Memorandum of Understanding and Agreement (MOU/A)
Between
Department of Veterans Affairs/Department of Defense
Palo Alto VA Medical Center (VAMC)
and
Department of Veterans Affairs
Office of Information and Technology
Enterprise Systems Engineering
Enterprise Testing Service

February 15, 2018

Version 1.0

Revision History

Date	Revision	Description	Author
February 15, 2018	1.0	MOU/A Between VA/DoD	ESE Enterprise Testing Service

Table of Contents

List of Tables

1. Purpose

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) and/or Interagency-sponsored teams utilize de-identified Veterans Health Information System and Technology Architecture (VistA) databases for the purposes of developing and testing health care systems and applications. VA OIT has been tasked with providing these teams with a Development and Testing Environment (DTE) for this purpose in managed and controlled environments in Development and Test Centers (DTC).

The VA OIT Enterprise Systems Engineering (ESE) Enterprise Testing Service (ETS) Test Center (ETSTC) is the designated custodian of a library of de-identified VistA databases from selected VA Medical Center/Department of Defense (DoD) sites; libraries will also be maintained in ESE ETS designated OIT partnered test sites. In support of this endeavor, the VA OIT ESE ETSTC is requesting a recent backup copy of the Palo Alto VA Medical Center (VAMC) patient/employee VistA database.

The purpose of this Memorandum of Understanding/Agreement (MOU/A) is to document the agreement between Palo Alto VAMC and the VA OIT ESE ETSTC and ETS's designated OIT partnered test centers. This MOU/A outlines the processes employed to ensure adequate privacy and security safeguards by VA OIT prior to deployment to the field using the de-identified database data, and to ensure proper handling and disposal of the data is accomplished when it has been determined that the data is no longer required for pre-production testing purposes.

2. Scope

The OIT is responsible for data management, complying with all conditions of use, establishment, and maintenance of security arrangements as specified in this Agreement to prevent unauthorized access to the data. As such, it is understood that the OIT will meet the following responsibilities in its use of the patient/employee database:

- Access to the patient/employee data provided by the Palo Alto VAMC will be limited to authorized personnel working for ETSTC for the purpose of de-identifying and running the Test Account Reset Utility on the database. Project teams working on approved projects will only have access to the database after the de-identification is complete. It should be noted that the ETSTC staff includes contractors who will need access to this database for set up and testing purposes. Access will not be granted until all security and privacy requirements for background checks, training, and business associate agreements are completed.
- Use of the data covered under this agreement, maintained in the ETSTC by authorized personnel, other than for those uses specified herein, must be fully justified by the requestor and approved by the VA OIT Program Manager (PM), as well as the Chief of Information Technology Systems Service, Information Security Officer (ISO), and Privacy Officer (PO) at the Palo Alto VAMC prior to use.

- VA OIT will treat the database as containing sensitive data, and as such, all printouts from the database will be handled and disposed of in accordance with VA and Veterans Health Administration (VHA) information security and privacy policies and procedures.
- If/when it has been determined that the database is no longer required, the ESE PM is responsible for notifying in writing that database is no longer required. The ETSTC is responsible for removing the data from the system and for destroying in accordance with VA and VHA media sanitization policies to prevent unauthorized access.
- All VA OIT personnel will access the data in the ETSTC in accordance with the minimum necessary standards outlined in VHA Handbook 1605.2.
- All VA OIT personnel with access to the data must have completed all required VA Privacy and Information Security Training.
- Connections to applications/environments that are located outside VistA will be provided when requested by a project team with valid justification. All requests will be analyzed, approved, and documented by ETSTC VA Management.
- Once testing is complete or when an employee leaves a project, the individual's access to the database will be terminated.

3. Services and Products to Be Provided

Services and products are identified as a complete set of the most current database backup. The database copy will be sent to the ETSTC, utilizing an approved secure transport method. The preferred method utilizes Secure File Transfer Protocol (SFTP).

The steps to securely obtain a copy of the Palo Alto VAMC datasets are as follows:

1. The ETSTC Point of Contact (POC) will make contact with the Palo Alto VAMC POC.
2. The Palo Alto VAMC POC, or delegate, will zip the datasets.
3. Upon a mutually agreed upon date, the Palo Alto VAMC POC will ***SFTP*** the zipped datasets to the ETSTC.
4. The ETSTC will install the copied datasets into the ETSTC Cache instance with the assistance of the Palo Alto VAMC POC.

After the Palo Alto VAMC database is loaded into the ETSTC Cache instance, the ETSTC is responsible for performing the following actions:

1. Run the National VistA Support (NVS) Test Account Reset Utility converting the database from production to test account mode
2. Run the De-Identification software to change sensitive patient Protected Health Information (PHI) and Personal Identifiable Information (PII) data. The de-identification process converts the patient and person identities to fictional identities. Live patient data is not used for development or testing.
3. Christen the domain to establish its new identity.

4. Once the new test database is established and verified, the original copy of the Palo Alto VAMC database will be deleted from the storage location.

If transfer by SFTP is unavailable, alternative methods can be discussed with the ETSTC and the Palo Alto VAMC.

4. Incident Reporting

The VA OIT official discovering a security incident involving data provided under this agreement will report it internally in accordance with the established incident reporting procedures, and to the corresponding POC in the facility as listed in this MOU/A so that the incident can be appropriately managed and reported within both organizations. Contact information for both the facility and VA OIT staff will be included in the MOU/A.

5. Terms of Agreement

This Agreement is effective upon the date of the signature of the last party signing this Agreement, and will remain in effect for three (3) years after the last date of signatures in the signature block below. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly-signed agreement should explicitly supersede this agreement, which should be referenced by title and date. If one or both parties wish to terminate this agreement prematurely, they may do so upon thirty (30) days advance notice or in the event of a security incident that necessitates an immediate response. Upon termination, all data and media associated with this agreement will be removed from ETSTC systems and destroyed in accordance with VA and VHA media sanitization policies.

6. Changes

This Agreement may be modified by the mutual agreement of both parties upon thirty (30) calendar days of notification, or sooner if the parties so desire. Any notification will be made in writing and signed by both parties. This Agreement, or any of its specific provisions, may be modified only by the signature approval of the parties' signatory to the Agreement or designees or by their respective official successors.

7. Points of Contact

The following individuals are key POCs for purposes of coordinating changes to this Agreement or other technical and administrative issues that may arise.

7.1. Facility

Tony Fitzgerald, Center Director
Palo Alto VA Medical Center
3801 Miranda Ave
Palo Alto, CA 94304
Voice: 650-492-5000 x65402

Tammy Ridder, Facility Chief Information Officer (FCIO)
Palo Alto VA Medical Center
3801 Miranda Ave
Palo Alto, CA 94304
Voice: 650-844-0402

Danny O'Dell, Information Security Officer (ISO)
Palo Alto VA Medical Center
3801 Miranda Ave
Palo Alto, CA 94304
Voice: 650-493-5000 x63844

7.2. VA ESE

Marilyn Hodge, Director
Enterprise Testing Service, Enterprise Systems Engineering
Birmingham Office of Information Field Office (OIFO)
600 Beacon Parkway West Suite 120
Birmingham, AL, 35209
Voice: 205-943-2320
Fax: 205-943-2400

8. Execution

This successor Memorandum of Understanding and Agreement is executed

this 15th day of February 2018.

9. Signatory Authority

We, the undersigned, mutually agree to the terms of this agreement.

Tony Fitzgerald Facility Director, Palo Alto VAMC	Date
Tammy Ridder Facility CIO, Palo Alto VAMC	Date
Marilyn Hodge Director, ETS, ESE	Date
Ray E. Lee Division Director, ESE ETSTC	Date
Rhodes, Gina S VA OIFO ISO, Bay Pines OIFO	Date
Chris Shorter (SES) EO, Facility Chief Information Officer	Date
Gallegos, Griselda EO ISO	Date

Appendix A. Acronyms

Table 1: Acronyms

Term	Definition
CIO	Chief Information Officer
DoD	Department of Defense
DTC	Development and Test Centers
DTE	Development and Testing Environment
ESE	Enterprise Systems Engineering
ETS	Enterprise Testing Service
ETSTC	Enterprise Testing Service Test Center
FCIO	Facility Chief Information Officer
ISO	Information Security Officer
MOU/A	Memorandum of Understanding/Agreement
NVS	National VistA Support
OIFO	Office of Information Field Office
OIT	Office of Information and Technology
PHI	Protected Health Information
PII	Personal Identifiable Information
PM	Program Manager
PO	Privacy Officer
POC	Point of Contact
SFTP	Secure File Transfer Protocol
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VistA	Veterans Health Information System and Technology Architecture