

DATA TRANSFER AGREEMENT

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

Purpose:

This Agreement establishes the terms and conditions under which the <insert name> will provide, and <insert name> will use the data to <be very specific in why data is being shared, and state the method of transfer and how that will be accomplished>
Any other uses will be subject to prior approval by the <transferring agency Director>.

TERMS OF THE AGREEMENT:

1. This Agreement is by and between the <INSERT NAME> and <INSERT NAME> (Owner), a component of the U.S. Department of Veterans Affairs.
2. This data transfer agreement covers the transfer and use of data by the <INSERT NAME> and <INSERT NAME>, for the project specified in this agreement. This Agreement supersedes any and all previous data.
3. 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.
4. The <transferring agency> retains all ownership rights to the data file(s) and VHA retains all ownership rights to the VHA data file(s) provided to the you under this Agreement.
5. The <Insert user name> will be designed as custodians of the VA data for the <user name> and will be responsible for complying with all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use and disclosure of the Owner's data provided under this agreement. The User agrees to notify the Owner within fifteen (15) days of any change of custodianship.

Technical Representative for <Transferring Agency>

Insert Name and Phone Number

Custodian for <User Agency>

Insert Name and Phone Number

6. The following named individuals are designated as their agencies' Points of Contact for performance of the terms of the Agreement.

Point-of-contact on behalf of <Transferring Agency>

Insert Name and Phone Number

Point-of-contact on behalf of <User Agency>

Insert Name and Phone Number

7. Except as VHA shall authorize in writing, the User 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 outside the **<User Agency>**. The User agrees that, access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to Owner's data to perform this Agreement.

8. The parties mutually agree that any derivative data or file(s) that is created from the original data may be retained by the User until the project specified in this DTA has been completed. The use of the data will be for the time period covered by the **<Insert MOU or Proposal Name> (Insert Time Frame)**. At the end of this period **<insert terms of agreement for return or data, destruction of data or renewing agreement>** you are authorized to keep the data on your system in a secure encrypted partition in accordance with FIPS 140-2 validation.

9. The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the Owner will notify the User to destroy or return such data at Users expense using the same procedures stated in the above paragraph of this section.

10. The User will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the Owner's data and to prevent unauthorized use or access to it. VA sensitive information must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be validated by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140 (See <http://csrc.nist.gov/cryptval/140-1/1401val.htm> for a complete list of validated cryptographic modules). Only approved encryption solutions using validated modules may be used when protecting data during transmission. Additional security controls are required to guard VA sensitive information stored on computers used outside VA facilities. All VA data must be stored in an encrypted partition on the hard drive and must be encrypted with FIPS 140 validated software. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. Further, the User agrees that the data must not be physically moved or transmitted in any way from the site indicated in item number 5 without first being encrypted and obtaining prior written approval from the data owner.

a. If the data user becomes aware of the theft, loss or compromise of any device used to transport, access or store VA information, or of the theft, loss or compromise of any VA data, the user must immediately report the incident to his or her supervisor. That supervisor must within one hour inform the **<Fill in VA Information Security Officer and the Director names and phone numbers>**. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements for responding to security incidents.

11. The authorized representatives of VHA and the Inspector General will be granted access to premises where the data are kept by the User for the purpose of confirming that the User is in compliance with the security requirements.

12. No findings, listing, or information derived from the data, with or without identifiers, may be released if such findings, listing, or information contain any combination of data elements that might allow the deduction of a veteran without first obtaining written authorization from the

appropriate System Manager or the person designated in item number 18 of this Agreement. Examples of such data elements include but are not limited to social security number, geographic indicator, age, sex, diagnosis, procedure, admission/discharge date(s), or date of death. The Owner shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from its files provided under this Agreement identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual. The Owners' review of the findings is for the sole purpose of assuring that data confidentiality is maintained and that individuals cannot be identified from the findings. The Owner agrees to make this determination about approval and to notify the User within two weeks after receipt of findings. The Owner may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual.

13. The User may not reuse the Owner's original or work file(s) for any other purpose.

14. In the event that the Owner determines or has a reasonable cause to believe that the User 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 appropriate System Manager or the person designated in item number 18 of this Agreement, the Owner in its sole discretion may require the User to: (a) promptly investigate and report to the Owner the User's determinations regarding any alleged or actual unauthorized use or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by the Owner, submit a formal response to an allegation of unauthorized disclosure; and (d) if requested, return the Owner's data files to the Owner. If the Owner reasonably determines or believes that unauthorized disclosures of Owner's data in the possession of User have taken place, the Owner may refuse to release further data to the User for a period of time to be determined by the Owner, or may terminate this Agreement.

15. The User 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 that are covered by §1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. §552a(i)(1)) may apply if it is determined that the User, or any individual employed or affiliated therewith, knowingly and willfully discloses Owner's data. Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than \$5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. §641 if it is determined that the User, 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.

16. All questions of interpretation or compliance with the terms of this Agreement should be referred to the VHA official name in item 18 (or his or her successor).

17. Authority for VHA to share this data for the purpose indicated is under the HIPAA Privacy Rule, is 45 CFR 164.512(k)(6)(ii), under the Privacy Act is routine use 30 in VA system of records, 121VA19, entitled National Patient Databases-VA and under 38 USC 5701(b)(3) and (e).

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 the terms specified herein.

Transferring Responsible Official Date
Organization Transferring Data

User Responsible Official Date
Organization Receiving Data

Concur/Non-Concur:

Transferring Agency ISO Name Date
Organization