement in place of this Agreement.

26. 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 of the terms specified herein.

_____ _____
<INSERT NAME OF ENTITY SIGNER> Date
<INSERT TITLE OF ENTITY SIGNER>
<INSERT PROGRAM OFFICE OF ENTITY>
<INSERT NAME OF ENTITY>

_____ _____
<INSERT NAME OF VHA SIGNER> Date
<INSERT TITLE OF VHA SIGNER>
<INSERT VHA PROGRAM OFFICE>
Veterans Health Administration

Concur/Non-Concur:

_____
<INSERT NAME OF VHA PROGRAM OFFICE ISO>

_____
Signature and Date

Concur/Non-Concur:

_____
<INSERT NAME OF VHA PROGRAM OFFICE PRIVACY OFFICER>

_____
Signature and Date

DATA ELEMENTS TO BE PROVIDED TO <INSERT NON-FEDERAL ENTITY NAME> FOR < PROVIDE BRIEF DESCRIPTION OF PROJECT>

The following identifiers **must be removed** from health information if the data are to qualify as a limited data set:

1. Names
2. Postal address information, other than town or city, state and Zip Code
3. Telephone Numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web universal resource locators (URLs)
14. Internet protocol (IP) address numbers
15. Biometric identifiers, including fingerprints and voiceprints
16. Full-face photographic images and any comparable images

Note: The above data elements apply to the individual, the individual's relatives, employer, and household members.

<INSERT LIST OF DATA ELEMENTS TO BE PROVIDED>