

## **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 SYSTEM 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>  
<INSERT TITLE OF ENTITY SIGNER>  
<INSERT PROGRAM OFFICE OF ENTITY>  
<INSERT NAME OF ENTITY>

---

Date

---

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

---

Date

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