**DATA USE AGREEMENT WITH FEDERAL ENTITIES**

**FOR DATA SHARING BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS (VA), VETERANS HEALTH ADMINISTRATION (VHA) AND <INSERT NAME OF FEDERAL ENTITY>**

1. **DEFINITIONS.**
   1. Data Ownership is defined as statutory or operational authority over specified information, including the responsibility for establishing the criteria for its creation, collection, maintenance, processing, dissemination, or disposal.
   2. Derived Data are data elements derived from other data elements using a mathematical, logical, or other type of transformation, e.g., restructuring, extracting, analyzing, aggregation.
   3. Disclosure is the release, transfer, provision of access to, or divulging in any other manner PII 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.
   4. Federal Entity is defined as a federal agency, created by Congress through statutes that define the scope of an agency's authority.
   5. Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual’s identity, such as their name, social security number, or biometric records alone or combined with other personal or identifying information which is linked or linkable to a specific individual.
   6. Protected Health Information (PHI) is defined as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as the Veterans Health Administration (VHA).
   7. Recipient under this Agreement is defined as the party that is receiving VHA individually identifiable information, which may consist of Protected Health Information.
   8. Security Rule means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C, effective April 20, 2005.
2. **PURPOSE/DATA ELEMENTS**. This Agreement establishes the terms and conditions under which the Minneapolis VA Health Care System (MVAHCS) will provide, and <INSERT FEDERAL ENTITY NAME> (Recipient) will use VHA data.

Description of the purpose of the data request: <INSERT DESCRIPTION OF THE PURPOSE OF THE DATA>

Description of the data requested: <DESCRIBE WHAT DATA IS REQUESTED. INDICATE IF DATA WILL BECOME PART OF A PRIVACY ACT SYSTEM OF RECORDS AND IF SO, PROVIDE TITLE AND NUMBER>

1. **DESCRIPTION OF DATA TRANSFER.** The following secure means of data transfer will be used: <INSERT DESCRIPTION OF THE SECURE MEANS OF DATA TRANSFER BETWEEN VHA AND RECIPIENT>
2. **POINTS OF CONTACT.**  The following named individuals are designated as their agency’s Point of Contact (POC) for performance of the terms of this DUA. The Recipient agrees to notify the Covered Entity within fifteen (15) calendar days of any change in the named contact.

POC/Federal Entity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

POC/VHA: **Associate Chief of Staff, Research Service, MVAHCS**

1. **DATA OWNERSHIP AND USE.** VHA will retain ownership of the original data. Although <INSERT NAME OF FEDERAL ENTITY> will own the copy of VHA Data transferred under this Agreement, the <Federal Entity Name> agrees not to disclose the VHA Data to any person outside of the <Federal Entity Name> except pursuant to a Freedom of Information Act (FOIA) request, as authorized by Federal statute or regulation, or pursuant to a court order from a court of competent jurisdiction. The parties mutually agree that any derived data, analyses, or findings created from the Data may be retained by the Recipient indefinitely.

<INSERT NAME OF FEDERAL ENTITY> agrees to use the VHA data consistent with the purpose outlined in this Agreement. <INSERT THE FOLLOWING IF DATA WILL BE PLACED IN A SYSTEM OF RECORDS ONCE RECEIVED BY THE RECIPIENT: <Federal Entity Name> agrees to only disclose and use the VHA Data consistent with the Privacy Act System of Records Notice (SORN) <INSERT TITLE AND NUMBER>.

1. **ACCESS TO THE DATA.** Access to the Data shall be restricted to authorized employees, contractors, subcontractors, and agents of the Recipient requiring access to perform their official duties, as authorized by this Agreement. The Recipient 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 VHA.
2. **DATA ASSURANCE AND PROTECTION.**  <INSERT RECIPIENT NAME>, its contractors and agents, shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with VHA Handbook 6500, to protect VHA data confidentiality and to prevent unauthorized access to the data provided by VHA. VHA reserves the right to conduct onsite inspections of Recipient’s IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures comply with VHA requirements.

All VHA data must be stored in an encrypted partition on the Recipient’s or its contractors’/subcontractors’ Information System (using validated encryption to secure VHA data stored on any Hard Drives, Portable drives, IT components, Non Volatile Memory, Disks, CDs or DVDs) using FIPS 140-2 or 140-3 validated software with a current certificate). See National Institute of Standards and Technology (NIST) 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.

VHA reserves the right to allow authorized representatives of VHA and the VHA Inspector General to be granted access to premises where the data are kept by the Recipient to confirm that the Recipient is following all requirements associated with this agreement.

The Recipient’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, if applicable.

1. **REPORTING.** If a Recipient’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 VHA’s data or the destruction of any device used to transport, access, or store such data), the Recipient will notify the VHA POC by phone or in writing within one (1) hour of detection. The VHA POC will contact the VA OI&T Information Systems Security Officer (ISSO) and VHA’s Privacy Officer. The Recipient 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 Recipient to remediate the incident or event. The Recipient will also provide VHA with status updates upon request and a written closing action report once the security event or incident has been resolved.
2. **AUTHORITIES.** Authority for MVAHCS Research to share this data for the purpose indicated under the HIPAA Privacy Rule, at 45 CFR § 164.514(e). Under the Privacy Act: Approval of use of the Data for research by the Minneapolis VA Health Care System’s IRB of record, 38 U.S.C. 5701(b)(3) and 38 U.S.C. 7332.
3. **TERMINATION.** This Agreement may be terminated by either party, at any time, and for cause upon 30 days written notice from the terminating party to the other party. This Agreement may only be terminated without cause by mutual agreement of the Parties.
4. **MISCELLANEOUS.** 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.
5. **SIGNATORIES**. 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 MVAHCS INVESTIGATOR>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<INSERT NAME OF RECIPIENT>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<INSERT NAME OF RECIPIENT INSTITUTION>

* 1. 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 terms specified herein.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<INSERT SIGNATURE OF MVAHCS INVESTIGATOR> Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<INSERT SIGNATURE OF RECIPIENT> Date

Concur Non-Concur

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

VA Information System Security Officer (ISSO) Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

VHA Research Privacy Officer Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Associate Chief of Staff/Research (or designee) Date