AGREEMENT FOR THE EXCHANGE OF VA DATA

WITHIN THE VA PORTLAND HEALTH CARE SYSTEM

BETWEEN  <INSERT REPOSITORY DIRECTORS NAME (REPOSITORY IRB#)> AND <INSERT RECIPIENT NAME (IRB#)>

Purpose:

This Agreement establishes the terms and conditions under which the VA Portland Health Care System (VAPORHCS), <INSERT REPOSITORY DIRECTOR NAME> will provide, and <INSERT RECIPIENT NAME> will use <ADD WHICHEVER STATEMENT APPLIES, OR CREATE ONE TO FIT THE SITUATION: VHA individually identified information/VHA protected health information (VHA III/PHI); de-identified data; coded data, etc>.

References and Authorities:

* The Privacy Act of 1974, 5 U.S.C. § 552a, as amended
* The Technology Transfer Act of 1986
* The Health Insurance Portability and Accountability Act of 1994, Pub. L. 104-191
* Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information (HIPAA Privacy and HIPAA Security Rules), 45 C. F. R. §§ 160, 164.
* Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001
* The HITECH Act, Pub. L. 109-1
* 38 U.S.C. 5701(b) (3), use of names and/or addresses

Terms of this Agreement:

1. This Agreement is by and between the VAPORHCS, <INSERT NAME OF REPOSITORY DIRECTOR> (hereinafter referred to as the “Sender”) and <INSERT RECIPIENT NAME> (hereinafter referred to as the “Recipient”).
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 pre-empts 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. The Sender will transfer to the Recipient, through <DESCRIBE HOW THE DATA WILL BE TRANSFERRED, (I.E., ELECTRONICALLY USING EMAIL AND PKI ENCRYPTION, CD/DVD WITH ENCRYPTION, FEDEX/UPS WITH TRACKING, ETC. AND INCLUDE THE FOLLOWING STATEMENT: "OR BY OTHER VA-APPROVED TRANSFER METHOD")) AND THE METHODS THAT YOU WILL TAKE TO SECURE THE TRANSMISSION OF THE DATA>, any and all related data for: <INSERT NAME OF RESEARCH PROTOCOL/STUDY/PROJECT OR IF PREPARATORY TO RESEARCH DESCRIBE THE PREPARATORY ACTIVITY AND POTENTIAL RESEARCH PROJECT>. The following data will be sent: <INCLUDE A COMPLETE LIST OF ALL DATA ELEMENTS THAT WILL BE SENT TO THE RECIPIENT>.
4. The type of Data being released include:
	1. [ ]  Identified (i.e., names, addresses, dates, etc)
	2. [ ]  Coded (i.e., direct identifiers removed, study code/ID included, etc)
	3. [ ]  De-Identified (all 18 HIPAA identifiers and study code/ID removed)
		1. [ ]  Verified Statistically; OR
		2. [ ]  Verified by Removal of 18 HIPAA identifiers and study code/ID
	4. [ ]  Limited Data Set[[1]](#footnote-1)
	5. [ ]  Other: Explain
5. The following named individuals are designated as VAPORHCS’s Points of Contact for performance of the terms of the Agreement.

**Point-of-contact on behalf of VA Portland Health Care System**

Insert Privacy Officer’s Name and Phone Number

Insert Information Security Officer’s Name and Phone Number

1. Recipient agrees that the data provided (hereinafter referred to as the “Data”) will be used solely for the purpose of <INSERT NAME OF RESEARCH PROTOCOL/STUDY/PROJECT OR IF PREPARATORY TO RESEARCH DESCRIBE THE PREPARATORY ACTIVITY AND POTENTIAL RESEARCH PROJECT>.
2. Recipient is designated as custodian of this Data and 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. If the custodianship is transferred within the organization the Recipient agrees to notify the Sender within (15) days of any change.
3. In addition to the Recipient’s access, the following individuals and/or entities will also have access to or use the Data as required by the protocol (attach another sheet if additional space is needed):

| **Name** |  | **Title** |  | **Location** |
| --- | --- | --- | --- | --- |
|       |  |       |  |       |
|       |  |       |  |       |
|       |  |       |  |       |
|       |  |       |  |       |

1. Access to the Data shall be restricted to authorized personnel only. Such personnel shall be advised of: (1) the confidential nature of the information; (2) safeguards required to protect the information; and (3) the administrative, civil and criminal penalties for noncompliance contained in applicable Federal laws. The Recipient agrees to limit access to, disclosure of and use of all Data provided under 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 the Data to perform the work described in this Agreement.
2. A number of VA directives exist to instruct employees on the proper handling of confidential and Privacy-protected Data. These include, but are not limited to, VA Handbook 5011/5, Chapter 4, (Alternative Workplace Arrangements), Security Guideline for Single-User Remote Access, Revision 3.0, VA Directive 6500, “Information Security Program,” VA Directive 6504, Restrictions on Transmission, Transportation and Use Of, and Access to VA Data Outside of VA Facilities and VA Directive and Handbook 6502, “Privacy Policy”, VHA Directive 1605, VHA Directive 1605.01 and 1605.2, and VHA series 1200 Handbooks.
3. No effort will be made to re-identify Data that are de-identified, which includes unscrambling social security numbers to reveal the real social security numbers.
4. The Sender <RETAINS -OR- RELINQUISHES> all ownership rights and responsibilities to the original and derivative Data file(s) provided to the Recipient under this Agreement. <DELETE IF RELINQUISHED, OTHERWISE: The Recipient of the data must provide the following information: 1) Describe where the data will be stored, 2) Describe means of accessing data and access audit methods, and 3) Provide date of project completion.> <DELETE IF RELINQUISHED, OTHERWISE: Describe disposition of data after project completion. Include initial data received, any new data that were generated based on the original data & any data repositories created from original data.>
5. IF RETAINING OWNERSHIP USE THE FOLLOWING LANGUAGE: Except as VA shall authorize in writing, the Recipient 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 those individuals listed in this Agreement. 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 in connection with the purposes established herein or as otherwise required under the Freedom of Infomration Act (FOIA), or other Federal law. VHA will clearly indicate in writing any information that is considered to be trade secret or confidential business information. If the Recipient is not an entity already observing HIPAA regulations and conducting HIPAA-related privacy and security trainings then the Recipient and all other individuals identified as having access to the Data in this Agreement must complete the VA trainings required by the Privacy Officer (PO) and Information System Security Officer (ISSO). Certificates demonstrating completion of either VA training, or the Recipient's applicable training, must accompany this Agreement when it is routed for signature.
IF RELINQUISHING OWNERSHIP USE THE FOLLOWING LANGUAGE: Upon completion of the Data transfer, the Sender relinquishes all ownership rights to the copy of the Data that was provided to the Recipient.
6. IF RETAINING OWNERSHIP OF THE DATA USE THE FOLLOWING LANGUAGE (this statement includes paragraphs 14-17; please see the bottom of paragraph 17 for relinquished instructions): The Recipient 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 Recipient agrees to notify the Sender within fifteen (15) calendar days of any change in the named Recipient. The administrative, technical and physical safeguards will be developed in accordance with VA Handbook 6500, to protect VA data confidentiality and to prevent unauthorized access to the Data provded. If co-mingling must be allowed to meet the requirements of the business/research need, the Recipient must ensure that VHA's information is returned to the Sender or destroyed in accordance with VA's sanitization requirements.
7. All VA coded or identifiable (including Limited Data Sets) Data and derivative data must be stored in an encrypted partition on the Recipient's information system hard drive using FIPS 140-2 validated software. (See http://csrc.nist.gov/groups/STM/cmvp/validation.html for more 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 VA Data stored on any portable drives, information technology (IT) components, disks, and/or CDs/DVDs.
8. 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 unless transmission refers to the return of the Data to the Sender. All electronic storage media use on non-VA leased or owned IT equipment/components that are used to store, process, or access VA Data 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 this Agreement, or (2) disposal or return of the IT equipment/components by the Recipient or any person acting on behalf of the Recipient.
9. Authorized representatives of the Department of Veterans Affairs and Office of Inspector General will be granted access to premises where the aforesaid file(s) are kept by the Recipient for the purpose of confirming that the Recipient is in compliance with security requirements.
IF RELINQUISHING OWNERSHIP RIGHTS USE THE FOLLOWING LANGUAGE: Maintenance, storage, security, and safeguards will be the responsibility of the Recipient upon completion of the Data transfer.
10. In the event that an employee, Recipient or other user of Data covered by this Agreement, loses confidential or Privacy-protected Data or the Data is stolen or removed from designated locations or used or disclosed for purposes other than outlined in this Agreement, the employee or Recipient must report the incident immediately upon discovery of the incident to the VAPORHCS ISSO, Privacy Officer, to the employee’s or Recipient’s immediate supervisor, and to the Recipient of the Data. The Recipient must notify the Sender, it is then the responsibility of the Sender to notify the Institutional Review Board (IRB) having oversight responsibility for the repository in accordance with the repository SOP. Senior management should be informed immediately by the supervisor or the Sender, who will further inform those in the chain of command. The incidents must also be reported to the Data Breach Response Service (DBRS) within one hour of the report of the incident. The incidents should be reported to the DBRS via the Information Security Officer (ISSO) or designee, and entered into the Privacy Security Event Tracking System (PSETS) by the Privacy Officer. The ISSO will report to the US-CERT (Computer Emergency Readiness Team) the information regarding the incident reported to the DBRS and in PSETS within the hour timeframe. A distribution list (VHA REPORTS TO US-CERT) has been established for use by the ISSO in reporting all incidents involving personally identifiable information via Exchange, and includes the key VHA representatives that need to be notified as well as the DBRS.
11. Failure to comply with VA policy and regulations pertaining to Cyber Security and safeguarding confidential and Privacy-protected Data may violate Federal law. Some of these laws carry civil and criminal penalties.
12. None of the VAPORHCS Data, any Data extracted or derived from this transfer, or other Data files provided by the VAPORHCS, will be released to any other organization or individual external to the VAPORHCS without approval of the Sender.  In addition, the Recipient will not publish nor release any information that is derived from the file that could possibly be expected to permit deduction of a beneficiary’s identity.  Infractions will be subject to prosecution under federal law.
13. The VAPORHCS has the authority to release this Data based on:
	1. [ ]  Data are de-identified (direct identifiers and study code/ID are removed) and thus does not include protected health information (PHI), which renders the Data not protected by the Privacy Rule. This includes de-identified data that was collected under a waiver as covered under the Technology Transfer Act.
	2. [ ]  Data are delivered as a Limited Data Set as defined by the HIPAA Privacy Rule at 45 CFR § 164.514(e) and thus satisfies the obligations under the HIPAA Privacy Rule.
	3. [ ]  HIPAA waiver approved by the IRB and Data sharing meets the following:
		1. Under the HIPAA Privacy Rule: documented approval of waiver of authorization from the IRB of record or Privacy Board that includes the following elements:
			1. Statement identifying the IRB or Privacy Board and the date on which the authorization was approved.
			2. Statement that the IRB or Privacy Board has determined that the waiver of authorization satisfies the following criteria: (1) the use or disclosure of PHI involves no more than minimal risk to the privacy of the individuals under criteria specified in the Privacy Rule, and (2) the research could not be practicably be conducted without access to the PHI; and documents a brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board in order to conduct the research.
			3. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures.
			4. The documentation is signed by the chair or other member as designated by the chair of the IRB or Privacy Board, as applicable.
		2. Under the Privacy Act: Approval of use of the Data for research by the VAPORHCS’s IRB of record.
		3. Under 38 USC 7332: Written assurance that the purpose for requesting the Data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, any individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner.
	4. [ ]  Review of the repository protocol that included justification for the information request, a summary of the research repository’s objectives, and a copy of its privacy and security plan.
	5. [ ]  Written informed consent and HIPAA authorization were obtained which document permission to share the data for the purpose(s) described.
14. The Recipient will ensure compliance with the terms and conditions of this Agreement. The VA or VHA may request verification of compliance. 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.
15. This Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the Sender will notify the Recipient to follow the disposition of the Data, if ownership was retained, as described in paragraph 13.
16. On behalf of both parties the undersigned individuals hereby attest that they are authorized to enter into this Agreement and agree to all the terms specified herein.

Sender’s Name Date

Sender’s Title

VA Portland Health Care System

Recipient’s Name Date

Recipient’s Title

VA Portland Health Care System

David M. Cohen, M.D. Date

Associate Chief of Staff, Research Service

VA Portland Health Care System

Information System Security Officer Date

VA Portland Health Care System

Privacy Officer Date

VA Portland Health Care System

Ronald Groenendaal Date

Area Manager - VA Portland

VA Portland Health Care System

1. A Limited Data Set is protected health information from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, e-mail address, Social Security Number (SSN), medical record number, health plan number, account number, certificate and/or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. A limited data set is not de-identified information or data. A limited data set can only contain elements of dates (e.g., date of visit/encounter, birth/death, admission/discharge, etc.), certain geographic information (city, state, zip code), and other numbers, characteristics, or codes not listed as direct identifiers. [↑](#footnote-ref-1)