# VA-approved methods for secure data transfer

There are several methods available to share VA research data (electronic and hard copy) with another VA or non-VA entity/institution.

The methods vary depending on the sensitivity of the data. Sensitive research study data must be encrypted in transmission with **FIPS 140-2 validated encryption** and portable storage devices and CD/DVDs must be encrypted with FIPS 140-2 validated encryption.

Please see the table below for the currently VA-approved data transfer methods, based on sensitivity:

| **Data Transfer Method from VA** | **Sensitive – to another VA** | **Sensitive – to non-VA entity** | **Non-sensitive – to another VA** | **Non-sensitive – to non-VA entity** |
|---|---|---|---|---|
| VA Encrypted Email[1] | X | X | X | X |
| VA SharePoint[2] | X | | X | |
| Shared Folder on the VA Network[3] | X | | X | |
| VA Encrypted Thumb Drive or External Hard Drive[4] | X | X | X | X |
| CD/DVD[5] | X | X | X | X |
| Physical Transport (sensitive)[6] | X | X | | |
| Fax[7] | X | X | X | X |
| Box (cloud storage)[8] | X | X | X | X |
| Electronic Case Report form (eCRF)[9] | X | X | X | X |
| VA unencrypted email | | | X | X |
| USPS or other delivery service (non-sensitive) (FedEx, UPS, etc.) | | | X | X |

1. **VA Encrypted Email using Azure Rights Management System (RMS).** 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 OI&T has issued a set of Frequently asked questions (FAQs) about Azure RMS use within VA and the Office of Research and Development has issued ORD FAQs for the use of Azure RMS in VA research. For additional information see the Azure RMS User Guide.

2. **VA SharePoint**. Verify with your Area Manager (Ryan.Chun@va.gov) the SharePoint that will be used to store the data is configured for the storage of VA sensitive information. Employing the principle of least privilege, the files and folders stored on the SharePoint must have access restricted by 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. For questions about user access and permissions, please contact the local SharePoint Administrator.

3. **Shared Folder on the VA Network**. Employing the principle of least privilege, the shared folder must have access restricted by 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. Please contact Heather.Freasier@va.gov for setting up and granting user access to a local shared folder.

4. **VA Encrypted Thumb Drive or External Hard Drive.** 1) The device must be encrypted with FIPS 140-2 validated encryption or successor validated encryption, 2) The device must be on the OIT Mobile technology and Endpoint Security Engineering Approved Devices and Apps list. 3) Accounted for on a VA Equipment Inventory List (EIL). For additional questions, please contact the local ISSO at v21sfcisostaff@va.gov.

5. **CD/DVD**. 1) CD/DVDs must be encrypted with FIPS 140-2 validated encryption or successor validated encryption unless exempted by VA Directive 6609, paragraph 2.i. 2) The password to the CD/DVD must be transmitted separately from the CD/DVD (e.g., via VA encrypted email). 3) The CD/DVD must be shipped via a secure delivery service that tracks the mail from pick-up to delivery. For additional questions, please contact the local ISSO at v21sfcisostaff@va.gov.

6. **Physical Transport**. Individuals physically transporting sensitive information outside of controlled areas must obtain written approval from the privacy officer, area manager and their supervisor. The authorization must define the type of media, security safeguards used to protect the media and a log must be maintained to document the data in transit. Hard Copy (paper) media must be double wrapped and transported in a secure physical container. Source: OIS Knowledge Service Control MP-5.

7. **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. Following are the precautions that must be taken to protect the security of fax transmissions.

# VA-approved methods for secure data transfer

(a) VA facilities should only transmit Personally Identifiable Information (PII) via fax when no other means exists to provide the requested information in a reasonable manner or time frame. VA health care facilities need to ensure Personally Identifiable Information (PII) is sent on a machine that is not accessible to the general public.

(b) The Health Insurance Portability and Accountability Act (HIPAA) Security Rule does not apply to faxing because the information is not in electronic format prior to sending. The HIPAA Privacy Rule requirements do, however, apply when faxing Protected Health Information (PHI). In the event that a fax is sent via automated systems, or fax back from a computer, then the HIPAA Security Rule does apply because the information was already in electronic format before it was transmitted.
Do not fax individually identifiable information unless someone is there to receive the information or the fax machine is in a secured location (e.g., locked room).

(c) The following statement should be used on fax cover sheets: ""This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above.""

(d) Staff should be trained to double check the recipient's fax number before transmittal and to confirm delivery by telephone or review of the appropriate confirmation of fax transmittal. If there has been an error, the incorrect recipient must be immediately contacted and requested to return or destroy the fax.

(e) Fax machines will be placed in controlled areas within VA office space sufficient to physically limit access to the machine by authorized VA staff only. Use of fax machines will be limited to authorized office personnel, and as necessary, or as equipment features allow, security codes used to prevent unauthorized use to transmit, or receive faxed documents.

(f) Staff periodically reminds regular fax recipients to provide notification in the event that their fax number changes.

(g) Fax transmittal summaries and confirmation sheets are saved and reviewed periodically for unauthorized access or use.

(h) Staff have pre-programmed and tested destination numbers in order to minimize the potential for human error.

**Source:** VA Directive 6609 and OIS Knowledge Service control SC-8.

8. **Box (cloud storage)**. The VA instance of Box can be used to transfer large data files to VA and non-VA entities. If VA employees would like to use this service, please submit a SaaS inquiry form to confirm your use case and obtain procurement approval.

9. **Electronic Case Report form (eCRF).** The eCRF must encrypt sensitive data in transmission using FIPS 140-2 validated encryption or successor validated encryption.