**DATA USE AGREEMENT WITH NON-FEDERAL ENTITIES**

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

1. **Purpose of the Agreement.** This Agreement establishes the terms and conditions under which the VHA Minneapolis VA Health Care System (MVAHCS) will provide, and <INSERT RECIPIENT NAME> will use, VHA data. <INSERT DESCRIPTION OF THE RESEARCH PURPOSE OF THE DATA AND WHAT DATA IS REQUESTED.>
2. **DATA ELEMENTS**.  The requesting entity must provide the following information:

2.1         Description of dataset: <INSERT DETAILED DESCRIPTION OF THE DATA SET, INCLUDING THAT IT IS DE-IDENTIFIED>

2.2        Name of Recipient's research protocol: <INSERT NAME OF THE RESEARCH PROTOCOL>

2.3        VHA data will not be transferred until a copy of the authority to perform the activities defined above is received.

1. **DESCRIPTION OF DATA TRANSFER AND STORAGE.** The requesting entity must provide the following information:
   1. Data transfer from VHA and Recipient: <DESCRIBE HOW DATA WILL BE SECURELY TRANSFERRED BETWEEN VHA AND RECIPIENT>
   2. Data storage: <DESCRIBE WHERE THE DATA WILL BE STORED>
   3. Data access and audit methods: <DESCRIBE MEANS OF ACCESSING DATA AND ACCESS AUDIT METHODS>
   4. Project will be completed by: <PROVIDE ANTICIPATED DATE OF PROJECT COMPLETION>
   5. Date of expiration of this DUA: <PROVIDE DUA EXPIRATION DATE>
   6. At the expiration of this agreement: <DESCRIBE WHAT WILL HAPPEN TO VHA DATA AT THE EXPIRATION OF THIS AGREEMENT>
   7. For the purpose of this DUA, VHA data will not be disclosed within the VHA or outside the VHA other than as permitted by this agreement and permitted within the protocol for which the data have been requested. A separate copy of VHA data may not be created by the Recipient in any way. Data cannot be physically moved or transmitted from the Recipient without first obtaining prior written approval from the information owner and the data being encrypted prior to said move or transmission.
   8. For the purpose of this DUA, any VHA data must be used, stored, and secured according to the requirements of the VHA series 1200 Handbooks, other applicable VHA and VHA requirements, and as described in the approved research protocol.
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/Non-Federal Entity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

1. **DATA OWNERSHIP, USE, DISCLOSURE.** VHA retains all ownership rights and responsibilities to the original data file(s) provided to the Recipient under this Agreement. Recipient may use original data and any data determined to be derived data. Derived data will become the property of the Recipient. Except as VHA shall authorize in writing, <INSERT REQUESTING ENTITY’S NAME> its contractors and agents, shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the VHA’s original data covered by this Agreement to any person or entity outside the Recipient and its team of subcontractors performing the Project. Without limitation to any other provision of this Agreement, the Recipient 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 considered to be trade secret or confidential business information.

Recipient shall use appropriate safeguards to protect the information from misuse, or inappropriate disclosure and to prevent any use or disclosure of the information other than as provided in this DUA, or as otherwise acquired by law or regulation.

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 agrees that access to the data covered by this agreement shall be limited to the minimum number of individuals who need access to VHA data to perform their duties relative to 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.

Recipient will provide a listing of all individuals who will have access to, or use the data. In addition, the VHA POC will maintain the list of names and descriptions of all entities to which the data has been disclosed.

Recipient agrees to maintain the confidentiality of all information contained in any Record that you access. Recipient will make reasonable effort to access only the minimum number or amount of records necessary for data analysis, and to use and/or disclose no more than the minimum amount of identifiable information, if applicable, in each record to accomplish the stated purpose. Additionally, Recipient agrees to make no effort to re-identify any data that are de-identified, or to attempt to ‘unscramble’ scrambled social security numbers (SSNs), if applicable, to reveal Real SSNs.

Adherence to VA’s ethical principles for access to and use of Veterans’ health data remains a component of the data release or disclosure. Questions about whether the ethical principles for data access and use are being met should be referred to the VA National Center for Ethics in Health Care (10E1E).

1. **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. **DATA DISPOSITION.** Recipients shall, at the expiration of this DUA (as noted in Section 3 above) return all data to VHA or destroy all data received. If the data is to be destroyed, the Recipient must certify that all data received from VHA under the scope of this agreement has been destroyed.
2. **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 non-compliance occur with applicable VA and VHA requirements, other applicable Federal regulations, or the research protocol as approved by the Institutional Review Board (IRB) and R&D Committee(s), VHA employees must take appropriate action. All such instances of non-compliance must be reported according to the facility’s policies and procedures and by VHA requirements. Such non-compliance must be reported to the investigator or VA employee who allowed the data to be transferred. If data are from a VA data repository, the data repository administrator or owner must notify the IRB(s) having oversight responsibilities for the repository in accordance with the repository’s procedures.

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, compromise of the integrity of the data, or the destruction of any device used to transport, access, or store such data), the Recipient will also notify the VHA POC by phone or in writing within one (1) hour of detection. 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.

The VHA POC will immediately report the incident to the VA Investigator’s facility’s OI&T Information Systems Security Officer (ISSO) and VHA’s Privacy Officer (PO), the investigator’s supervisor, and others as stipulated in VA, VHA, and local facility’s requirements. If must be reported to the Privacy Officer and ISO of the facility from which the data were transferred, in addition to the investigator or VA employee who allowed the transfer of the data. If data are from a VA research data repository, the research data repository administrator must also notify the IRB having oversight responsibilities for the repository in accordance with the research data repository’s procedures.

1. **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.
2. **TERMINATION.** 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. Upon such notice, VHA will require the Recipient to destroy or securely return the original data at Recipient’s expense.
3. **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.
4. **SIGNATORIES**.
   1. On behalf of both parties, the undersigned individuals are acknowledging the agreement as outlined and agree to all terms specified herein.

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

<INSERT NAME OF VHA 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 VHA 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