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), for the purpose of <SELECT ONE – public health or research>; 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 for <SELECT ONE – public health or research>, 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. VHA will retain ownership of the original data and <INSERT ENTITY NAME> will receive a copy. The copy of the data transferred under this agreement becomes the property of <INSERT ENTITY NAME> subject to the terms of this Agreement.

6. 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.

7. 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.

8. 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 ENTITY NAME>, its contractors and agents, shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with the HIPAA Security and Privacy Rules, to protect VHA data confidentiality and to prevent unauthorized access to, use or disclosure of the data provided by VHA. <INSERT ENTITY NAME> will ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information.

10. 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.

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 Covered Entity's data to perform their duties as authorized by this Agreement.

12. 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.

13. 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 receipt of the Notice of Termination of the Agreement, the Data Requestor within 15 days must, at its own expense, destroy or return the limited data set. The Media Destruction guidance can be found at the NSA site: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml. If the Data Requestor chooses to destroy the Data, a Certificate of Destruction signed by the Security point of contact (POC) and the agency approving official must be provided to the VHA POC listed in Paragraph 4.

14. 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).

15. 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.

16. 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.

17. 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

ATTACHMENT A

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>