Office of Research and Development

2022 Research IT FAQs and Guidance

Updated March 2022

Contents

OI&T Services

1. What are the basic IT services?

The basic IT services are the core IT elements that every VA user should expect to enable them to perform their duties. The basic services include desktops/laptops, printers, wireless cards, smartphones, help desk and telecommunications support. The elements are tailored to specific user requirements – so for example, users without a requirement for mobility are not issued a laptop or smartphone. Also included are enterprise software agreements for the most frequently used PDF reader (Adobe), Microsoft Office 365 (including SharePoint, Teams (with One Drive for files as part of TEAMS) and Outlook), access to limited File Share storage for administrative documents, Microsoft Edge, Windows Explorer, or Chrome (for standard web-services like access to Internet knowledge sources). Most of these basic IT services can now be requested thru the Your IT icon on your PC or Laptop:

https://yourit.va.gov/va

Support matrix (note that most ORD users will use first option in matrix):

I want to procure…	Process to use	Process used by	How to Access	Maximum Limit	Additional Comments
Endpoints for new employees	Just-In-Time (JIT)	Requesting Service	YourIT - Computer Services (Google Chrome Browser	Up to 15 Users	This is strictly for the issuance of an endpoint for the new user. Other equipment needs and software are supported below.
Expansion or new Tier 3 equipment (outside of activations)	YourIT ticket to tier 3	OI&T staff Only	YourIT	Dependent on funding availability	Infrastructure Operations and/or Solution Delivery is required to do an assessment of need and they will procure based upon needs
Lifecycle Refresh for aged equipment	Consultation with IT Asset Management	OI&T Staff Only	E-mail through IT chain of command	Dependent on funding availability	Coordinated by IT Asset Management on a recurring basis upon inventory review.
Equipment or Software for Reasonable Accommodation	Reasonable Accommodation	Local Reasonable Accommodation Coordinators (LRACs) Only	www.cap.mil	Case Dependent	Coordinated by the Local Reasonable Accommodation office. If IT item is not supplied by CAP funding, consult IT.

2. What about more advanced services like servers, storage, backup, and encryption and application software?

These advanced services should also be provided by OIT. OIT has the core competency and skills necessary to keep server operating systems up to date, to apply patches and hot fixes to keep the equipment in synch with VA standards, and expertise in data lifecycle management (backup, archive, retention, etc.). Research groups have expertise in managing research folders, understanding folder content, managing folder permissions, and understanding the unique data retention requirement of the NARA-approved Research Record Control Schedule. Close cooperation between OIT and Researchers is necessary to maintain the "back office" services provided by OIT while allowing ORD staff to manage research folders, permissions, and content.

3. How do I submit a request for the following Information Technology (IT) services and capabilities?

a. Funded Innovations, New Application Development, IT Enhancement, Interface Development, Platform Support
b. Unfunded Innovations, New Application Development, IT Enhancement, Interface Development, Platform Support
c. Servers, Cloud Services, Tech Refreshes, Databases, Other IT needs

The Account Management Office (AMO) Centralized Request Submission Portal provides a process for VHA Business Owners to submit IT requests for review and evaluation to ensure the requests meet the VA's and OIT's goals & priorities. The AMO process facilitates capturing your IT needs and requirements and ensures your request will be reviewed and submitted to the appropriate intake team within AMO for further discussion and action.

The National Innovation and Development Request Portal also facilitates the request process for VHA software and development requirements.

4. What OIT standardization practices affect ORD?

In recent years, OIT has introduced several standardization efforts to help reduce IT costs and preserve function and performance for users. Investigators should be aware of these standard practices, and acquisitions should be planned to comply with these OIT standards.

a. ***"One-CPU" policy***. This practice looks at users who have been issued both a PC and a laptop. In most cases, that user can be issued a docking station for their laptop in their office and the PC can be reclaimed. As laptop purchases are made, older laptops will be replaced, and if the user is eligible, their office PC may be replaced by the docking station (if they have a mobile computing requirement). Docking stations support a full range of features, including dual monitors. ORD should expect that a portion of their oldest hardware (HW) in these areas to be replaced over the course of FY16 as part of regular OIT lifecycle management.

b. ***Reduction of Desktop Printing***. This practice reduces the number of personal printers attached to individual user PCs in their offices. Now, OIT's practice is to provide "printing services" using

networked printers located in convenient areas and/or for the business units to lease networked Multifunction Devices (MFD) that print, copy, scan, and fax. The cost per page for printing (accounting for all the consumables) is much lower for MFD devices than for individual printers. Any reduction in printed pages with PHI/PII is of value to the VA and the Veterans we serve.

c. ***"Virtual First" server provisioning***. This practice offers "cloud" servers and storage by requiring applications to run on virtual servers rather than multiple physically separate servers. Many applications can be run in a virtual environment and virtual provisioning is faster, easier and lowers costs. OIT has invested heavily in larger virtualized server farms with attached storage to improve the ratio of virtual to physical servers in their enterprise. Investigators should encourage migration from local server farms, with physically separate servers, to more centralized server farms to support their data storage and computing needs at lower cost and with better performance where this is appropriate.

d. ***Cloud First – computing services***. OIT is embracing 'cloud first' policies to modernize and improve service delivery. ORD is attempting to align its data requirements with this strategy. For more information see the VA Enterprise Cloud Services FAQ. From the ECS FAQ page, you will find a link to enter a new ECS request using the VIPR process.

5. Where can I find more information about IT Operations and Services (ITOPS) Field Support?

The OIT-ITOPS SharePoint site contains a wealth of information about all the IT service delivery organizations – including Field Operations, Enterprise Operations, Engineering, and the National Service Desk. In particular, the Field Operations sub-sites contain information on all the Field Supervisory staff (Facility CIO, VISN CIO, Regional Directors and key IT Service Line staff). There is also a site for "tenant support" that describes the processes and services provided to all IT customers regardless of their VHA program office origin.

OIT-IT Operations and Services (ITOPS) – Main Page
https://vaww.vashare.oit.va.gov/sites/itops/home.aspx

OIT-End User Operations – Main Page
https://vaww.vashare.oit.va.gov/sites/euo/pages/default.aspx

OIT-ITOPS –Find your Facility/VISN CIO and Regional Director
Development, Security, and Operations - Directory - ITOPS ALL (EUO 211)

OIT- End User Operations Wiki
End User Operations Wiki Knowledge Repository

6. My research involves development, how does OIT support DevSecOps?

The most recent OIT reorganization has created an agile DevSecOps organization that offers tools like GitHub, Data Analytics Program (DAP), Robotic Process Automation, Rockies Data Analytics Platform, Slack, Jive and App Dynamics to VA users with training. For reference, please refer to the following OIT Digital Services Resources:

- DevSecOps Overview
- Digital VA Product Marketplace
- OIT Services

Visit the Office of Information and Technology's (OIT) Account Management Office (AMO) Centralized Request Submission Portal or National Innovation and Development Request Portal for instructions on submitting potential development requests for OI&T support.

7. My research involves medical images (MRI, CT scan, etc.) or other special data types (voice recording, HD video recording). Where can I obtain advice about IT support?

ORD research frequently deals in data of various data types that are not in database format. Examples include research-grade medical imaging (CT scans, MRIs, etc.), output from laboratory instruments (EEG machines, PFT machines, other biological and laboratory science machines with proprietary output), voice recordings (stress analysis and other qualitative analysis of wave-forms), and pictures/videos – including HD formats. These data types require special handling. In the case of medical imaging, where the imaging modality is like those used in the hospital Radiology department, the acquisition, transfer, storage, and manipulation of the images is not supported by OIT, but rather by Clinical Engineering/Radiology. OIT is responsible for the networking between image modality and PACS system, but the clinical/research service that owns the modality is responsible for the workstations, software, PACs archive, etc.

8. What services are available to VA researchers that are already approved?

ORD has been working on several capabilities to get much needed services pre-approved by OIT security. One such field is the general category of electronic data capture (eDC) and the development of a Clinical Trials Management System.

As additional vendors and services achieve Authority to Operate (ATO) status, they will be listed in the VA OIT SaaS Marketplace and the ORD "Service Catalog" that's currently in development. Local investigators can access these services by contracting with the vendors and using non-IT funding to pay for the services.

The current plan for the Service Catalog is focused on vendors that can provide 'patient generated data' including surveys and questionnaires outside the VA firewall. Future work by ORD will seek to develop an IDIQ contracting vehicle to access the pre-qualified vendors. In the meantime, local site investigators can contract individually thru the federal representative and local contracting officers. Questions about these vendors can be directed to Joseph Holston of the ORD Informatics group at joseph.holston@va.gov.

Other services are in process including qualitative data analysis software (NVivo) and secure file sharing (BOX). Additional information on VA Cloud SaaS products such as BOX can be found in the SaaS Marketplace | DigitalVA

VA investigators should refer to the TRM (http://trm.oit.va.gov/) which lists over 470 products approved products that are used by VA investigators for research.

Note: Regardless of whether major applications or information systems are hosted within or outside of the VA network, information systems that store or process VA owned sensitive information should be used under an official VA ATO. Having an ATO means that the system has been evaluated under the federal requirements for system security. Regular VA business desktops and servers operate under VA ATO designations associated with specific medical center facility area boundaries. Some systems are complex or sophisticated enough to operate under their own ATO. Some examples include the GenISIS system, REDCap (the VA version), Westat, IRBNet, Qualtrics and ASCEND. Additionally, Research Scientific Computing Devices (RSCD) that go through the Enterprise Risk Analysis (ERA) process will be securely isolated behind isolation architectures that reside within their own accreditation boundary. The OIS Research and Operational Technology Cybersecurity Division (formerly Research Support Division-RSD) ISSOs manage over 30 systems that have received or are in the process of receiving a VA ATO. To see the status of the list of enterprise research systems managed by ROTC-D ISSOs visit the ROTC-D Application and Information System Tracker.

Research Software

1. How can I get SAS for my research program?

SAS is the vendor of commonly used statistical/analytic tools. The VINCI/CDW system has a SAS grid that may be appropriate for many of your research needs. Guidance for requesting SAS capabilities and associated VINCI Workspaces or Applications can be requested at VINCI Central. The VINCI Governance Board has directed investments in infrastructure upgrades to VINCI and SAS to improve customer experience and numbers of supported investigator groups. These new investments have allowed VINCI to increase the number of users it serves by *40% each year for the past 5 years without degrading performance*. Investigators are encouraged to use these resources since they are provided by OIT at no cost to the VA Research program. However, it is recognized that certain projects may not be appropriate for the VINCI environment. The VINCI staff will assist the investigator in determining, on a case-by-case basis, whether a study can be hosted by VINCI or must be hosted at another location. Identifying all the various requirements is essential to this process and discussing individual needs with the VINCI/CDW team is encouraged. CSP coordinating centers also provide SAS for the use of the large multi-center clinical trials. For other studies that have a particular regulatory requirement and obligations to oversight groups (for which VINCI and the SAS grid may not be feasible, contact ORD at VHAORDITSupport@va.gov to discuss your options.

2. What options are there for statistical programming software other than SAS?

VINCI also provides SPSS, Stata and R. Guidance for requesting SAS capabilities and other associated statistical programming software can be requested at VINCI Central Services - Workspaces - Applications Portal. Even though SAS has been a common tool used in research and other areas, ORD and OIT recognize that several options for this capability exist. In specific, open-source tools (like R, http://www.r-project.org/. "The R Project for Statistical Computing") provide similar functionality of SAS without the costs. Where SAS is unavailable or unnecessary, investigators are encouraged to explore the use of R and other open-source tools as adequate substitutes.

VINCI Central has a list of software applications and lots of other useful information available here: VINCI Central

3. My research project relies on desktop database tools that have been identified as either in a divest or unapproved state within the VA Technical Reference Module (TRM). What are my options?

During the past few years, OIT has been interested in removing desktop database tools because of specific security vulnerabilities. During that time, ORD cataloged the harm to VA Research that would result from application removal with no plan to migrate legacy data to 'acceptable' databases (MS SQL Server, Oracle, MS SharePoint – all tools approved by the TRM with baseline database configurations and encryption of the database native to the app). Researchers can use the "Search VA TRM" function on the TRM Portal for available database applications and tools that are approved for use on the VA Production Network. If you have a 'mission critical' application using any desktop database applications that have been identified as in either a divest or unapproved state within the TRM, please review TRM FAQ#36 which provides guidance on coordinating with your Area Manager to request the development of a Plan of Action & Milestone (POA&M) to support approval for its continued use.

4. Where can I find information about business intelligence tools, database tools and VINCI resources?

There are several good sites for information about Health Services Research & Development (HSRD) tools and resources. Many of these tools and resources may be used by other ORD programs (CSRD, BLRD, RRD and CSP).

VINCI Central
https://vincicentral.vinci.med.va.gov/SitePages/Home.aspx

VHA Data Portal
http://vaww.vhadataportal.med.va.gov/Home.aspx

ViREC Portal
https://www.virec.research.va.gov/

VIReC Cyberseminars
https://www.virec.research.va.gov/Resources/Cyberseminars.asp

BISL CDW Resources
Business Intelligence Service Line (BISL) (sharepoint.com)

5. What if I only need to access my local VAMC VISTA/CPRS data for "work preparatory to research" purposes – Do I need to use VINCI?

No. ORD and ORO policy does not require the use of VINCI when doing work limited to your VAMC especially when doing "work preparatory to research" (typically – exploratory data analysis to

determine the size of a potential patient cohort or the number of patients who may qualify for a proposed trial). See attached ORO guidance:

2013 ORO FAQ on Local Data Access for

6. Cerner/EHRM

The transition from CPRS/VISTA to Cerner's Millennium EHR (Electronic Health Record Modernization – EHRM) is taking place over a 7 to 10 year period. The VA Millennium EHR has been deployed in Spokane since October 2020, and implementation will continue next in VISNs 20, 10, and 12 throughout FY22 and FY23 according to the OEHRM Provisional Deployment Schedule. Applications and information systems that rely on a connection to the EHR or use EHR/CDW data should consider the rollout schedule and the implications of the transition for future sustainment. Visit the VA Research Resource Guide [EHRM and Research], for communications, FAQs, resources, and updates regarding EHRM, or reach out directly to the ORD transition team with questions or concerns, ResearchEHRMHelp@va.gov.

Research Hardware

1. Should IT Hardware that supports these basic services be "owned" by OIT or by Research?

All hardware in this basic & advanced infrastructure stack should be owned by OIT and recorded in an EIL (Equipment Inventory List) *managed by the local Area Manager (formerly facility CIO)* since all Lifecycle Management funds (money available to replace the oldest hardware first according to industry accepted standards) are distributed by OIT based on information on equipment age from the EIL. OIT maintains the Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS) as well as MAXIMO for this purpose. It is necessary for OIT to control these inventory items and lists per VA policy. If devices and hardware that belong to this basic infrastructure stack are purchased by ORD using funds from their non-profit corporation (NPC), that equipment should be donated to the VA and listed on the OIT EIL for that medical center. (**See Question #21, "inventory management requirements for Research devices and/or RSCDs."**)

2. What is *scientific computing*?

"Scientific computing" can be defined as a scientific instrument that is driven by a PC/laptop or other CPU containing device, where the instrument is non-functional without that CPU/operating system and application. In a sense, the computer is functionally embedded in the instrument. For the purposes of budget formulation and budget execution, it is allowable to use non-IT funds to procure "scientific computing" capability.

Examples of items which may be purchased using non-IT funds include:

e. Hardware: computers embedded or directly interfaced to scientific or clinical instrumentation and used to acquire and analyze data from these instruments. If removal of the computer or computer interface would render the scientific instrument inoperable, the embedded or interfaced computer can be considered "scientific"
f. Software: programs developed specifically for acquisition and analysis of medical or scientific data from an instrument. For example, software used to interpret electroencephalograms, audiograms, or other complex waveforms, software used to manipulate and interpret three-dimensional radiographic images (CT, MRI, etc.).
g. Clinical/Biomedical: equipment commonly used in clinical care, and which contains a PC or laptop, but that equipment has been purchased by the Research Service and is dedicated to research patients. Examples may include PFT machines, EEG machines, Audiometry equipment and other similar devices.

3. What is a "Research Scientific Computing Device (RSCD)"?

VA OIS RSCD Memorandum defines a Research Scientific Computing Device (RSCD) as any standalone or network-capable system or device that cannot obtain VA-approved baseline configuration settings, and/or interfaces with scientific/clinical instrumentation(s) 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.

- A 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.
- A RSCD system is a suite of hardware, software, and scientific applications (including databases and webservers) that are physically part of, and dedicated to, the mission of research and/or scientific studies.

4. Where are RSCDs used most often?

RSCDs are most often seen in rooms, areas and floors occupied by Biological and Laboratory Science Research & Development (BLRD "wet labs"), and in rooms, areas and floors occupied by Rehabilitation R&D (RRD). However, examples of clinical/biomedical equipment purchased by Health Services Research & Development (HSRD) and Clinical Science R&D (CSRD) do exist.

5. What is the process for submitting a RSCD for connection to the VA Network?

Researchers, research staff, and business owners can review the requirements for submitting a RSCD for connection to the VA Network through the Enterprise Risk Analysis (ERA) process at https://dvagov.sharepoint.com/sites/OITSSPPlatform/SiteAssets/Risk_Analysis.aspx . Additional training on the process is available at the RSCD ERA Training Resource Guide.

6. Should Device Isolation Architecture be used for Research Scientific Computing Devices?

Yes, we recommended segregating this equipment into the RSCD isolation architecture or Virtual Local Area Network (VLAN) established jointly by OIT, Office of Information Security (OIS), and ORD. The ERA facilitates the process for conducting a risk assessment that results in RSCDs being identified and designated for network isolation within Research VLANs. The network isolation and segmentation is similar to the isolation that is used for Medical Devices and Biomedical equipment. Information pertaining to the RSCD Enterprise Risk Analysis including FAQs, Templates, Resources (Training videos and slides) can be found on the OIS System Security Support Risk Analysis Portal under Research Scientific Computing Devices.

Network isolation protects the scientific devices from scans, patches and upgrades that are performed on all IP addressable devices attached to the main VA network or "*backbone*." In many cases the scientific instruments can't accept patches and fixes without breaking the instrument or its calibration. In addition, in cases where groups of RSCDs need to communicate with each other and with other IT resources (like storage, backup, etc.), using the network isolation promotes movement and protection of data without the need to move data on thumb drives, by CD/DVD or temporary storage on external hard drives. Mobile media like thumb drives, external hard drives and CD/DVD make it more likely that data will be lost, or viruses and other threats introduced.

Additional RSCD Isolation and TRM requirements can be located at TRM Frequently Asked Questions FAQ #26.

7. What are the inventory management requirements for Research devices and/or RSCDs?

All equipment maintained in VA facilities is required to be inventoried even if the VA does not own the equipment. Research devices and/or RSCDs are often donated or acquired using non-OIT funds and are supported by the scientific team acquiring the equipment. This support may include patches to operating system, upgrades to firmware or application layers, and management of data including backup and restoration.

VA Directive 7002 states, "The VA CIO is responsible, at the Department level, for ensuring the integrity and security of VA's IT assets, including physical inventory as well as data protection and the sanitization of data when IT resources are retired from service."

VA Handbook 7002 states, "Equipment owned by an affiliated institution, or purchased by such institution from grant funds, 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."

- OIT maintains the Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS) as well as MAXIMO for this purpose.
- OIT Owned: All hardware in this basic & advanced infrastructure stack should be owned by OIT and recorded in an Equipment Inventory List (EIL) managed by the local area manager since all lifecycle management funds (money available to replace the oldest hardware first

according to industry accepted standards) are distributed by OIT based on information on equipment age from the EIL.

- Equipment purchased by ORD using funds from their non-profit corporation (NPC) should be donated to the VA and listed on the OIT EIL for that medical center.

- Affiliate organization (e.g., university partners) purchased and owned IT equipment that's used at VHA facilities must be entered into the EIL.

  Note: equipment on an EIL does not indicate VA Ownership.

- Annually, a physical inventory of all nonexpendable property and designated sensitive items will be conducted. (VA Handbook 7002, Part 8).

Inventory Best Practices

- There can be several EILs.
  - Group devices in a useful manner on their own EIL.
- Document a clear SOP for inventory processes.
  - Make it accessible for all staff.
- Identify a single point of contact to coordinate research inventory for your project.
  - When inventory becomes a standard practice, it is easier to maintain.
- Make sure the team has a way to input equipment into inventory.
  - Create an Excel spreadsheet with the necessary data for input to the database
- Make it easy to identify equipment.
  - Colored labels are a great visual indicator. Choose any number of color combinations to indicate research equipment, affiliate owned, or to identify equipment entered in an EIL.
  - Colored labels do not have to be on the equipment – Being visible nearby works as well.

It's best to involve VAMC clinical engineering staff in support of many RSCDs, or for Research to obtain a support contract for their maintenance. For example, large neuroimaging research centers may require considerable clinical engineering support for routine maintenance, troubleshooting, and storage/backup of data.

8. My research utilizes portable storage devices, mobile devices and/or applications. How do I proceed?

Many research protocols now involve portable storage devices and mobile devices (laptops, tablets, flash drives, removable media, smartphones, and wearable devices). The ISSO conducting an information security review of your research study will verify any portable storage devices, mobile devices, and mobile applications used in the study are approved for use. The following guidance should be followed when using such devices within your research project:

a. VA Mobile Devices. mobile devices (excluding portable storage, digital cameras, video recorders and audio recorders) must meet VA approved configuration baselines and require approval by ITOPS

Mobile Technology and Endpoint Security Engineering. Please see this List of approved VA Mobile Devices. If a mobile device is not on the approved list, you can request to have the device assessed for approval. The request should be submitted through the Mobile Device Management (MDM) Intake Process. All devices must be accounted for on a VA Equipment Inventory List (EIL).

ITOPS Mobile Technology and Endpoint Security Engineering maintains a list of approved Android and Apple devices. Mobile devices that are not listed on the approved Android and Apple devices list must be submitted to ITOPS Mobile Technology and Endpoint Security Engineering for approval using the Mobile Device Intake Process.

The Information System Owner (ISO), local CIO, or designee and supervisors must authorize the use of mobile devices within their Operating Unit prior to their implementation. VA mobile devices must be accounted for on a VA Equipment Inventory List (EIL).

***Note**: VA mobile devices will be encrypted using FIPS 140-2 (or its successor) validated encryption, if technically possible. If not technically possible, the documented justification and review/approval by the local Information System Owner (ISO) and CIO is required. 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 vulnerability will need to be documented in accordance with the OIS Plan of Action and Milestones (POAM) Management Guide.*

Source: IS Knowledge Service Security Control AC-19

b. VA Portable Storage Devices. VA portable storage devices must be approved by *Solution Delivery Security Engineering* before the device can be used in VA. Approved portable storage devices can be found on the Security Engineering FIPS 140-2 Validated Removable Storage Devices list.

If a portable storage device is not on the Security Engineering FIPS 140-2 Validated Removable Storage Devices list, it must be submitted for approval before it can be used in VA. Portable storage devices can be submitted for approval using the Request New Product/Technology Review process. If the study team plans to purchase a portable storage device, the device must be submitted for approval prior to purchase.

The Information System Owner (ISO), local CIO, or designee and supervisors must authorize the use of portable storage devices within their Operating Unit prior to their implementation. VA portable storage devices must be accounted for on a VA Equipment Inventory List (EIL).

***Note**: VA mobile devices will be encrypted using FIPS 140-2 (or its successor) validated encryption, if technically possible. If not technically possible, the documented justification and review/approval by the local Information System Owner (ISO) and CIO is required. 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 vulnerability will need to be documented in accordance with the OIS Plan of Action and Milestones (POAM) Management Guide..*

c. **VA Digital Cameras, Video Recorders and Audio Recorders.** When feasible, limit the audio files collected to a minimum amount of Personally Identifiable Information/Protected Health Information (PII/PHI) elements (e.g., name, Social Security Number (SSN), date, etc.) that are relevant and necessary to accomplish the legally authorized purpose of collection. VA digital cameras, video

recorders and audio recorders must be approved by OIT Solution Delivery/Security Engineering before the devices can be used. Approved VA digital cameras, audio recorders, and video recorders that have been approved will have an Initial Product Review document on file. VA digital cameras, audio recorders, and video recorders that have not been approved by Security Engineering can be submitted for assessment and approval using the Request New Product/Technology Review process.

If a digital camera, audio recorder, and/or video recorder 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 TRM Content Request Form to begin this process.

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

***Note**: VA Digital Cameras, Video Recorders and Audio Recorders must be encrypted using FIPS 140-2 (or its successor) validated encryption, if technically possible. If not technically possible, the documented justification and review/approval by the local Information System Owner (ISO) and CIO is required. The Deputy Assistant Secretary (DAS) for OIS or designee must also review/approve VA Digital Cameras, Video Recorders and Audio Recorders that cannot be encrypted using FIPS 140-2 (or its successor) validated encryption. The vulnerability will need to be documented in accordance with the OIS Plan of Action and Milestones (POAM) Management Guide. VA FIPS 140.2 Approved Removable Storage Devices*

Memory Seal

Supervisors ensure their mobile device(s) have a security seal (tamper proof tape) placed over the memory card slot and/or the main device seam to ensure the storage medium is not removed.

Media Sanitization

The destruction of storage mediums (i.e., internal HDD, SD card, micro SD card, etc.) will be in accordance with VA Handbook 6500.1 Electronic Media Sanitization and OIT/OIS SOP MP-6 Electronic Media Sanitization.

Additional Security Requirements for VA Digital Cameras, Video Recorders and Audio Recorders

Users of VA Audio Recorders must ensure the device is compliant with the additional security requirements in the OIT ITOPS Security Technical Implementation Guide (STIG) for Recordable Mobile Devices (Audio Files Only)

Users of VA Digital Cameras and Video Recorders must ensure the device is compliant with the additional security requirements in the OIT ITOPS Security Technical Implementation Guide (STIG) for Recordable Mobile Devices (Cameras – Photo/Video/Audio)

The Information System Owner (ISO), local CIO, or designee and supervisors must authorize the use of Digital Cameras, Video Recorders and Audio Recorders within their Operating Unit prior to their

implementation. VA Digital Cameras, Video Recorders and Audio Recorders must be accounted for on a VA EIL.

d. **Loaning or Gifting of VA mobile devices to research subjects**. Currently no procedures exist for the loaning or gifting of mobile devices (e.g., iPhone(s), iPad(s), wearable devices) to research subjects. The Research Information Security Task Force (RIS-TF) chartered by the Executive in Charge, Veterans Health Administration (VHA) and the Executive in Charge, VA Office of Information Technology, has established a sub-working group to address the lack of governance and to recommend secure pathways for the loaning of Government Furnished Equipment (GFE) mobile devices to Research Study Subjects in compliance with VA Security Policy.

e. **Sponsor Provided Mobile Devices.** Many sponsored research protocols now involve mobile devices (tablets, smartphones, and wearable devices). In general, when a subject is given a sponsor provided mobile device as part of a sponsored research protocol, and the research subject has executed a written authorization for the disclosure of their data to the study sponsor, and the VA does not retain ownership of the data, the device is not subject to VA security requirements. Researchers must secure mobile devices when not in use.

f. **VA Mobile Application Development**. Guidance on the development of mobile applications can be found on the VA Mobile Developer Portal. The portal provides an overview of the mobile app development, workflow and how to navigate the developer portal.

g. **VA Sponsored and Third-Party Mobile Applications.** VA sponsored and third-party mobile applications must be reviewed and approved before the mobile application can be used in VA research. Requests for the review and approval of VA sponsored and third-party mobile applications are submitted using the Office of Connected Care, VA Mobile App Intake Portal. (VA Network access required)

Additional Mobile Application Information:

- VA Mobile Site
- VA Mobile FAQs
- VA Mobile App Store

Funding and Purchasing

1. What is contained in VA Directive 6008 on the funding of IT versus non-IT acquisitions?

The VA issued VA Directive 6008 – Acquisition and Management of VA Information Technology Resources (dated 8/29/2016). This Directive revises and updates the original 2006 IT versus non-IT guidance. It does several other things including defining IT and affirming the VA CIO oversight authority for all IT under Federal Information Technology Acquisition Reform Act (FITARA). It also rescinds the prior VA CIO guidance on mobile devices and applications and defines the process for the purchase of medical & research equipment as well as the process for obtaining permission to purchase SaaS using non-OIT funding. This VA Directive should be read and understood by every research office and investigator.


VA Directive 6008 dated 20160831.pdf


VA DIRECTIVE 6008 Signed Memo.pdf

VA Directive 6008 is currently undergoing major revisions to update it for the use of the VA Enterprise Cloud Services (VA ECS) in Amazon and Azure. ORD is actively working with OIT to include language that would allow the VA Medical & Prosthetics Research Appropriation to purchase "cloud credits" from the VA ECS for data science research. When this revised policy is finalized and issued, VHA ORD will issue new guidance to the VA Research field on accessing cloud services thru the VA ECS.

For more information on Cloud Computing Considerations at the VA (Cloud Characteristics, Cloud Deployment Models, Types of Cloud Computing Services, Cloud Credits, Security Requirements, etc.) please visit the VA's Enterprise Cloud Solution Office's Resource Page.

Please see the VAEC Fact Sheet below for a quick reference on the VA Enterprise Cloud and contact VHAORDITSupport@va.gov if you have any questions.


VA Enterprise Cloud-Flyer.pdf

2. Can University Foundation/Non-Profit Corporation funds be used to buy IT?

Yes – although this should not be a standard practice. NPC funds are in short supply at most stations. One-time purchases that don't commit to multi-year obligations could be supported. In this case, the NPC executes the transaction, following existing VA and OIT standards, and donates the IT items to the VA. Per VA Directive 6008, VHA can purchase IT-related assets and services funded by Grants or other Research Efforts, but only for the "initial costs." Once the equipment is donated to the VA, subsequent sustainment (HW Maintenance, SW License and Support, lifecycle replacement) of that equipment should be financed and supported by OIT.

3. Can other sources of grant funds be used to buy IT?

Yes. Examples include funds from an NIH grant, from a Pharma, BioTech or other industry partner grant, Tech Transfer Cooperative Research and Development Agreement (CRADA) or from other Federal or non-Federal sources. Just as with expenditure of NPC funds, this should not be standard practice nor should complex multi-year commitments be made because the funding may lapse, and the IT infrastructure would go unsupported. The local research contracting officers execute the transaction, following existing VA and OIT standards, and donate the IT items to the VA. Per VA Directive 6008, VHA can purchase IT-related assets and services funded by Grants or other Research Efforts, but only for "initial costs". Once the equipment is donated to the VA, subsequent sustainment (HW Maintenance, SW License and Support, lifecycle replacement) of that equipment should be financed and supported by OIT.

4. Can OIT "Activation" funds be used to buy IT?

Yes. Examples include funds from an NIH grant, from a Pharma, BioTech or other industry partner grant, Tech Transfer Cooperative Research and Development Agreement (CRADA) or from other Federal or non-Federal sources. Just as with expenditure of NPC funds, this should not be standard practice nor should complex multi-year commitments be made because the funding may lapse, and the IT infrastructure would go unsupported. The local research contracting officers execute the transaction, following existing VA and OIT standards, and donate the IT items to the VA. Per VA Directive 6008, VHA can purchase IT-related assets and services funded by Grants or other Research Efforts, but only for "initial costs". Once the equipment is donated to the VA, subsequent sustainment (HW Maintenance, SW License and Support, lifecycle replacement) of that equipment should be financed and supported by OIT.

5. Can non-OIT funds be used to buy services like SaaS?

VA Directive 6008 allows for the purchase of **Software as a Service** (SaaS) using non-OIT funding. The same Directive outlines the process to be followed (including a series of approval steps ending with VA CIO approval – see VA Directive 6008, Section 2.m). Section 2.m lists an Exemption Process for any proposed IT-related acquisition that is seeking to use funding outside of the VA IT Systems Appropriation.

OIT has created a 'fast-track' approach to acquiring and obtaining IT services under the SaaS guidelines. Guidance on adopting and procuring SaaS services waiver can be obtained at this URL: Adopting Software as a Service at VA | Office of Information and Technology

This site has useful Frequently Asked Questions (FAQ), and information on cloud hosting. It also facilitates new requests. There is a Service Catalog of available services including GITHUB and Lighthouse. Once a SaaS request is placed at this URL, you will be contacted by the OIT team for the details of the specific instance you are considering. Note: a TRM waiver used to be required – but because most SaaS acquisitions won't be on the VA Network, a TRM waiver is no longer required.

The cost of the service once awarded would now be borne by the VA Medical & Prosthetics Research Appropriation rather than the IT Appropriation. If widely used, the dollars available to research and investigators would shrink as the costs of supporting SaaS increase. This trade off should be considered in any long-range budget planning.

For more info on IT vs Non-IT funding and considerations please follow this link: Welcome to the IT / NonIT Portal (sharepoint.com)

6. When do OIT funds get distributed?

There are no OIT funds distributed to the OIT field for the purposes of supporting field IT needs in support of research. As a result – ORD and OIT are pursuing a course to centralize as much as possible to achieve economies of scale and to permit faster execution on new requirements. Please escalate problems to VHAORDITSupport@va.gov when they arise.

Research Data Security

1. Where can I find more information about Information System Security Officer (ISSO) Field Support?

R&D stakeholders are encouraged to work with their local Facility ISSO which serves as the primary point of contact for research related information security questions/concerns. The **OIS- Research and Operational Technology Cybersecurity Division (ROTC-D)** is an enterprise level team of cybersecurity specialists and ISSOs that consults with stakeholders focusing on information security topics of national and enterprise scope and/or in support of major/centralized ORD IT programs. Requests for research cybersecurity and information security guidance can be submitted to OIS-ROTC-D through the VHA Regulatory Research Cybersecurity Guidance Process to ensure uniform interpretation of OIT policies to avoid medical center to medical center variability in policy interpretation and enforcement. The cybersecurity and monitoring functions are centralized while the ISSOs support local users at the medical center level. ISSOs are organized in a hierarchy with Facility>VISN>Information System Security Manager (ISSM)>ISSO in every location. Escalation of unresolved issues in the field security organization can be done like escalation of issues in the Service Delivery organization. IT Security useful links are below:

OIS- Research and Operational Technology Cybersecurity Division (ROTC-D)

- ROTC-D Guidance Resource Portal
- Service Now 'yourIT" VHA Regulatory Research Cybersecurity Guidance Request Portal
- Toolkit: Research Information Security & Cybersecurity
- Email: oisispssssrsdinformationsecuritysupport@va.gov

OIS-Information Security

- About OIS

OIT-Enterprise Security Operations (ESO)- Information Security

- ESO Overview Resource Portal
- Find Your Local ISSO

2. What cyber security resources are available to train me and staff on cyber hygiene and best practices?

R&D stakeholders who access VA information and information systems shares the responsibilities and duties to protect privacy and ensure information security to keep the organization in good standing while adhering to the VA's Rules of Behavior.

The following Talent Management System (TMS) resources are available to help you maintain awareness of adequate cyber security best practices:

- **TMS ID 10176**: VA Privacy and Information Security Awareness and Rules of Behavior
- **TMS ID 4486857**: Research Institutional Review Board ISSO Protocol Review
- **TMS ID 4486855**: VA Research Overview for Information System Security Officers and Managers (ISSOs/ISSMs)

- **TMS ID 4486853**: Research Electronic Case Report Form (eCRF)/Web Portal Security Review for ISSOs
- **TMS ID 4533233**: Preparing for a Research Cybersecurity/Information Security Compliance Assessment
- **TMS ID 4284816**: IS Webinar Series: Cyber Spotlights

The following OIS ROTC-D Monthly National Cybersecurity Research Teleconference (MNCRT) on Demand training and awareness resources are also available to help you maintain awareness of adequate cyber security best practices:

- Monthly National Cybersecurity Research Teleconference (MNCRT) On Demand

3. Who do I contact in OIS about the ATO and Assessments and Authorizations (A&A) process?

R&D stakeholders can review the OIS Authorization Requirements Standard Operating Procedures (SOP) to obtain step-by-step guidance and information on the VA ATO process.
VA researchers should contact their local ISSO pertaining to the procedures on obtaining VA authorization for the use of external information systems. For ATO guidance on enterprise major research applications, researchers can also contact OISISPSSSSRSDCybersecurityATOMOUSupport@va.gov.

Data Sharing and Collaboration

1. What methods are approved to transmit or transfer VA research data/information?

- **Approved methods to transfer sensitive research information to another VA facility:**
  - **VA Encrypted Email.**
  - **Azure Rights Management System (RMS) Email.** 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. OI&T approved RMS Procedures.
  - **VA SharePoint**. Verify with the local facility OIT ITOPS Area Manager the SharePoint site is configured for the storage of VA sensitive information.
  - **Shared Folder on the VA Network**. Employing the principle of least privilege (AC-6.1), 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
  - **VA Box**. VA Box is used for large file transfers. To request approval to use VA Box, the requestor will need to submit a SaaS Inquiry Form.
  - **VA Portable Storage Device (external hard disk drive or USB flash drive)**

The device must be on the Security Engineering FIPS 140-2 Validated Removable Storage Devices list and accounted for on a VA Equipment Inventory List.

- **CD/DVD**. CD/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 pick-up to delivery.
- **USPS or other delivery service.** VA Directive 6609 provides specific guidance on the mailing of VA sensitive information.
- **Facsimile Machine (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. OIS knowledge service, security control SC-8, control level guidance provides the precautions that must be taken to protect the security of fax transmissions.
- **Physical Transport.** Individuals physically transporting sensitive information outside of controlled areas (VA facility) must obtain prior approval. The required approval/signatory authorities can be found in IS Knowledge Service Security Control MP-5, Control Level Guidance section.

- **Approved Methods to Transfer non-Sensitive Data to another VA facility:**
  - Unencrypted email.
  - Any of the approved methods to transfer sensitive research information to another VA facility.

- **Approved Methods to Transfer Sensitive Data to a non-VA entity include:**
  - **Azure Rights Management System (RMS) Email.** 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. OI&T approved RMS Procedures.
  - **DocusSign.** ORD has purchased a supply of envelopes to be used in research studies requiring documentation of informed consent and or HIPAA Authorization. The process to request the use of DocuSign is to complete the form at the ORD SharePoint site located here: https://dvagov.sharepoint.com/sites/VHAORPPE/DocuSign
  - **VA Box**. VA Box is used for large file transfers. To request approval to use VA Box, the requestor will need to submit a SaaS Inquiry Form.
  - **VA Portable Storage Device (external hard disk drive or USB flash drive).**
    The device must be on the Security Engineering FIPS 140-2 Validated Removable Storage Devices list and accounted for on a VA Equipment Inventory List.
  - **CD/DVD**. CD/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 pick-up to delivery.
    - **USPS or other delivery service.** VA Directive 6609 provides specific guidance on the mailing of VA sensitive information.
    - **Facsimile Machine (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. OIS knowledge service, security control SC-8, control level guidance provides the precautions that must be taken to protect the security of fax transmissions
    - **Physical Transport (MP-5).** Individuals physically transporting sensitive information outside of controlled areas (VA facility) must obtain prior approval. The required approval/signatory authorities can be found in IS Knowledge Service Security Control MP-5, Control Level Guidance section.

- **Approved Methods to Transfer non-Sensitive Data to a non-VA entity include:**
    - Unencrypted email.
    - Any of the Approved methods to transfer sensitive research information to a non-VA entity.

2. My research requires an external connection to our University Affiliate. What guidance is there on the various types of authorized external connections?

Research is heavily collaborative. Almost all research has some requirement for external connections to non-VA collaborators and university affiliates. To support this business need OIT has recently developed an enterprise-wide secure solution with VA Guest WiFi/eduroam. VA Guest WiFi/eduroam service solutions will be available at VA Medical Centers (VAMC) that choose to procure/fund the service. Once the solution is procured, services will be deployed in a phased approach at VA Medical Centers (VAMC) based on an enterprise site deployment and onboarding schedule.

Eduroam will allow VA Principal Investigators (PI) and research team members across the VA to connect through the internet to their affiliate institutions when visiting other participating institutions by simply opening their WiFi-enabled device. Through the eduroam service, VA PI and research team members will have access to an affiliated university's resources, including journals, publications, and scientific research sites.
VA PI and research team members may use eduroam services to conduct business with university affiliates, access university affiliate resources, and access public internet sites however, Eduroam services are not authorized to transmit VA data or VASI such as PHI/PI.

OIS coordinated and collaborated with ORD to develop guidelines that apply to the use of eduroam services for research purposes which can be found within the Memorandum, "Acceptable Use Guidance for VA Guest WiFi and Education Roaming (eduroam) Service Solutions within VHA Facilities with Research Programs"

OIT has also developed a Guest WiFi/eduroam FAQ with guidance on the request process for the enterprise service. If you would like more information on Guest WiFI/eduroam services at your facility, please contact the VA OIT Wireless Infrastructure Research-Guest Project Team at vawirelessinfresearch-guestprojectteam@va.gov.

As a reminder, Secure External Connection requirements are provided within VA Directive 6513 "Secure External Connections" dated 10/12/2017. The VA OIT Enterprise Security External Chance Council (ES-ECC) provides an overview on the Types of External Connections within the Enterprise Connections Define Guidance Document. Directive 6513 specifies that all incoming/outgoing IP traffic to/from the VA domain must transverse one of the Trusted Internet Connections (TIC) maintained by OIT. This is a Department of Homeland Security (DHS) requirement on all Federal Departments. BPGs do not comply with the DHS regulation dealing with TIC traffic and thus BPGs are being phased out. External connections (i.e. air-gap) identified as processing or sharing sensitive/restricted data and that are not operating through a Trusted Internet Connection (TIC) gateway must be identified as non-compliant, reported as a security incident to the Computer and Security Operations Center (VA CSOC), must be configured to meet Office of Management and Budget (OMB) requirements through an approved transition/modification schedule for that connection, and can be addressed through the Plan Of Action & Milestones (POA&M) process with your local facility Information System Security Officer (ISSO).

- Directive specifies the process for seeking an external connection and the waiver process to be followed if the required connectivity cannot be established (compensating controls must be in place). It also specifies the need to have an MOU/ISA in place and to have the MOU/ISA recorded in the System Security Plan (SSP) at your local site. Your Area Manager and ISSO should be made aware of all external connections that exist or are required for research purposes to ensure those connections are tracked within the Enterprise Security External Change Council's (ES-ECC) External Connection Compliance Tracking (ECCT) Tool. The MOU/ISA is reviewed and approved by the OIS Business Requirements Division (BRD) once an identified Business/Information System Owner submits the required documents within the OIS MOU ISA Document Site portal. Work with your local ISSO for this process.

ORD continues to work with OIT to describe the external connection requirements for VA Research and provide more standard and uniform connectivity. We are seeking uniform OIT standards for external interconnections between VAMC and academic affiliates for the purposes of research and education. If you are having specific problems at your site, contact the ORD Informatics group at VHAORDITSupport@va.gov.

3. My question isn't here, what should I do?

You can contact ORD Informatics at VHAORDITSupport@va.gov for all other questions. Additionally, you can escalate your question or issue thru the normal escalation process for IT issues (discuss at the Area Manager level, and if issues are not resolved, bring to the VISN CIO and/or OIT Regional Director. Issues that are not resolved at the Regional Level should be brought to the attention of the ORD Informatics group.

Find you area managers (EUO 211): Development, Security, and Operations - Directory - ITOPS ALL