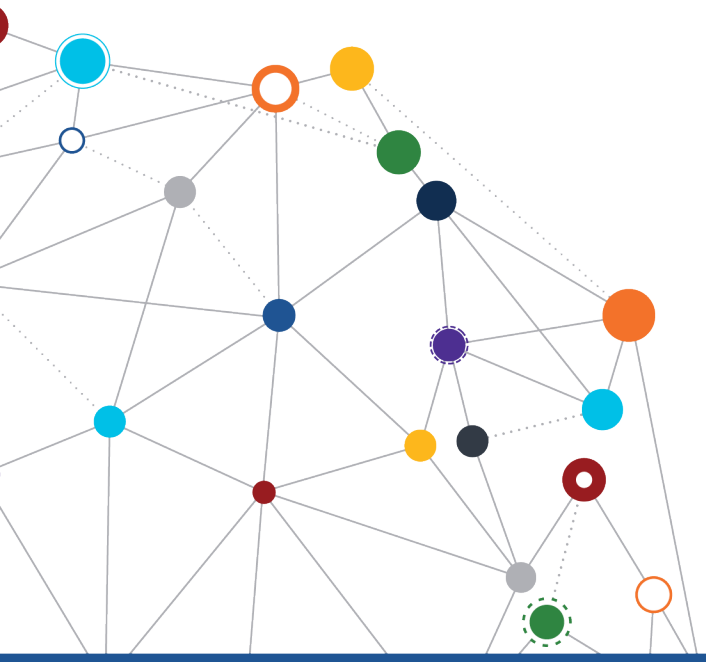
OFFICE OF
INFORMATION
AND TECHNOLOGY

Enterprise Research Data Security Plan (ERDSP) User Guide

January 2021 | Version 2.0 | OIS-System Security Support Department – Research Support Division
FOR VA INTERNAL USE ONLY



DOCUMENT CONTROL CHANGE SHEET

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of the entire document. Increment the version number's decimal (minor) portion here, on the cover page and in the headers for each revision. The policies herein are to be considered active and in effect until this record is reissued. This record does not expire.

Revision Date	Document Revision History Summary of Changes	Version	Author
4/2/20	Beta testing version.	1.0	Terry Peters
4/27/20	Incorporated changes from beta testing.	1.1	Terry Peters
6/9/2020	Incorporated recommended changes from ORD and ORO	1.2	Terry Peters
10/3/2020	Revised external information systems and VA mobile device sections	1.3	Terry Peters
1/26/21	Final draft.	2.0	Terry Peters
1/28/21	Initial Review	2.0	DuJuan Williams
1/28/21	Initial Review	2.0	Carol Johnson
2/1/21	Tech Writer Review	2.0	Kerry Cooper

Table of Contents

1. Overview

The Enterprise Research Data Security Plan (ERDSP) is a standardized security plan template designed to provide VA Research & Development (R&D) stakeholders (Principal Investigators (PIs), Information System Security Officers (ISSOs), Research Coordinators, Research Administrative Officers and Institutional Review Boards (IRBs) with a tool to aide in documenting the safeguards to protect research data, information and resources. The security plan template provides a mechanism for PIs to document their plan for managing risks to protect research data within a research study and promotes the standardization of the ISSO review during the IRB/R&D Committee research study information security process in accordance with VA and Federal policies. The ERDSP was developed as a mitigating control to assist PIs and research data stewards in establishing a comprehensive research data security plan and addressing VA security policy requirements during the planning and design phases of the research study/protocol. The development of an ERDSP is a part of the VA's efforts to ensure data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity and availability of research data.

2. Purpose

As part of the comprehensive VHA Research and Development Committee review process, this Research Support Division (RSD) ERDSP User Guide introduces a standardized process for conducting the ISSO research protocol review to support effective research protocol data management. This User Guide may be used by R&D stakeholders involved in the review of research conducted within local VA Medical Center (VAMC) R&D Committees or IRBs. This user guide also provides R&D stakeholders with procedures, supplemental information, examples and meaningful use cases for completing the ERDSP and reviewing the ERDSP template for compliance with VA security policy.

3. Scope and Applicability

This ERDSP User Guide outlines the procedures for all R&D stakeholders whose research projects, protocols or studies are overseen by a VA R&D Committee and that involve the collection, processing, storage or transmission of research data to submit an ERDSP during the VA R&D Committee approval process.

Note: If you are unable to open the ERDSP PDF file in Chrome or Firefox, you will need to disable your web browser “in-browser PDF reader”.

4. Roles and Responsibilities

The roles and responsibilities for R&D stakeholders in the VA OIS ERDSP R&D Committee review process are as follows:

Principal Investigator:

- Submits an ERDSP which documents the PI's security plan for research data use, storage and security to the facility ISSO

Information System Security Officer:

- Reviews proposed research study to ensure that the research complies with information security requirements for VA research data, evaluating the protocol/studies data usage and making recommendations to ensure implementation of reasonable safeguards for the data as determined within the ERDSP template and ERDSP User Guide

Research & Development Committee:

- Reviews research proposals and approves the research, requires modifications to obtain approval or disapproves the research
- Provides approval of research contingent upon ISSO review of the ERDSP

Research Support Division:

- Provides ERDSP template guidance to the R&D/IRB Committee stakeholders
- Maintains ERDSP template and ERDSP User Guide/SOP documentation
- Provides ERDSP template training and awareness to the R&D Committee/IRB stakeholders

5. Enterprise Research Data Security Plan Template Procedures

The ERDSP template supports the implementation of administrative, technical and operational safeguards that are commensurate with the sensitivity of the data and the overall security risk to the VA. The ERDSP template and the ERDSP User Guide provide a consistent evaluation criterion for assessing a research protocol's data usage, storage, sharing and transmission requirements by:

(1) Aligning the questions on the ERDSP template with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and the NIST Cyber Security Framework (CSF).

(2) Categorizing research data to ensure appropriate levels of protection according to the risk level of data type in accordance with Federal Information Processing Standard (FIPS) Publication 199 and NIST 800-60, Vol 1.

(3) Establishing high-risk research study conditions that determine when an information security review is required.

(4) Providing relevant information and guidance to researchers ensuring accurate and relevant documentation of the ERDSP template.

(5) The information in the ERDSP User Guide corresponds to the sections and questions on the ERDSP template. The ERDSP template is a branching logic form; the questions that appear on the form are based on answers provided to previous form questions.

If you have questions or suggestions to improve the ERDSP template and guide, please submit the questions or suggestions through the ERDSP feedback and suggestions form.

5.1 Completing the ERDSP template for New Study Submissions

1. Date
   "Enter the date the ERDSP was completed"
2. Research Study Title
   "Enter Research Study Title"
3. Study Number
   "Enter IRB-assigned study number"
4. Type of Research Study
   "Enter the type of research study (Animal, Basic Laboratory or Human)
5. VA Facility
   "Select the VA facility name from the drop-down list or, if the submission is for multiple VA sites, enter the facility name for the primary PI on the study"
6. Purpose of Submission
   "Enter the Purpose of Submission (Amendment or New)"
7. Next step is the completion of Section 1: Research Study Conditions.

5.2 Completing the ERDSP template for Study Amendments

1. Date
   "Enter date the ERDP was completed"
2. Research Study Title
   "Enter Research Study Title"
3. Study Number
   "Enter R&D Committee Assigned Study Number"
4. Type of Research Study
   "Enter Type of Research Study (Animal, Basic Laboratory or Human)"
5. VA Facility
   "Select the VA facility name from the drop-down list or, if the submission is for multiple VA sites, enter the facility name for the primary PI on the study"
6. Purpose of Submission
   "Enter Purpose of Submission (Amendment or New)"

a. Amendment to Research Study

(1) Guidance

An ERDSP is required to be completed for all research study amendments except amendments submitted solely for the purposes listed in Appendix C – Research Study Amendment ERDSP Determination Aide.

For a study amendment, only the sections of the ERDSP that are affected by the amendment must be completed.

(2) ERDSP Questions

(a) **Will the amendment make changes to any of the sections of the ERDSP?**

For this question, answer "Yes" if the study amendment changes any of the sections of the ERDSP or answer "No" if none of the sections will be changed. If "No", sign the ERDSP and submit the form with the study submission.

(b) **Select the sections of the ERDSP that will be changed/updated by the amendment and complete those sections only.**

For this question, select the sections of the ERDSP that will be changed. Selecting a section will reveal the ERDSP questions that are required to be completed for the section.

Section 1: Research Study Conditions
Section 2: Data Classification
Section 3: Data Source and Collection
Section 4: Data Access and Storage
Section 5: Data Sharing with VA Research Facilities
Section 6: VA Mobile, Portable Storage Devices and Mobile Applications
Section 7: VA Software
Section 8: Agreements and Authorizations
Section 9: External Information Systems and Data Sharing with External Entities

b. Section 1: Research Study Conditions

(1) Guidance

Based on the risk assessment conducted for Research Protocol Data Management within VHA Research, the research study conditions were developed to identify high-risk research studies that require explicit ISSO review.

The research study conditions selected will expand the form and display new sections of the ERDSP template to be completed.

Section 1: Research Study Conditions
Section 2: Data Classification
Section 3: Data Source and Collection
Section 4: Data Access and Storage
Section 5: Data Sharing with VA Research Facilities
Section 6: VA Mobile, Portable Storage Devices and Mobile Applications
Section 7: VA Software
Section 8: Agreements and Authorizations
Section 9: External Information Systems and Data Sharing with External Entities

Upon completion of the form, the ISSO review requirement section at the end of the form will state if an ISSO review is required for the research study. If an ISSO review is not required, the PI will still include the signed and completed ERDSP in the IRB submission.

Research studies not requiring explicit ISSO review may be audited to ensure proper completion of the ERDSP.

(2) **ERDSP Questions**

(a) **Will any research study data be transmitted or transferred to an external entity? (MP-5/SC-8)**

For this question, answer "Yes" if any research study data will be transmitted or transferred to an external entity (e.g., affiliate, collaborator, sponsor, contractor, consultant). Otherwise, answer "No" and proceed to the next question. For additional information on the methods to transfer study data to a non-VA institution, see Section 9 – External Information Systems and Data Sharing with non-VA Entities.

Use Case Scenario #1. The Boston VA is participating in a collaborative human research study with Harvard University. Per the research protocol, each VA subject will execute a HIPAA authorization for the disclosure of a copy of his or her study data to Harvard University. The VA will transmit the copy of VA research study data to Harvard University using the Azure Rights Management System (RMS). For this research study, the question should be marked "Yes", as the VA will transmit a copy of VA research study data to an external entity.

Use Case Scenario #2. The Palo Alto VA is participating in a collaborative human research study with their affiliate university. The research study involves the analysis of MRI brain images which will be taken at the VA and analyzed at the affiliate university. Per the research protocol, each VA subject will execute a HIPAA authorization for the disclosure of a copy of his or her protected health

information to the affiliate university. The VA will transfer a copy of the MRI images to the affiliate university using a VA-approved encrypted external hard disk drive. For this research study, the question should be marked "Yes", as the VA will transfer a copy of the MRI images to the affiliate university.

(b) **Will the Research Study use any external information systems or devices? (AC-20)**

For this question, answer "Yes" if any external information systems or devices will be used in your research study. Otherwise, answer "No" and proceed to the next question. For additional information on external information systems and devices, see Section 9: External Information Systems and Data Sharing with External Entities.

Use Case Scenario #1 The Durham VA is participating in a clinical trial sponsored by Novartis. Per the research protocol, each VA subject will execute a HIPAA authorization for the disclosure of a copy of his or her protected health information to the sponsor. The VA will disclose a copy of the research study data to the sponsor using a sponsor-provided Electronic Case Report Form (eCRF) hosted by Rave Medidata. For this research study, the question should be marked "Yes", as the eCRF provided by the sponsor is considered an external information system.

(c) **Will the research study use any mobile devices? (AC-19/MP-4)**

For this question, answer "Yes" if any mobile or portable storage devices will be used in the research study. Otherwise answer "No" and proceed to the next question. For additional information see Section 6: VA Mobile, Portable Storage Devices and Mobile Applications

Use Case Scenario. The Bronx VA is conducting a research study that involves conducting in-person interviews of research subjects at the VA. The PI will use a VA issued digital voice recorder to record the subject interviews and will upload them to the VA network after each interview. For this research study, the question should be marked yes, because digital voice recorders are considered a mobile device.

(d) **Will the research study use any mobile applications?**

For this question, answer "Yes" if your research study will utilize any mobile applications otherwise answer "No" and proceed to the next question.

Use Case Scenario. The Miami VA is conducting a research study that requires reminders be sent to research subjects. The study will use the Annie App, which is approved for use in the VA and is listed in the VA App Store. For this research study, the question should be answered "Yes", because the Annie App is a mobile application.

c. Section 2: Data Classification

(1) Guidance

(a) VA Research data is classified as sensitive and non-sensitive. The classification of the data will determine the level of protection applied to the data. The research data classifications were determined using Federal Information Processing Standard (FIPS) Publication 199 and NIST SP 800-60. The classification is determined by assessing the impact of the loss of Confidentiality, Integrity and Availability (CIA) of the information. For sensitive and non-sensitive data, the loss of the Integrity was determined to be moderate, resulting in both sensitive and non-sensitive data having a Moderate Baseline Impact.

(b) **Sensitive – Data Types**: III, PII, PHI, Animal Research (Category D & E with picture & video), Genomic (Human), Intellectual Property, (FISMA Requirement = Moderate FISMA Baseline Impact)

(c) **Non-Sensitive – Data Types:** Deidentified Research, Unpublished Research (Basic Animal Research, except for Category D & E with picture and video, and Non-Human Basic Lab, Animal Research (Category B & C), (FISMA Requirement = Moderate FISMA Baseline Impact)

(d) **Public – Data Types:** Published Research (Aggregate data that can be submitted to peer review journals and/or presented at conferences, included in grant applications), (FISMA Requirement = Low FISMA Baseline Impact)

Pubic data is classified as non-sensitive but is listed separately on the ERDSP template and user guide due to the FIPS Publication 199 classification of low for confidentially, low for integrity and low for availability.

(2) ERDSP Questions

Question 1 – Select the classification of the data that will be used in this research study. Select all that apply. (RA-2)

For this question, select the classification for each type of data that will be used in your research study.

(3) ISSO Review Requirements

The ISSO should review the protocol and verify that the data classification select is correct, and the level of protection applied to the research study data is commensurate with the classification of the data.

d. Section 3: Data Sources and Collection

(1) **Guidance**

(a) Data sources supply the information required to conduct the research study. Commonly used VA data sources include but are not limited to:

1 Research Study Subject

2 Vista/CPRS/Cerner

3 CDW

4 VA/CMS data

5 Databases

6 Laboratory results

7 Non-VA Medical Records

8 MVP

9 See the VHA Data Portal for additional VHA data sources

(b) Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion, which enables one to answer stated research questions, test hypotheses and evaluate outcomes. Commonly used data collection methods include but are not limited to:

1 Audio recording

2 Behavioral observations

3 Chart reviews

4 Control/focus groups

5 Questionnaires

6 Interviews

7 Photographs

8 Biological specimens

9 Video recording

10 Secondary dataset

(c) The following applications have a VA Authority to Operate (ATO) and can be used to collect, analyze, process or store research study data.

1 Westat (Surveys and Questionnaires)

2 VINCI

3 VA REDCap

4 MVP

5 DocuSign

6 The VA Cloud Software Catalog lists additional cloud-based applications that are in the process of obtaining a VA ATO or already have a VA ATO.

(d) Electronic Methods to obtain informed consent

See Research Guidance for the Use of Electronic Methods to Securely Obtain Informed Consent.

(2) **Best Practice**

When collecting research data at non-VA locations, a best practice is to collect the data on a VA-issued laptop. This ensures the data is encrypted and properly protected when outside of controlled areas.

(3) **ERDSP Questions**

(a) **Question 1 - Does the research study involve more than one VA participating site?**

For this question, select "Yes", if more than one VA site is participating in the study. Answer "No", if only one VA site is participating in the research study.

(b) **Question 2 - Provide the name of each participating VA site listed within the IRB application.**

Self-explanatory

(c) **Question 3 - Select the data sources to be used in this research study. Select all that apply.**

For this question, select all data sources that will be used in the research study. If a data source is not listed, select "Other" and enter your source in Question 4.

(d) **Question 4 - Describe the "Other" and/or database sources used in the research study.**

For this question, provide details about the "Other" and "Database" sources used in the research study. If a database is used in the research study provide the name of the database, physical location, and the database owner.

(e) **Question 5 - Select the data collection methods that will be used in the research study. Select all that apply.**

For this question, select the data collection methods that will be used in the research study. If a data collection method is not listed, select "Other".

(f) **Question 6 - Describe the "Other" data collection methods used in the research study.**

For this question, provide details about the "Other" data collection methods used in the research study.

(g) **Question 7 - Will the research study use any VA applications or websites?**

For this question, select "Yes" if any VA applications or websites will be used to collect, analyze, process or store research study data. Otherwise, answer "No" and proceed to the next question.

(h) **Question 8 - Provide the name and URL (web address) of the VA applications and/or websites that will be used in the research study.**

For this question, provide the name of each VA application or website that will be used in your research study (e.g., VA REDCap, VINCI).

(4) **ISSO Review Requirements**

(a) The ISSO will verify that the data sources and data collection methods listed on the ERDSP are correct.

(b) The ISSO will verify websites and applications listed in this section have a VA ATO.

e. Section 4: Data Access and Storage

(1) **Guidance**

(a) Concept of least privilege Access to research study data must be restricted and employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. This principle applies to electronic and hard copy (paper) data. **SOURCE:** IS Knowledge Service Security Control AC-6

(b) **Access and storage of electronic data on the VA network.** Access to electronic research data stored on the VA network must be restricted by allowing accesses for authorized users (or processes acting on behalf of users) only which are necessary to accomplish assigned tasks. This can be accomplished by requesting the local IT Operations and Services (ITOPS) staff set access permissions on research study folders in Windows Active Directory, through a "YourIT" ticket.

For sites that have implemented Shared Folder and File Exchange (SFFX), this can be accomplished by contacting the research POC for SFFX.

(c) **Access and storage of hard copy (paper) data.** Sensitive research hard copy (paper) data must be stored securely when not in use. Sensitive research study hard copy (paper) data can be stored in lockable cabinets, safes or in a locked room. Access to the storage area must be limited to users requiring access to accomplish assigned taskings. Sensitive research study hard copy (paper) data should never be stored in shared rooms, cabinets or safes where unauthorized individuals may have access to the data and should never be stored in roll-away cabinets that can be easily moved or stolen. **SOURCE**: IS Knowledge Service Security Control MP-4.

(d) **Storage of electronic VA data on external information systems and applications**. VA-owned data is not authorized to be collected, processed or stored on external information systems (e.g., sponsor, affiliate, contractor and collaborator information systems) unless the system has been evaluated and received a VA ATO determination. If the determination requires the external information system to obtain a VA ATO, the system cannot be used until the until the AO has granted a VA ATO. For additional guidance, see External Information Systems and Data Sharing with non-VA Entities. **SOURCE**: IS Knowledge Service Security Control SA-9 and VA Handbook 6500.3.

7 **Research Scientific Computing Devices** A Research Scientific Computing Device (RSCD) within the VA is defined as a standalone or network-capable system or device that cannot obtain VA-approved baseline configuration settings and/or interfaces with scientific/clinical instrumentation in direct support of research activities and scientific studies.

To avoid confusion between medical devices and Special Purpose Systems (SPS): any device that has been modified for research purposes and/or interfaces with scientific/clinical instrumentation in

direct support of research activities and scientific studies, the device will be classified as an RSCD and will go through the RSCD Enterprise Risk Analysis (ERA) process.

Network-connected research scientific computing devices must undergo a risk assessment. Guidance for submitting the risk assessment can be found on the System Security Support Risk Analysis Portal under the "Research Scientific Computing Devices (RSCD)" column. Additional Enterprise Risk Analysis (ERA) submission and requirement information can found in the ERA Joint User Guide.

8 **Standalone Computers, Medical Devices and Research Scientific Computing Devices.** A standalone computer, medical device or scientific computing device, refers to a device that can run local applications on its own without needing a connection to a wide area network (WAN) or a local area network (LAN).

Standalone computers, medical devices and research scientific computing devices cannot contain the only copy of VA information. A backup of the information on the device must be created at regular intervals and stored securely. For help with backing up the information on these types of devices, submit a "YourIT" ticket to your local ITOPS staff.

(e) **Use Case Scenario #1** Dr. Jones shares an office with two other PIs who are not co-PIs for his current research study. Dr. Jones has begun collecting hard copy (paper) informed consent forms and HIPAA authorizations from the research subjects participating in the current study and needs to securely store them. Dr. Jones discussed the issue with his ISSO and decides that the best method to prevent unauthorized access to the documents is to store them in a lockable file cabinet in his office, with access limited to research study staff.

(f) **Use Case Scenario #2** Dr. McClure plans to use a standalone computer with specialized software to analyze research study data for his research study. Because the computer is not connected to the VA network, the research study will need to develop a plan to back up the data to the VA network on a regular basis. Dr. McClure discussed the issue with the local facility ISSO and the ISSO recommended the use of a VA encrypted USB flash drive or external hard disk drive to move the data from the standalone computer to the VA network.

(g) **Best Practice.** A best practice for controlling access to electronic file folders is Shared Folder and File Exchange (SFFX). SFFX is a VA developed and maintained web application for managing shared user data access and security. SFFX allows designated research personnel to manage research electronic files and folders. Interested VA research facilities should contact their local ITOPS Area Manager to request implementation of SFFX to manage access to research data.

(2) **ERDSP Questions**

(a) **Question 1 - Will access to the research study electronic data employ the concept of least privilege, allowing only authorized access to users (or processes acting on behalf of users)**

who are necessary to accomplish assigned tasks in accordance with VA mission and business functions? (AC-6)

For this question, answer "Yes" if access to the research study electronic data will employ the principle of least privilege and restrict access to those individuals requiring access to the data to accomplish assigned tasks? Otherwise, answer "No" and proceed to the next question.

(b) **Question 2 - Describe how sensitive hard copy (paper) documents will be physically secured. (MP-4)**

For this question, describe the method used to protect sensitive hard copy (paper) documents when not in use.

(c) **Question 3 - Provide the storage location of the VA research study electronic and paper data stored at the VA or offsite research locations. (AC-3/AC-6/MP-4)**

For this question, provide the primary storage location for VA electronic and hard copy (paper) data. You are not required to provide the location of additional copies of the data.

For the electronic data stored on the VA network, provide the file path that maps to the location of the electronic data. Example: "vhanflnas8\research service\research study 20-19". If you are unsure of the correct file path for your electronic data, contact your research administrative officer or submit a "YourIT" ticket to your local ITOPS staff for assistance.

If the electronic data is stored within an application, provide the name of the application where the data will be stored (e.g. "Data will be stored in the MVP Datamart" or "Data will be stored in the VINCI application workspace").

(d) **Question 4 - Will the research study use a standalone computer, medical, and/or research scientific computing device? (CP-9)**

For the question, answer "Yes" if any research study data will be stored on a standalone computer, medical device or research scientific computing device. Answer "No", if no standalone computer, medical and/or research scientific computing device will be used in the study.

(e) **Question 5 - Describe the process to back up the VA research study data stored on the standalone computer systems, medical devices, and/or research scientific computing devices. (CP-9)**

For this question, describe the process for backing up data on standalone devices and the frequency of such backups. If the research study staff are unsure of the process to back up the data, submit a "YourIT" ticket to the local ITOPS staff requesting assistance with developing a backup solution for

the standalone device. In the case of a medical device, contact the local facility Biomedical Engineering Office for assistance.

(3) **ISSO Review Requirements.**

(a) The ISSO will verify that electronic and hard copy (paper) VA research data is stored within the VA-authorized boundary (e.g., VA facilities, VA leased space and external information systems and applications with a VA ATO).

(b) The ISSO will verify that any external information systems used to process, store or transmit VA data has been evaluated for a VA ATO.

(c) The ISSO will verify that the research study has a process in place to backup user level data stored on standalone computers, medical devices and research scientific computing devices used in the research study and that the process meets VA security requirements.

f. Section 5: Data Sharing with VA Research Facilities.

(1) **Guidance**

There are several methods available to share study data (electronic and hard copy) with another VA research facility. The methods vary depending on the sensitivity of the data. Sensitive research study data must be securely transmitted/transferred. Electronic media must be encrypted with FIPS 140-2 (or its successor) validated encryption and non-digital (paper) media must be double wrapped and transported in a secure physical container.

(a) **Sensitive Data**

1 **VA Encrypted Email (SC-8/SC-28)**

2 **VA SharePoint (AC-6)**

Verify with your Area Manager that SharePoint is configured for the storage of VA-sensitive information and that access permissions are applied to the study information on the SharePoint to restrict access to those users (or processes acting on behalf of users) who are necessary to accomplish assigned tasks.

3 **Shared Folder on the VA Network (AC-6)**

Access to the shared folder must be restricted by allowing only authorized users (or processes acting on behalf of users) who are necessary to accomplish assigned tasks.

4 **Azure Rights Management System (RMS) (SC-8/SC-28)**

RMS is the protective technology used by Azure Information Protection. It uses encryption, identity, and authorization policies to help secure file attachments and email. Information can be protected both within VA and outside VA because the protections remain with the data, even when it leaves the VA. VA Office of Information & Technology (OI&T) has issued a set of frequently asked questions (FAQs) about Azure RMS use within VA and the Office of Research and Development (ORD) has issued ORD FAQs for the use of Azure RMS in VA research.

5 VA Encrypted Thumb Drive or External Hard Drive (AC-19)

USB Flash drives and external hard disk drives are required to meet the following requirements:

- The device must be encrypted with FIPS 140-2 (or its successor) validated encryption.
- The device must be on the Endpoint Security Engineering approved devices and apps list.
- The device must be accounted for on a VA equipment inventory list.

6 CD/DVD (AC-19)

CDs/DVDs must meet the following requirements:

- Encrypted with FIPS 140-2 (or its successor) validated encryption unless exempted by VA Directive 6609, paragraph 2.i.
- The password to the CD/DVD must be transmitted separately from the CD/DVD.
- The CD/DVD must be shipped via a secure delivery service that tracks the mail from pick-up to delivery. **SOURCE**: IS Knowledge Service Security Control AC-19 and VA Directive 6609.

7 Physical Transport (MP-5)

Individuals physically transporting sensitive information outside of controlled areas must obtain written approval from their supervisor, privacy officer (PO), System Owner and/or designee and ITOPS Area Manager. The written authorization applies to sensitive hard copy (paper) media and electronic media containing sensitive information (e.g.; laptops, tablets, CDs/DVDs, USB flash drives, external hard disk drives, SD cards) transported outside of controlled areas. **SOURCE:** OIS Knowledge Service Security Control MP-5.

8 FAX

Care should be taken to assure confidentiality when faxing sensitive information. Facilities must take reasonable steps to ensure the fax transmission is sent to the appropriate destination. Before sending a fax, users should review the FAX guidelines in the IS Knowledge Service Security Control SC-8, Control Level Guidance section. **Source:** OIS Knowledge Service Security Control SC-8.

(d) **Non-Sensitive Data**.

1 Unencrypted VA email

2 US Postal Service or other delivery service (FedEx, UPS)

3 Any of the methods used for sensitive data

SOURCE: VHA Directive 1605.01, paragraph 2.g.(6)

(2) **Use Case Scenario:**

Dr. Jones is collaborating with another VA facility on a research study analyzing MRI images of subjects with PTSD. Dr. Jones needs to send copies of the MRIs to the other VA facility, but the files are too large to email. Dr. Jones contacted his Area Manager and ISSO for assistance and they recommended he purchase a VA-approved external hard disk drive, encrypted with FIPS 140-2 (or its successor) validated encryption to transfer the data.

(3) **ERDSP Questions**

(a) **Question 1 - Will the research study share data with another VA facility? (AC-21)**

For this question, answer "Yes" if the research study will be sharing data with another VA facility. Otherwise, answer "No" and proceed to next question.

(b) **Question 2 - Provide the name of each VA research facility that data will be shared with and describe the method used to securely transfer the data. (SC-8)**

For this question, list the name of each VA facility that research study data will be shared with and describe the process to transfer the data.

(c) **Question 3 - Will research study personnel physically transport sensitive data outside their VA facility? (MP-5)**

For this question, answer "Yes" if research personnel will physically transport sensitive research study data (electronic or hard copy (paper)) outside their facility. Otherwise, answer "No" and proceed to the next question.

(4) **ISSO Review Requirements.**

(a) The ISSO will verify that electronic methods used to share research study data with other VA facilities are commensurate with the categorization of the data (e.g.; sensitive data must be encrypted in transmission).

(b) If research study personnel will transport sensitive digital and non-digital media outside of controlled areas, the ISSO will document in their study review:

"Personnel transporting sensitive information outside of controlled areas are required to obtain Supervisor, Privacy Officer (PO), System Owner and / or designee, Area Manager, or other designee approval, or it is documented and approved within a VA contract or agreement." **SOURCE**: IS Knowledge Service Security Control MP-5

The ISSO was removed from the approval process by the Acting Principal Deputy Assistant Secretary for OI&T memorandum, dated July 24, 2017, Subject: Amend Directive 7002, Logistics Management (VAIQ# 7776160).

g. Section 6: VA Mobile, Portable Storage Devices and Mobile Applications

The guidance in this section does not apply to external entity provided mobile devices, applications and portable storage devices. See Section 9: External Information Systems and Data Sharing with External Entities for guidance on devices provided by external entities.

(1) **Guidance**

(a) **Mobile Devices** Mobile devices are essentially general-purpose computing platforms. They are not restricted to performing one operation and can instead be used in many different domains—including medical, industrial and entertainment. A mobile device is defined as a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations (e.g., smart phones, smart watches, tablets, video recorders, digital cameras, wearable devices, e-readers, handheld gaming consoles, audio recorders, etc.). **SOURCE:** NIST SP 800-53 Rev. 4

VA Mobile devices (*excludes voice recorders, digital cameras and portable storage devices*) are required to meet the following requirements.

1 Accounted for on a VA EIL

2 Encrypted with FIPS 140-2 (or successor) validated encryption. If it is not technically possible to encrypt a mobile device, the documented justification and review/approval by the local ISO and Area Manager is required. The Deputy Assistant Secretary (DAS) for Office of Information Security (OIS) or designee must also review/approve VA mobile devices that cannot be encrypted. **SOURCE:** Information Security Knowledge Service, control AC-19

3 Listed on the Mobile Technology and Endpoint Security Engineering list of approved mobile devices

4 Securely stored when not in use

Mobile devices (*excludes voice recorders, digital cameras and portable storage devices*) not on the approved mobile devices list must be submitted for assessment and approval by the ITOPS Mobile Technology and Endpoint Engineering team. Mobile devices can be submitted for assessment and approval using the Mobile Device Intake Process. If the study plans to purchase a mobile device, the device should be submitted for assessment and approval prior to purchasing the device.

If the mobile device comes with pre-installed software, the software must be evaluated by the Technical Reference Model (TRM). Before submitting the software to the TRM for approval, the requestor should verify that the software is not already approved for use by checking the TRM Technology/Standard List.

If the software is not approved on the TRM Technology/Standard list, the software must be submitted to the TRM for assessment. The requestor will need to submit a Content Request Form to begin this process.

Users should pay special attention to the "Decision" tab of the TRM Technology/Standard List. This tab discusses the decision, constraints on the use of the software and the software versions that are approved for use in VA.

(b) **Voice Recorders** VA voice recorders are required to meet the following requirements:

1 Accounted for on a VA EIL.

2 Use and configuration of the device complies with the ITOPS, Security Technical Implementation Guide (STIG) for Recordable Mobile Devices (Audio Files Only).

3 Assessed by ITOPS Security Engineering.

4 Encrypted with FIPS 140-2 (or successor) validated encryption.

The following voice recorders have been assessed for use by ITOPS Security Engineering:

1 Olympus 9500 Digital Voice Recorder

2 Philips Pocket Memo Voice Recorder DPM 8000

SOURCE: Security Engineering Research Analysis (SERA) Documents

Voice recorders that have not been assessed by ITOPS Security Engineering must be submitted for assessment before the device can be used in VA research. Device assessment requests can be submitted using the Request New Product/Technology Review process.

If the voice recorder comes with pre-installed software, the software is required to be evaluated by the Technical Reference Model (TRM). Before submitting the software to TRM for approval, the requestor should verify that the software is not already approved for use by checking the TRM Technology/Standard List.

If the software Is not approved on the TRM Technology/Standard list, the software can be submitted to TRM for assessment using the Content Request Form.

Users should pay special attention to the "Decision" tab of the TRM Technology/Standard List. This tab discusses the decision, constraints on the use of the software and the software versions that are approved for use in VA.

(c) **Digital Cameras** Digital cameras are required to meet the following requirements:

1 Accounted for on a VA EIL.

2 Use and configuration of the device complies with the ITOPS Security Technical Implementation Guide (STIG) for Recordable Mobile Devices (Camera – Photo/Video/Audio).

If the camera comes with pre-installed software, the software is required to be evaluated by the Technical Reference Model (TRM). Before submitting the software to the TRM for assessment, the requestor should verify that the software is not already approved for use by checking the TRM Technology/Standard List.

If the software Is not approved on the TRM Technology/Standard list, the software will need to be sent to the TRM for assessment. The requestor will need to submit a "Content Request Form" to begin this process.

Users should pay special attention to the "Decision" tab of the TRM Technology/Standard List. This tab discusses the decision, constraints on the use of the software and the software versions that are approved for use in VA.

(d) **Portable storage devices** Portable storage devices are information system components that can be inserted into and removed from an information system and that are used to store data or information. Portable storage devices include CDs/DVDs, external hard disk drives, USB flash drives and flash memory cards. VA portable storage devices are required to meet the following requirements:

1 Encrypted with FIPS 140-2 (or successor) validated encryption. If not technically possible to encrypt a portable storage device, the ISSO will inform the PI or designee that documented justification for using the unencrypted device is required and must be reviewed and approved by the local ISO and Area Manager. The Deputy Assistant Secretary (DAS) for OIS or designee must also review/approve devices that cannot be encrypted using FIPS 140-2 (or its successor) validated encryption. The local ISSO will maintain the original and a copy of the document will be provided to the CIO.

The unencrypted mobile device vulnerability must also be documented in a Plan of Action and Milestone (POA&M), in accordance with the OIT Plan of Action and Milestones (POA&M) Management Guide. This will denote the deviation from policy and will request risk acceptance from the Authorizing Official (AO) and Authorizing Official Designated Representative (AODR). **SOURCE**: Information Security Knowledge Service Security Control AC-19.

2 Accounted for on a VA EIL.

3 Listed on the FIPS 140-2 Validated Removeable Storage Devices list.

(e) **Securing mobile and portable storage devices**

Mobile and portable storage devices must be secured when not in use. Below are some examples of how to secure these devices when not in use.

1 Stored in a locked cabinet in the principal investigators (PI's) office, with access to the locked cabinet limited to research study personnel.

2 Stored in the PI's office, with access to the office limited to research study personnel.

3 Stored in a locked cabinet in room 444, 4th floor research lab, with access to the locked cabinet limited to the PI.

(f) **Data Backups**

VA mobile and portable storage devices cannot contain the only copy of VA information. A backup of the information on the device must be created at regular intervals and stored securely. For help with

backing the information for these types of devices, submit a "YourIT" ticket to your local ITOPS staff for assistance.

(g) **Mobile Applications**

The implementation of mobile technology applications must be reviewed and approved by the VA Mobile Device Management (MDM) team. A request for a mobile application assessment must be submitted to the MDM team for inclusion in the TRM. The TRM will then publish decisions for mobile technologies. If the technology in question can be downloaded on a computer as a separately installable component, the TRM will conduct an assessment of the computer installable version of the technology only. For example, software such as iTunes would be assessed because it can be downloaded on a computer.

To verify if a mobile application is approved for use in the VA, check the VA APP Store for apps created for Veterans and Healthcare Professionals and the MDM approved apps list. If the mobile application is not listed on either of the approved lists, the application must be submitted for review and approval.

If the mobile application has been already developed, submit the mobile application to MDM using the instructions on the MDM SharePoint site.

If a new mobile application will be developed, the requestor must submit a VIPR request during the initial planning stage of the mobile application development. There are several VIPR processes on the AMO SharePoint site. Select the process in the "Mobile Application Development" section for "VIPR Request for Mobile App Development".

(2) **Use Case Scenario** Dr. Taylor has a research study that will utilize a standalone research scientific computing device to analyze tissue samples. Because the device is standalone and not on the VA network, Dr. Taylor will need to create a process for backing up the data.

Dr. Taylor decides the best course of action is to use a VA-issued USB flash drive to transfer the data to VA network folder on a weekly basis. Following local facility policy, Dr. Taylor submits a request to local ITOPS staff for a VA-issued USB flash drive. The local ITOPS Area Manager approves the USB flash drive, issues it to Dr. Taylor and informs him that before he can begin using the device, he must complete two additional steps.

Step 1 - In order to connect the USB flash drive to the VA network, Dr. Taylor will need to submit an "Enterprise Device Control Waiver Request" using the OIT Electronic Permission Access System (ePAS). Dr. Taylor submitted the request and has received approval to connect the USB flash drive to the VA network.

Step 2 - Following local policy, Dr. Taylor has created a network folder for the data and has employed the principle of least privilege by requesting local ITOPS staff restrict access to the folder to research study staff.

(3) **ERDSP Questions**

(a) **Question 1 - Select the types of VA mobile and portable storage devices that will be used in the research study. (CM-8/AC-19)**

For this question, select all VA mobile and portable storage devices that will be used in the research study. If a mobile device is not listed, select "Other" and provide the type of device in the space provided in the following question.

(b) **Question 2 - Provide the make, model, EE number for each VA mobile device. (AC-19/CM-8)**

For this question, provide the make, model, and EE number for each VA device. If "Other" is selected in Question 1, provide the type, make, model and EE number for the device.

(c) **Question 3 - Are all VA mobile and portable storage devices encrypted with FIPS 140-2 (or successor) validated encryption? (AC-19.E05/SC-28)**

For this question, answer "Yes" if all VA mobile and portable storage devices including CDs/DVDs, have FIPS 140-2 (or its successor) validated encryption. Otherwise, answer "No" and provide justification in the text box for not encrypting the device.

(d) **Question 4 - Will the research study data stored on VA mobile and portable storage devices be backed up on a regularly scheduled basis? (AC-19/CP-9)**

For this question, answer "Yes" if research study data stored on mobile, portable storage, or IoT devices will be backed up on a scheduled basis. Answer "No" if data will not be backed up on a scheduled basis and provide justification in the response to the next question.

(e) **Question 5 - Describe the process for backing up user level data stored on mobile and portable storage devices and the frequency for such backups. (AC-19/CP-9)**

For this question, describe the process to back up research study mobile, portable storage or IoT devices. If the data cannot be backed up, please provide a detailed justification.

(f) **Question 6 - Describe the process for securing mobile and portable storage devices when not in use. (PE-2/PE-4/PE-5)**

For this question, describe the process for securing each mobile device when not in use.

(g) **Question 7 - Will the research study use any mobile applications? (SA-11)**

For this question, answer "Yes" if a VA mobile application will be used in the research study. Otherwise, answer "No" and proceed to the next question.

(h) **Question 8 - Provide the name of the mobile application, application owner, application download link, and purpose of the mobile application in the research study. (SA-11)**

For this question, provide the name of the mobile application, vendor name, a link to the mobile app's website and the purpose of the mobile app in the research study.

(i) **Question 9 - Has the mobile application been approved for use in the VA? (SA-11/SC-18)**

For this question, answer "Yes" if the app has been approved for use in the VA or "No" if the app has not been approved for use in the VA.

(4) **ISSO Review Requirements**

(a) The ISSO will verify that all VA mobile devices and portable storage devices used in the study are on a VA-approved list. If a device is not on a VA-approved list, the ISSO should document in the study review the requirement for the study team to submit the device for evaluation and approval before it can be used in VA research.

(b) The ISSO will verify that each VA mobile device used in the research study has a VA EIL EE number listed on the ERDSP. If a device does not have a VA EIL EE number, the ISSO should instruct the PI to contact logistics service or the appropriate POC to have the device added to the appropriate EIL.

(c) The ISSO will verify that there is an acceptable plan in place to back up research study data stored on mobile devices.

(d) The ISSO will verify that any VA mobile applications used in the research study have been approved for use in the VA.

(e) If not technically possible to encrypt a mobile device or portable storage device, the ISSO will inform the PI or designee that documented justification for using the unencrypted mobile device is required and must be reviewed and approved by the local ISO and Area Manager. The Deputy Assistant Secretary (DAS) for OIS or designee must also review/approve VA mobile devices that cannot be encrypted using FIPS 140-2 (or its successor) validated encryption. The local ISSO will maintain the original and a copy of the document will be provided to the CIO.

The unencrypted mobile device vulnerability must also be documented in a Plan of Action and Milestone (POA&M), in accordance with the OIT Plan of Action and Milestones (POA&M) Management Guide. This will denote the deviation from policy and will request risk acceptance from the Authorizing Official (AO) and Authorizing Official Designated Representative (AODR). **SOURCE**: Information Security Knowledge Service Security Control AC-19.

h. Section 7: VA Software

(1) Guidance

If software will be purchased or acquired for installation on a VA network-connected device, the software must be approved by the Technical Reference Model (TRM). Per TRM FAQ Questions 18 and 26; the TRM will only assesses commercial-off-the-shelf (COTS) software products that will be used on the VA production network (network connected). If the software to be purchased or acquired will be installed on a (1) standalone IT system, or (2) a medical device (standalone or installed on a medical device VLAN or (3) a research scientific computing device (standalone or installed on the a research scientific computing device VLAN, the software is not required to be assessed by the TRM. **SOURCE**: TRM FAQ Questions 18 and 26.

If the software being purchased or acquired for the research study is not on the TRM technology/standard list, but will be installed on a network connected device, it must be assessed by the TRM. Requests for a TRM assessment of new software are submitted via the TRM Content Request Form.

It is highly recommended that researchers utilizing TRM-approved software review the "Decision" tab of the software entry in the TRM Technology/Standard List. The decision tab will supply details on any constraints imposed on the use of the software.

Software costing $5,000 or more must be accounted for in the proper automated inventory system, by indicating the proper equipment entry (EE) number and inventoried annually. Software licenses will be tracked and accounted for by the appropriate Program Manager for whom the software was originally purchased. **SOURCE:** VA Handbook 7002, Part 4, paragraph 4.b.

(2) ERDSP Questions

(a) Question 1 - Will any software be purchased or acquired for use within this research study? (CM-10)

For this question, answer "Yes" if any new software will be purchased for this research study, regardless of software ownership. Otherwise, answer "No" and proceed to the next question.

(b) **Question 2 - Is the software approved for use in the VA Technical Reference Model (TRM)? (CM-8)**

For this question, answer "Yes" if the software being purchased or acquired for this research study is listed on the TRM Technology/Standard List. If the software is not on the TRM Technology/Standard List, select "No". If the software will be installed on a standalone system, TRM approval is not required.

(c) **Question 3 - Provide the name of the software, vendor, vendor website address, and the purpose of the software. (CM-10)**

For this question, provide the name of the software and the software vendor, as well as the vendor website address. Additionally, describe in detail the purpose of the software and how it will be used in the research study.

(3) **ISSO Review Requirements**

The ISSO will verify that software purchased or acquired for installation on a VA network-connected device is approved by the TRM.

i. Section 8: Agreements and Authorizations

(1) **Guidance**

VA research studies may involve the use of agreements and authorizations. Below are the most common types of agreements and authorizations used.

(a) **Contracts** VA contracts with external entities (non-VA entities) will follow the guidance in VA Handbook 6500.6. Questions concerning the contracting process should be directed to your local VA Contracting Office. Questions concerning the "Checklist for Information Security in the Initiation Phase of Acquisitions" or "contract security language" should be directed to your local ISSO. If questions concerning the VA Handbook 6500.6, "Checklist for Information Security in the Initiation Phase of Acquisitions" or "contract security language" cannot be resolved at the facility level, they should be elevated to the Business Requirements Division for assistance.

(b) **Cooperative & Development Agreement (CRADA)** CRADA defines the responsibilities and obligations of each partner in conducting collaborative research and development and provides the collaborating parties with rights to any patentable invention made by a Federal employee in the performance of the agreement.

For additional information on CRADAs, see VHA Directive 1206 and ORD SOP "Submitting CRADA Amendments to OGC Specialty Team Advising Research (STAR)". ORD CRADA templates are located on the "Office of Research & Development Forms, Templates and Model Agreements" page.

(c) **Data Use Agreement (DUA)** A DUA is an agreement that (a) governs the sharing of data between a data owner and requestor; (b) defines ownership as related to the data exchange; (c) establishes the specific terms of use and disclosure for the requestor; (d) provides a means to transfer liability for the protection of the data to the Requestor; (e) Is considered "internal' if the requestor is within the VA, and "external" if requestor is outside the VA; (f) serves as a means to establish criteria for using, disclosing, storing, processing and disposing of data; and (g) satisfies HIPAA requirements when providing information within a limited data set (LDS).

ORD is revising the research DUA templates. Until the revised templates are released, researchers should follow the guidance in VHA Handbook 1200.12. If assistance is needed with a DUA, research study staff should contact ORD regulatory.

(d) **HIPAA Authorization** A written authorization signed by the individual, to whom the information or record pertains, for the release of individually identifiable information. **SOURCE**: VHA Directive 1605.01, paragraph 13.

(e) **Material Transfer Agreement** A Material Transfer Agreement (MTA) is a legally binding agreement that is used when biospecimens are shared or transferred. An MTA defines the rights and obligations of the providers and recipients of the biospecimens. **SOURCE:** Draft ORD Guidance on Material Transfer Agreements.

(2) **ERDSP Questions**

(a) **Question 1 - Will the research study have any agreements, authorizations or contracts? (AC-21)**

For this question, answer "Yes" if the research study will utilize any types of agreements or contracts. Otherwise, answer "No" and proceed to the next question. If your agreement is not listed, select "Other" and provide information about your agreement in the comment field. You can also use the comment field to explain or add details about your agreements.

(b) **Question 2 - Select the agreements that will be used in the research study. (AC-21)**

For this question, select each type of agreement or contract that will be used in the research study.

(c) **Question 3 - Describe the purpose of each agreement or contract and provide the names of each entity involved in the agreement or contract. (AC-21)**

For this question, describe the purpose of each agreement or contract and provide the name of each party involved in the agreement or contract.

(3) **ISSO Review Requirements.**

(a) The ISSO will review any research study contracts in accordance with VA Handbook 6500.6.

(b) The ISSO will review the data transmission method listed in the DUA for transferring research study data to the requestor. The ISSO will verify that the data transfer method is commensurate with the classification of the data (e.g.; VA sensitive information must be encrypted in transmission with FIPS 140-2 (or successor) validated encryption).

(c) The ISSO will ensure system interconnections used in the research study are documented and approved in accordance with Enterprise Security External Change Council (ESECC) procedures.

j. Section 9: External Information Systems and Data Sharing with External Entities

(1) Guidance

(a) **External Information Systems** External information systems are information systems or components of information systems that are outside of the authorization boundary established by the VA and for which the VA typically has no direct supervision nor authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to:

1 Personally owned information systems or devices. These types of devices include personal computers, notebook computers, smart phones, tablets, personal digital assistants, hotspots, external hard disk drive and USB flash drives;

2 Privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, shopping malls or airports);

3 Information systems or devices owned or controlled by non-Federal Government organizations (e.g., affiliate, collaborator, contractor, consultant and sponsor information systems);

4 Federal information systems or devices that are not owned, operated or under the direct supervision and authority of the VA (e.g.; National Institutes of Health (NIH), Health and Human Services (HHS), National Cancer Institute (NCI)).

External information systems (e.g.; sponsor, affiliate and collaborator information systems) and devices are not allowed to collect, process or store VA data unless the system has been evaluated and received a VA ATO determination. If the information system is required to undergo the VA assessment and authorization process and obtain a VA ATO, the system cannot be used until the AO

has granted a VA ATO. **SOURCE**: IS Knowledge Service Security Control SA-9 and VA Handbook 6500.3.

(b) **Personally owned information systems**. Personally owned information systems (capable of storing data) may not be used onsite at a VA facility to directly connect to VA's network. Use of personally owned information systems on-site to perform assigned official duties must be approved by the Information System Owner, local CIO, or designee. **SOURCE**: IS Knowledge Service Security Control AC-20.

(c) **Sponsor and collaborator provided information systems, applications and devices**.

1 Sponsor and collaborator information systems, applications and devices can be used to collect study data from a VA research subjects, if the subject has executed a written HIPAA authorization for disclosure of their data to the sponsor or collaborator and absent an agreement that restricts the affiliates or other entity's further use or disclosure of the information (e.g., Contract, MOU, MOA, or Data Use Agreement); ownership of the disclosed data transfers to the recipient and VA cedes control over the information.".

There should be a process in-place for the VA researchers to download a copy of the information provided by each VA subject to the sponsor or collaborator. The information must be retained in accordance with VHA Record Control Schedule (RCS) 10-1.

2 Sponsor and collaborator provided information systems and applications can be used by the VA to transfer a copy of research study data to a sponsor or collaborator if the subject has executed a written HIPAA authorization for disclosure of their data to the sponsor or collaborator and absent an agreement that restricts the affiliates or other entity's further use or disclosure of the information (e.g., Contract, MOU, MOA, or Data Use Agreement); ownership of the disclosed data transfers to the recipient and VA cedes control over the information." When the VA discloses a copy of research study data, the VA discloses a copy of the research study data and retains the original in accordance with VA records control schedule (RCS) 10-1.

Per VHA Directive 1605.01: "If a research subject properly executes a written authorization for disclosure of his or her protected health information to an affiliate institution or other entity, transfer of the information constitutes a "disclosure" under the Privacy Act and HIPAA Privacy Rule. Depending on the agreement between the transferring facility and the receiving entity, VA may or may not retain data ownership. Absent an agreement that restricts the affiliates or other entity's further use or disclosure of the information (e.g., Contract, MOU, MOA, or Data Use Agreement); ownership of the disclosed data transfers to the recipient and VA cedes control over the information." **SOURCE**: VHA Directive 1605.01, paragraph 13.a.(12).

3 Sponsor and collaborator information systems and applications collecting, processing or storing VA-owned data must be evaluated and receive a VA ATO determination before the system

can be used in VA research. If the determination requires the information system or application to undergo the VA assessment and authorization process and obtain a VA ATO, the system cannot be used in VA research until the AO has granted a VA ATO. **SOURCE**: IS Knowledge Service Security Control SA-9 and VA Handbook 6500.3.

- Software as a Service (SaaS) cloud-based applications are submitted for an ATO determination through the SaaS inquiry form process. The request will be routed to the Project Special Forces (PSF) team who will schedule a meeting with the requestor to discuss the use of the application in the research study. Based on the information provided by the requestor, the PSF team will make an ATO determination. It should be noted that the ATO process is lengthy (12-24 months) and is costly for both the VA and application owner. **SOURCE:** OIT Software as a Service OIT Software as a Service page.

- Non-SaaS information systems are submitted for an ATO determination through the Governance Risk and Compliance (GRC) committee SharePoint. The request will be routed to the GRC committee who will schedule a meeting with the requestor to discuss the use of the information system in the research study. Based on the information provided by the requestor, the GRC committee will make an ATO determination. It should be noted that the ATO process is lengthy (12-24 months) and is costly for both the VA and information system owner.

4 Sponsor and Collaborator Provided Mobile Applications

If a sponsor- and collaborator-provided mobile application will be installed on a VA mobile device, the mobile application must be submitted to the Mobile Technology and Endpoint Security Engineering for evaluation and approval. The instructions for submitting a mobile application for review and approval can be found on the Mobile Technology and Endpoint Security Engineering SharePoint, under "mobile application intake process".

(d) Sponsor and collaborator e-consent applications

1 Remote Informed Consent Sponsor- or collaborator-provided e-consent applications can be used to obtain remote informed consent from VA research subjects if the following conditions are met:

- The research study participant has executed an authorization for the disclosure of their data to the sponsor or collaborator;

- The e-consent application meets FDA 21 CFR, part 11 signature requirements;

- The e-consent application allows VA researchers to download copies of completed informed consent forms;

- The use of the e-consent application is approved by VHA CO ORD Regulatory.

2 **In-Person Informed Consent** The subject completes and signs the informed consent electronically in the presence of research study staff. This is generally done using a sponsor or VA tablet or laptop during a study visit.

Sponsor and collaborator provided e-consent applications can be used to obtain in-person informed consent if the following conditions are met:

- The research study participant has executed an authorization for the disclosure of their research study data to the sponsor or collaborator;

- The e-consent application allows VA researchers to download copies of completed in-person informed consent forms.

(e) **Affiliate IT equipment, medical and scientific computing devices**

1 Affiliate IT equipment, medical devices and scientific computing devices used in a VA research project at a VA facility must be accounted for on a VA EIL. Per VA handbook 7002;

"Equipment owned by an affiliated institution or purchased by such institution from grant funds to be used by a VA investigator in a research project at a VA installation will be accounted for in the appropriate VA property accountability system regardless of cost of the equipment. The investigator or designee responsible for all such equipment will maintain a jacket file on the equipment." **SOURCE:** VA Handbook 7002, Part 11, paragraph 3.

2 If a research study will use an affiliate-provided medical or scientific computing device that will be connected to the VA network, the device must undergo a risk assessment. Guidance for submitting the risk assessment can be found on the System Security Support Risk Analysis Portal under the "Research Scientific Computing Devices (RSCD)" column. Additional Enterprise Risk Analysis (ERA) submission and requirement information can found in the ERA Joint User Guide.

(f) **Commonly used external information systems and applications.**

1 Electronic Case Report Form (eCRF) application

2 Electronic Data Capture (EDC) System

3 Electronic Clinical Data Management System (eCDMS)

4 Electronic Clinical Trial Management System (eCTMS)

5 eConsent Applications

6 Interactive Web Response System (IWRS)

7 Interactive Voice Response System (IVRS)

8 Electronic Patient-Reported Outcomes (ePRO) application

9 Survey/Questionnaire Applications

10 Electronic IRB (eIRB) Human Subject Application System

11 Non-VA REDCap Applications

12 Affiliate/Sponsor Information Systems

(d) **Approved methods to transfer sensitive data to an external entity (non-VA)**

1 **Sponsor, Collaborator, Vendor Information Systems or Applications**

The information system or application must encrypt sensitive data in transmission from the VA client to the information system or application using FIPS 140-2 (or successor) validated encryption.

2 **Azure Rights Management System (RMS)**

Azure RMS is the protective technology used by Azure Information Protection. It uses encryption, identity and authorization policies to help secure file attachments and email. Information can be protected both within the VA and outside the VA because the protections remain with the data, even when it leaves the VA. VA OI&T has issued a set of Frequently asked questions (FAQs) about Azure RMS use within the VA and the Office of Research and Development has issued ORD FAQs for the use of Azure RMS in VA research.

3 **VA-Encrypted USB Flash Drive or External Hard Disk Drive**

- The device must be encrypted with FIPS 140-2 (or successor) validated encryption.
- The device must be on the OIT Mobile Technology and Endpoint Security Engineering Approved Devices and Apps list.
- The device must be accounted for on a VA Equipment Inventory List.

4 **CD/DVD**

- CDs/DVDs must be encrypted with FIPS 140-2 (or successor) validated encryption unless exempted by VA Directive 6609, paragraph 2.i.

- The password to the CD/DVD must be transmitted separately from the CD/DVD.

- The CD/DVD must be shipped via a secure delivery service that tracks the mail from pickup to delivery. **SOURCE**: VA Directive 6609, paragraph 2.i.and OIS Knowledge Service, Security Control AC-19.

5 **FAX**

Care should be taken to assure confidentiality when faxing sensitive information. Facilities must take reasonable steps to ensure that the fax transmission is sent to the appropriate destination. Before sending a fax, users should review the FAX guidelines in the IS Knowledge Service Security Control SC-8, control level guidance section.

6 **Physical Transport**

Individuals physically transporting sensitive information outside of controlled areas must obtain written approval from their supervisor, PO, system owner and/or designee and the local ITOPS Area Manager. The approval applies to sensitive hard copy (paper) media and electronic media containing sensitive information (e.g.; laptops, tablets, CDs/DVDs, USB flash drives, external hard disk drives, SD cards, etc.) transported outside of controlled areas. **SOURCE**: OIS Knowledge Service Security Control MP-5.

(e) **Approved methods to transfer non-sensitive VA data to an external entity**

1 Unencrypted email

2 USPS or other delivery service (FedEx, UPS)

3 Any of the methods used for sensitive data

(f) **Information Systems within VA facilities without a VA ATO (AC-20)**

Information systems within VA facilities without a VA ATO cannot be used to collect, process or store VA research data. These information systems include affiliate wired and wireless information systems and internet service provider (ISP) wired and wireless information systems with VA facilities. Information systems residing within VA facilities must be accounted for on the External Connections Compliance Tracking System.

Information systems within VA facilities without a VA ATO can be used by research staff to access research informational websites, research journals, research publications, and other publicly available information.

The patient wireless system within each VA facility cannot be used to transmit, process or store VA research data. This system is for patient use only.

Questions concerning these types of information systems within your facility should be directed to the facility ISSO or local ITOPS Area Manager.

Use Case Scenario #1**:** The Atlanta VA Medical Center is participating in a collaborative research study with Emory University. The Emory University REDCap system will be used to electronically survey both VA and Emory research participants and each VA subject will execute an authorization for the disclosure of their data to Emory University. The study will not have any additional agreements that restricts Emory's use of the data.

In this use case, the data disclosed by VA study participants to Emory is not owed by the VA; therefore, the Emory University REDCap system is not subject to VA security requirements.

Use Case Scenario #2: The Miami VA medical center will be conducting a collaborative research study with the Tampa and Bronx VA medical centers. The study requires VA research subjects to complete weekly surveys and the use of an electronic survey application is preferable over paper-based surveys. The study teams decide to use the Vanderbilt University REDCap system to collect the surveys since the VA REDCap system cannot be used to survey VA research subjects due to limitations on its capability. Each VA subject will execute an authorization for the disclosure of their data to Vanderbilt University.

In this use case, the Vanderbilt University REDCap system will need to be evaluated for a SaaS ATO before the system can be used in VA research. Vanderbilt University is not a collaborator on the study, but instead is acting as a 3rd party and is collecting data on behalf of the VA. The data collected by the Vanderbilt REDCap system is considered VA data.

Use Case Scenario #3: The Palo Alto VA Medical Center will be conducting a study that requires study participants to receive weekly medication reminders. This capability is currently not available in the VA and the study team decides to contract with an outside vendor to provide the weekly reminders. Each VA subject will execute an authorization for the disclosure of their data to the vendor.

In this use case, the vendor application will need to be evaluated for a SaaS ATO before the system can be used in VA research. The vendor is not a collaborator on the study, but is acting as a 3rd party and is collecting data on behalf of the VA. The data collected by the vendor application is considered VA data.

(2) **ERDSP Questions**

(a) **Question 1 - Will any research study data be transmitted or transferred to an external entity? (AC-21)**

For this question, answer "Yes" if research study data will be transmitted or transferred to an external entity, regardless of data ownership or data classification (sensitive/non-sensitive). Otherwise, answer "No" and proceed to the next question.

(b) **Question 2 - Provide the name of the external entity(s) and describe the method used to securely transfer the research study data. (AC-21)**

For this question, provide the name of each external entity research study data will be transferred to and the method used to transfer the data. If the transfer method is an information system or application, provide the URL (web address).

(c) **Question 3 - Will VA retain ownership of the research study data shared with the external entity? (AC-20)**

For this question, answer "Yes" if the VA will retain ownership of the data shared with the external entity. Otherwise, answer "No" and proceed to the next question.

(d) **Question 4 - Will the research study utilize any external information systems or devices? (AC-20)**

For this question, answer "Yes" if research study data will be collected, processed and/or stored on an external information system. Otherwise, answer "No" and proceed to the next question.

(e) **Question 5 - Who owns the data being collected, processed, analyzed or stored on the external information system?**

For this question, provide the name of the owner of the research study data collected, processed, analyzed or stored on the external information system.

(f) **Question 6 - Select the type of external information system or application that will be used in the research study. (AC-20)**

For this question, select the type of external information system or application that will be used in the research study. If "Other" is selected, provide the type of external information system the next question.

(g) **Question 7 - Provide the name, web address and purpose of each external information system or application used in the research study (AC-20)**

For this question, provide the name of the external information system and the web address of the system and describe what the system will be used for in the research study (e.g.; The Janssen COVID-19 clinical trial will use a Rave Medidata eCRF to collect a copy of VA research study data disclosed to the sponsor. The eCRF web address is https://login.imedidata.com/login)

(h) **Question 8 - Will any external entity provided mobile, portable storage, medical or research scientific computing devices be used in the research study? (AC-20)**

For this question, answer "Yes" if an external entity provided mobile, portable storage, IoT, medical or research scientific computing device will be used in the research study. Otherwise, answer "No" and proceed to the next question.

(i) **Question 9 - Select the type of external entity provided mobile, portable storage, medical or research scientific computing device(s) that will be used in the research study. (AC-20)**

For this question, select the types of devices that will be used in your research study (select all that apply). If "Other" is selected, provide the details for the "Other" information system in the next question.

(j) **Question 10 - Provide the make, model, owner and purpose of each external entity provided mobile, portable storage, medical and research scientific computing devices used in the research study. (AC-20)**

For this question, provide the make, model, owner and purpose of each eternal external entity-provided device used in the study and include the purpose of each device.

(k) **Question 11 - Will the research study use any affiliate provided mobile, portable storage, medical, research scientific computing devices or laptops at a VA facility? (AC-20)**

For this question, answer "Yes" if affiliate laptops, mobile, medical or research scientific computing devices will be used in the research study and located at a VA facility. Otherwise, answer "No" and proceed to next question.

(l) **Question 12 - Will the research study use any external entity provided mobile applications? (AC-20)**

For this question, answer "Yes" if the research study will use an external entity provided mobile application in the research study. Otherwise, answer "No" and proceed to the next question.

(m) **Question 13 - Provide the name of the mobile application, entity providing or creating the mobile application, website to download the application and the purpose of the application in the research study. (AC-20)**

For this question, provide the name of the mobile application, the name of the organization or vendor creating or providing the mobile application, the website to download the mobile application and the purpose of the mobile application in the research study.

(3) ISSO Review Requirements.

(a) The ISSO will verify that external information systems and applications used in the research study are not collecting, processing or storing VA data, unless the system or application has a VA ATO.

(b) The ISSO will verify that the information system owner, local ITOPS area manager or designee has approved (in writing) the use of personally owned information systems or devices.

(c) The ISSO will verify sensitive data transmitted electronically outside of the VA, regardless of ownership, is encrypted in transmission with FIPS 140-2 (or its successor) validated encryption.

The ISSO will use the external web portal guidance on the RSD SharePoint to verify the encryption of sensitive data in transmission or the ISSO can submit the website to RSD for review, using the RSD eCRF Web Portal Tracker.

(d) If the research study will use a information systems within VA facilities without a VA ATO, the ISSO will inform the PI that the network cannot be used to transmit, collect, process or store VA research data.

k. Principal Investigator or Designee Signature

The PI or designee is required to sign the form once it has been completed.

l. Research Study Contacts

Enter the required fields for the following POCs:

"Information System Security Officer"

1. Name
2. E-Mail Address
3. Phone Number
4. Facility Location

"Principal Investigator"

1. Name
2. E-Mail Address
3. Phone Number
4. Facility Location

“Research Study Coordinator”

1. Name
2. E-Mail Address
3. Phone Number
4. Facility Location

Appendix A – Definitions

Authorization to Operate (ATO). The official management decision, given by a senior organizational official, after completing a security assessment, to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. **SOURCE:** NIST SP 800-37

Authorizing Official (AO). A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. In the VA, this is the VA CIO. **SOURCE:** VA Handbook 6500.3.

Azure Rights Management System (RMS). Azure Rights Management Services (RMS) is an information protection technology that works with Azure RMS-enabled applications to help safeguard business information from unauthorized use—both online and offline and, inside and outside the VA environment. Utilizing proven security technologies—including RSA 2048-Bit encryption, certificates, modern 0authentication, and authorization policies—Azure RMS helps the VA create reliable information protection solutions. Azure RMS augments the VA's security strategy by providing protection of information through persistent usage policies, which remain with the information, no matter where the information it goes. This helps the VA prevent sensitive information from getting into the wrong hands, either accidentally or intentionally. **SOURCE**: Azure Rights Management Services (RMS) Frequently Asked Questions (FAQs).

Commercial IRB. A commercial IRB is an IRB that is external to a university or research institution that provides services for academic and non-academic researchers. Commercial IRBs and university-based IRBs must comply with the same federal regulations governing research with human participants. **SOURCE:** ORD Guidance on the use of Commercial IRBs

Cooperative Research and Development Agreement. A Cooperative Research and Development Agreement (CRADA) is an agreement established pursuant to 15 U.S.C. 3710a between the VA and one or more non-Federal parties under which VA may accept, retain, and use funds, personnel, services, facilities, intellectual property, equipment or other resources from the other party, as well as provide personnel, services, facilities, intellectual property, equipment or other resources, excluding funding, toward the conduct of specified research and development that is consistent with the VA's mission. **SOURCE**: VHA Directive 1200.01.

Collaborative Research. Collaborative Research is a research collaboration involving investigators from the VA and other institutions, with VA investigators having a substantive role in the design, conduct, and/or analysis of the research. **SOURCE:** VHA Directive 1200.01.

External Entities: Organizations that are outside of the VA, such as other government agencies, private industry organizations, and the general public. Internal VA administrations (Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA)) are not considered external entities. **SOURCE:** VA Handbook 6517.

External Information Systems. External information systems are information systems or components of information systems that are outside of the authorization boundary established by the VA and for which the VA typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to:

- Personally owned information systems (e.g., computers, smartphones, tablets, or personal digital assistant);
- Privately-owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, shopping malls, or airports);
- Information systems owned or controlled by non-Federal Government organizations (such as VA affiliate's information systems); and
- Federal information systems that are not owned, operated, or under the direct supervision and authority of the VA. **SOURCE:** IS Knowledge Service Security Control AC-20.

Individually Identifiable Information. Individually identifiable information is any information pertaining to an individual that is retrieved by the individual's name or another unique identifier, as well as individually identifiable health information regardless of how it is retrieved. Individually identifiable information is a subset of personally identifiable information (PII) and is protected by the Privacy Act. **SOURCE:** VHA Directive 1605.01

Information System (IS): An information system (IS) is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. **SOURCE:** NIST SP 800-53

Internet of Things (IoT). Manufacturers are creating an incredible variety and volume of internet-ready devices broadly known as the Internet of Things (IoT). Many of these IoT devices do not fit the standard definitions of information technology (IT) devices that have been used as the basis for defining device cybersecurity capabilities (e.g., smartphones, servers, laptops). The IoT devices in scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-term Evolution [LTE], Zigbee and/or, Ultra-Wideband ([UWB)]) for interfacing with the digital world. The IoT devices in scope for this publication can function on their own, although they may be dependent on specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some

functionality. Many IoT devices have computing functionality, data storage, and network connectivity along with functionality associated with equipment that previously lacked these computing functions (e.g., smart appliances). In turn, these functions enable new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also enable the collection and analysis of data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events. **SOURCE**: NISTIR 8259.

Medical Device. A medical device/system is defined as any device or system that meets any of the following requirements:

- Is used in patient healthcare for diagnosis, treatment (therapeutic), or physiological monitoring of patients. This includes server-based medical equipment and clinical systems. Examples of medical devices/systems include, but are not limited to, physiological monitoring systems, ventilators, infusion pumps, Computed Tomography (CT) scanners, MUSE cardiology information system, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS), and laboratory analyzers. Medical devices directly connect directly to the patient; process human and other biologic specimens, create medical images, display electrophysiological waveforms, obtain physiologic measurements, or directly perform provide therapeutic support directly to the patient.

- The device/system has gone through the Food and Drug Administration's (FDA's) Premarket Review or 510k Process.

- Is incorporated as part of a medical device system in such a fashion that if modified, the device or system component could have a negative impact on the functionality or safety of the main medical device/system.

SOURCE: VA Directive 6550.

Mobile Device. Mobile devices are essentially general-purpose computing platforms. They are not restricted to performing one operation and can instead be used in many different domains—including medical, industrial and entertainment. A mobile device is defined as a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. (e.g.; smart phones, smart watches, tablets, video recorders, cameras, e-readers, handheld gaming consoles, audio recorders). **SOURCE:** NIST SP 800-53

Office of Information Security (OIS) Knowledge Service (KS): The VA's knowledge portal for providing cybersecurity policies, procedures, and guidance. **SOURCE**: VA Directive 6500.

Portable Storage Device. Portable storage devices are an information system components that can be inserted into and removed from an information system, and that are used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks (CDs/DVDs), USB flash drives, external hard disk drives, and flash memory cards (SDs). **SOURCE:** NIST SP 800-53

Protected Health Information. The HIPAA Privacy Rule defines protected health information (PHI) as individually identifiable health information transmitted or maintained in any form or medium by a covered entity, such as VHA. **NOTE:** VHA uses the term protected health information to define information that is covered by HIPAA but, unlike individually identifiable health information, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. PHI excludes employment records held by VHA in its role as an employer, even if those records include information about the health of the employee obtained by VHA in the course of during the employment of the individual. **SOURCE:** VHA Directive 1605.01.

Research Scientific Computing Device. A research scientific computing device (RSCD) within the VA is defined as a standalone or network- capable system or device that cannot obtain VA- approved baseline configuration settings, and/or interfaces with scientific/clinical instrumentation in direct support of research activities and scientific studies. These systems have the purpose of ultimately contributing to healthcare services and the well-being of veterans.

• An RSCD includes instrument(s) that have an internal operating system and central processing unit used to acquire/analyze data and for indicating, measuring, and recording physical quantities, attributes, and other formulas.

• An RSCD system is a suite of hardware, software, and scientific applications, to include databases and webservers, which are physically part of and dedicated to the mission of research and/or scientific studies.

To avoid confusion between medical devices and special purpose systems (SPS): Any device that has been modified for research purposes and/or interfaces with scientific/clinical instrumentation in direct support of research activities and scientific studies, the device will be classified as an RSCD and will go through the RSCD Enterprise Risk Analysis (ERA) Process. **SOURCE:** Research Scientific Computing Devices (RSCD) FAQs.

Risk Assessment.: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other operations, and the Nation, arising through the operation of an information system. Part of risk management

incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. **SOURCE:** VA Handbook 6517.

Security Controls. The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. **SOURCE:** VA Handbook 6517

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. **SOURCE:** VA Handbook 6517

Sponsor. Sponsor means a person who takes responsibility for and initiates a clinical investigation. The sponsor may be an individual or pharmaceutical company, governmental agency, academic institution, private organization, or other organization. The sponsor does not actually conduct the investigation unless the sponsor is a sponsor-investigator. A person other than an individual that uses one or more of its own employees to conduct an investigation that it has initiated is a sponsor, not a sponsor-investigator, and the employees are investigators. **SOURCE:** FDA**.**

VA Data or VA Information. VA Data or VA information is data or information owned, in the possession of, under the control of, or collected by the VA or any entity acting for or on behalf of the VA. The data may be identifiable, de-identified, sensitive, or non-sensitive. **SOURCE:** VHA Directive 1200.01.

VA Sensitive Information and Data. VA sensitive information and data means includes all VA data, on any storage media or in any form or format, which that requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information whose that through improper use or disclosure could adversely affect the ability of an agency to accomplish its mission and safeguard, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions. **SOURCE:** VHA Directive 1200.01.

Appendix B - Research Study Agreements, Authorizations and Data Sharing

There are several different types of agreements that can be used to share VA research data. The purpose of this table is to identify the different types of agreements, associated guidance and points of contract for each agreement and the VA security requirements for data shared under these agreements.

Type of Agreement	Guidance	VA Security Requirements	POC
HIPAA Authorization	VHA Directive 1605.1, paragraph 13.a.12.	If a copy of VA research data is disclosed to a research study sponsor or collaborator under a HIPAA authorization and the VA does not retain ownership of the data, the data is not subject to VA security requirements. Per VA Directive 1605.01, paragraph 13.a.(12): "If a research subject properly executes a written authorization for disclosure of his or her protected health information to an affiliate institution or other entity, transfer of the information constitutes a "disclosure" under the Privacy Act and HIPAA Privacy Rule. Depending on the agreement between the transferring facility and the receiving entity, VA may or may not retain data ownership. Absent an agreement that restricts the affiliate's or other entity's further use or disclosure of the information (e.g., Contract, MOU, MOA, or Data Use Agreement),; ownership of the disclosed data	PO

Type of Agreement	Guidance	VA Security Requirements	POC
		transfers to the recipient and VA cedes control over the information."	
Research Data Use Agreement	VHA Handbook 1200.12	1. If a copy of VA research data is disclosed to a non-Federal entity under a data use Agreement in accordance with VHA Directive 1200.12, and the VA does not retain ownership, the data is not subject to VA security requirements. 2. If the VA retains ownership of the research data disclosed under a data use agreement (DUA), the DUA must document the terms and conditions from VHA Handbook 1200.12.	ORD
Cooperative Research and Development Agreement	VHA Directive 1605.01, paragraph 13.c VHA Directive 1206	CRADAs are required to meet the requirements of VHA Directive 1206. A Data Use Agreement (DUA) is not required to share VA sensitive information, if the research study is being conducted under a CRADA, as the protections of a DUA are built into the VA CRADA templates used by research staff.	ORD
Contract	VA Handbook 6500.6	VA contracts are required to meet the requirements of VA Handbook 6500.6.	ISSO/VA contracting
Material Transfer Agreement	Draft ORD Guidance on Material Transfer Agreements	The material transfer agreement (MTA) is required to meet the requirements of the draft ORD MTA guidance.	ORD

Appendix C – Research Study Amendment ERDSP Determination Aide

The research study amendment ERDSP determination aide is provided to assist research & development (R&D) committee members, research office staff, principal investigators (PIs), and information system security officers (ISSOs) in determining whether an amendment to a previously approved R&D committee research study requires an updated ERDSP.

If the research study amendment will only make the types of changes listed below, an ERDSP is not required for the study amendment.

Research Study Amendment ERDSP Determination Aide
Research study amendments that make minor changes to recruitment procedures, recruitment materials, or submission of new recruitment materials to be used in accordance with approved recruitment methods
Minor changes to project documents such as paper surveys, paper questionnaires, or brochures. (e.g., grammatical changes, changes in questions or information that does not affect the security of the research study)
New project documents to be distributed to or seen by participants that are similar in substance to those previously approved
Changes in payment to participants or the amount participants are paid that are not significant enough to affect the risk/benefit ratio of the project
An increase or decrease in the number and volume of participants or specimen collections
Changes to the HIPAA Authorization; except changes that affect data sharing with external collaborators or sponsors.
Change in participant population and enrollment target numbers, to include increasing the number of VA sites that will be participating in the project;

Change in risk/benefit analysis
Changes in recruitment strategy and/or participant payment procedures;
Changes in informed consent procedures or document content; except changes that affect the sharing of research study data with external collaborators or the research study sponsors.
Change in PI/SC, Co-PI/SCs, anyone serving in an investigator role, or anyone mentioned by name in the protocol, informed consent, recruitment materials, or other research study documents in which current point of contact (POC) information is essential.
Adding or removing of research study staff members

Appendix D – Minimum Security Standards

The standards in this table are intended to reflect the minimum-security requirements to protect VA research information.

Type	Security Control #	Security Requirements	Sensitive	Non-Sensitive	Public Data
Agreements and Authorizations					
Contracts	SA-9	Meet the requirements of VA Handbook 6500.6.	**Y**	**Y**	
Cooperative & Development Agreement (CRADA)	AC-21	Meet the requirements of VHA Directive 1200.06.	**Y**	**Y**	
Data Use Agreement (DUA) - Research	AC-21	Meet the requirements of VHA Handbook 1200.12.	**Y**	**Y**	
	SC-8	The ISSO must review the method used to transmit the data to the requestor to ensure the method used is commensurate with the classification of the data.	**Y**	**Y**	
Material Transfer Agreements	AC-21	Meet the requirements of the draft ORD Guidance on Material Transfer Agreements	**Y**	**Y**	
Access Control					
Electronic and Hard Copy (paper) Data	AC-6	Access to research information must be controlled and employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish	**Y**	**Y**	

		assigned tasks in accordance with organizational mission and business functions.			
Data Classification					
VA Sensitive Data (III, PII, PHI, Animal Research (Category D & E with Picture and Video), Genomic (Human), and Intellectual Property)	SC-8	Encrypted with FIPS 140-2 (or its successor) validated encryption when emailed or electronically transmitted.	**Y**		
	AC-19	Encrypted with FIPS 140-2 (or its successor) validated encryption when stored on mobile devices and portable storage Devices			
	AC-6	Access to VA data must be controlled and employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions.			
	MP-4	Hard copy (paper) data must be physical controlled and securely stored when not in use.			
	MP-5	Individuals physically transporting sensitive information outside of controlled areas must obtain written approval from their supervisor, privacy officer (PO), system owner and/or designee and ITOPS area manager.			

VA Non-Sensitive Data (Deidentified Research, Unpublished Research (Basic Animal except for category D&E with picture and video and Non-Human Basic Lab, Animal Research (Category B & C) and public data	AC-6	Access to VA data must be controlled and employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions.		**Y**	
Data Sharing					
Data shared with another VA facility.	SC-8	Sensitive data must be encrypted with FIPS 140-2 (or its successor) validated encryption when emailed or electronically transmitted.	**Y**		
	AC-19	Encrypted with FIPS 140-2 (or its successor) validated encryption when stored on mobile devices and portable storage Devices	**Y**	**Y**	
	MP-5	Individuals physically transporting sensitive information outside of controlled areas must obtain written approval from their supervisor, privacy officer (PO), system owner and/or designee and ITOPS area manager.	**Y**		

	N/A	Transmitted/transferred using any of the methods in Section 5: Data Sharing with VA Research Facilities.	**Y**	**Y**	
Data shared with a research study sponsor or collaborator	AC-21	Authorization or agreement to share the data	**Y**	**Y**	
	SC-8	Encrypted in transmission with FIPS 140-2 (or its successor) validated encryption	**Y**		
External Information Systems					
Personally owned information systems or devices	AC-20	Personally owned information systems (capable of storing data) may not be used onsite at a VA facility to directly connect to VA's network. Use of personally owned information systems on-site to perform assigned official duties must be approved by the Information System Owner, local CIO, or designee.	**Y**	**Y**	
External information systems and applications collecting, processing or storing VA data	SA-9	VA-owned data is not authorized to be collected, processed or stored on external information systems (e.g., sponsor, affiliate, contractor and collaborator information systems) unless the system has been evaluated and received a VA ATO determination. If the determination requires the external information system to obtain a VA ATO, the system cannot be used until the until the AO has granted a VA ATO. For additional guidance, see External Information Systems and Data Sharing with non-VA Entities. **SOURCE**: IS Knowledge Service Security Control SA-9 and VA Handbook 6500.3.	**Y**	**Y**	
External Information Systems and applications	AC-21	Authorization or agreement to disclose the data.	**Y**	**Y**	

used to transfer a copy of VA study data	SC-8	Data must be encrypted in transmission with FIPS 140-2 (or its successor) validated encryption	**Y**		
Sponsor or collaborator provided mobile application	AC-20	Sponsor and collaborator provided mobile applications are not required to meet VA security requirements if the data collected by the applications is not owned by the VA.	**Y**	**Y**	
Mobile applications that will be used to collect, process or store VA data	SC-18	Approved by the Mobile Device Management (MDM) team.	**Y**	**Y**	
Sponsor or collaborator provided mobile devices	AC-20	Sponsor and collaborator provided mobile devices are not required to meet VA security requirements if the data collected by the applications is not owned by the VA.	**Y**	**Y**	
	MP-4	When the mobile device is in the possession of the VA, the device must be protected and securely stored when not in use	**Y**	**Y**	
VA Mobile Applications					
Commercial-off the-shelf (COTS) applications	SC-18	Approved by the Mobile Device Management (MDM) team.	**Y**	**Y**	

New mobile application development	SC-18	Approved by the Mobile Device Management (MDM) team.	**Y**	**Y**	
VA Mobile Devices					
Mobile Devices (excludes voice recorders, video recorders, digital cameras and portable storage devices)	CM-8	Inventoried on a VA EIL	**Y**	**Y**	
	AC-19	Approved by the Mobile Device Management (MDM) team.			
	CM-7	Device software approved by TRM			
	MP-4	Protected and securely stored when not in use			
	MP-5	Encrypted with FIPS 140-2 (or its successor) validated encryption			
	MP-6	Sanitized in accordance with VA Directive 6500 and NIST SP 800-88 when the device is no longer needed.			
Voice Recorders	CM-8	Inventoried on a VA EIL	**Y**	**Y**	
	AC-19	Approved by Mobile Technology and Endpoint Security Engineering			
	CM-7	Device software approved by TRM			
	MP-4	Protected and securely stored when not in use			

	MP-5	Encrypted with FIPS 140-2 (or its successor) validated encryption			
	MP-6	Sanitized in accordance with VA Directive 6500 and NIST SP 800-88 when the device is no longer needed.			
	ITOPS STIG for Recordable Mobile Devices (Audio Files Only)	Flash memory card (SD) must remain inserted into the device with a security seal (tamper proof) placed over the SD card.			
		Reformatting the mobile audio/voice device(s) memory component(s) (HDD, flash memory card (SD) etc.) after each data transfer and limit the number of files contained on the mobile device(s) to less than 400 files per device.			
Digital Cameras and Video Recorders	CM-8	Inventoried on a VA EIL	**Y**	**Y**	
	CM-7	Device software approved by TRM	**Y**	**Y**	
	MP-4	Protected and securely stored when not in use	**Y**	**Y**	
	MP-6	Sanitized in accordance with VA Directive 6500 and NIST SP 800-88 when the device is no longer needed.	**Y**	**Y**	
	ITOPS STIG	Flash memory (SD) card must remain inserted into the device with a security seal (tamper proof) placed over the SD card. Sanitized in accordance with VA Directive 6500 and NIST SP 800-88 when the device is no longer needed.	**Y**	**Y**	

	ITOPS STIG	Reformat the mobile device(s) memory component(s) (e.g.; HDD, flash memory card) after each data transfer and limit the number of files contained on the mobile device(s) to less than 400 files per device. Flash memory (SD) card must remain inserted into the device with a security seal (tamper proof) placed over the SD card.	**Y**	**Y**	
Portable Storage Devices					
USB flash drives and external hard disk drives	AC-19	Approved by Mobile Technology and Endpoint Security Engineering	**Y**	**Y**	
	CM-8	Inventoried on a VA EIL			
	MP-4	Protected and securely stored when not in use			
	MP-6	Sanitized in accordance with VA Directive 6500 and NIST SP 800-88 when the device is no longer needed.			
	MP-5	Encrypted with FIPS 140-2 (or successor) validated encryption			
CD-DVD	AC-19	Encrypted with FIPS 140-2 (or its successor) validated encryption unless exempted by VA Directive 6609, paragraph 2. i.	**Y**	**Y**	
	MP-4	Protected and securely stored when not in use			
	MP-6	Sanitized in accordance with VA Directive 6500 and NIST SP 800-88 when the CD/DVD is no longer needed.			

	VADIR 6609	Password to de-crypt the CD/DVD must be transmitted separately from the CD/DVD.			
	VADIR 6609	The CD/DVD must be shipped via a secure delivery service that tracks the mail from pick-up to delivery.			
Research Scientific Computing Devices					
Network Connected.	RA-3	Completion of the Enterprise Risk Assessment (ERA).	**Y**	**Y**	
Standalone Information Systems					
Computers, Laptops, Medical and Scientific Computing Devices	CP-9	Must have a process in place to backup user level data contained on the device.	**Y**	**Y**	
Software					
Software installed on network connected VA Information Systems	CM-7	Must be approved by TRM.	**Y**	**Y**	

Appendix G - ERDSP Process Guide

The ERDSP process guide provides a general overview of the ERDSP submission, review and approval process. Depending on the type of research study, (Human, Basic Science or Animal), R&DC subcommittees such as Safety and Institutional Animal Care and Use Committee (IACUC) would be included in the process.