Welcome to
VA Privacy and Information Security Awareness and Rules of Behavior

FOUNDATIONS

for a Secure VA

U.S. Department of Veterans Affairs, Office of Information and Technology, IT Workforce Development

Contents

Purpose of This Document

This text-only course transcript is designed to accommodate users in any of the following circumstances:

- You are using a screen reader, such as JAWS, to complete course material and have difficulty with the interactions in the online version.
- You are experiencing difficulties accessing the online version due to computer network or bandwidth issues.
- You have completed the online version and want to print a copy of the course material for reference.

This version of the *VA Privacy and Information Security Awareness and Rules of Behavior* Text-Only Course Transcript is valid for fiscal year (FY) 2024 (October 2023 through September 2024).

You should take the online version of this course if possible; however, if you complete the course using this text-only transcript, you must complete the following steps:

Print, initial each page of, and sign the Information Security Rules of Behavior (ROB) for your particular user type.

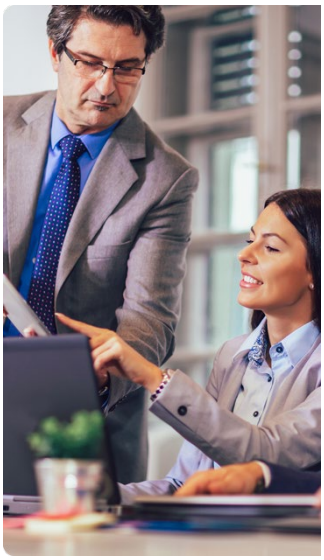
1. There are two versions of the ROB, one for Organizational Users and one for Non-Organizational Users. You must select the user group that applies to you, initial each page, and then sign the Acknowledgement and Acceptance section. Review the definitions of Organizational and Non-Organizational Users on the next page to determine your user group.
2. Contact your supervisor or Contracting Officer Representative (COR) to submit the signed ROB and to coordinate with your local Talent Management System (TMS) Administrator to ensure you receive credit for completion.

Using Hyperlinks Within This Document

Throughout this document, you can access glossary terms, located in Appendix C, by selecting the available hyperlinks. To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt +<left arrow> on your keyboard. Some browsers will not permit the Alt+<left arrow> navigation feature; therefore, it is recommended that you download the PDF to your desktop and then open the PDF in Adobe Acrobat.

Topic 1: Introduction

1.1 Welcome



Welcome to the *VA Privacy and Information Security Awareness and Rules of Behavior* training course.

1.2 Purpose of Taking This Course

The purpose of this course is to provide information security and privacy training to everyone at the Department of Veterans Affairs (VA).

Regardless of your role, you may encounter VA sensitive information and information systems, which everyone is obligated to protect. As an Organizational User or Non-Organizational User, you need to stay current on how to protect VA sensitive information. This course will help you learn the right way to access, use, and store VA information and protect VA systems in accordance with the ROBs and VA Privacy Principles.

The VA Privacy Principles are a collection of principles that guide how VA handles personal information and evaluates information systems, processes, programs, and activities that affect individual privacy. These 10 principles establish an overarching privacy framework for all personnel and business partners who maintain Veteran and VA Employee data on behalf of VA. These rules and principles help us build a strong foundation of privacy and security awareness.

- The Principle of Openness – When VA collects personal data from an individual, VA will inform him or her of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act System of Records Notice (SORN) has been published in the Federal Register and posted on the VA Systems of Records website.
- The Principle of Individual Participation – Unless VA has claimed an exemption from the Privacy Act, everyone will be granted access to his or her records, upon request; provided a list of disclosures made outside VA; and provided the opportunity to make corrections to his or her file if errors are identified.
- The Principle of Limited Collection – VA will collect only those personal data elements required to fulfill an official function or mission. Those collections will be conducted by lawful and fair means.
- The Principle of Limited Retention – VA will retain personal information only for as long as necessary to fulfill the purposes for which it is collected. Records will be destroyed in accordance with established VA records management principles.
- The Principle of Data Quality – VA will make every effort to maintain accurate, relevant, timely and complete data about individuals.

- The Principle of Limited Internal Use – VA will use personal data for lawful purposes only. Access to any personal data will be limited to those individuals within VA with an official need for the data.
- The Principle of Disclosure – VA personnel will guard all personal data to ensure that all disclosures are made with written permission or in strict accordance with privacy laws.
- The Principle of Security – All personal data shall be protected by safeguards appropriate to ensure security and confidentiality. Electronic systems will be periodically reviewed for compliance with the security principles of the Privacy Act, the Computer Security Act, Heath Insurance Portability and Accountability Act (HIPAA), and related statutes. Electronic collection of information will be conducted in a safe and secure manner only.
- The Principle of Accountability – VA, its employees, and contractors are subject to civil and criminal penalties for certain breaches of privacy. VA shall be diligent in sanctioning individuals who violate privacy rules.
- The Principle of Challenging Compliance – An individual may challenge VA if he or she believes that VA has failed to comply with these principles, privacy laws, or the rules in a SORN. Challenges may be addressed to the VA Privacy Service.

  Source: VA Privacy Service site – Privacy Principles

To do your part in helping VA uphold federal laws and keep the organization in good standing, you must take this course prior to gaining access to VA information or information systems. You must then take the course annually to maintain that access. Depending on your role and the information systems you have access to, you may be required to complete additional role-based information security and privacy training.

VA employees and contractors who have access to Protected Health Information (PHI) are also required to complete *Privacy and HIPAA Focused Training* (VA TMS ID: 10203).

1.3 Requirement for Health Professions Trainees

As with any rule, there can be exceptions. If you are a Veterans Health Administration (VHA) Health Professions Trainee (e.g., student, intern, resident, or fellow), you are not required to complete this course. Instead, you are required to complete the following courses:

- First-time trainees must complete *VHA Mandatory Training for Trainees* (VA TMS ID: 3185966).
- Each subsequent year, trainees must complete *VHA Mandatory Training for Trainees-Refresher* (VA TMS ID: 3192008).

1.4 Types of VA Sensitive Information

Federal agencies have over 100 different ways of describing unclassified information that requires protection due to law, regulation, or policy. This information is now referred to across the federal government as Controlled Unclassified Information (CUI). VA sensitive information is considered a type of CUI, which includes Sensitive Personal Information (SPI), such as Federal Tax Information (FTI),

Personally Identifiable Information (PII), and PHI. Some examples are Veteran medical records, personal and financial employee records, credit card information, and information related to VA's security. You are responsible for keeping all VA sensitive information safe.

- **CUI** is unclassified information that requires protection due to law, regulation, or policy. VA is in the process of implementing the CUI Program to fulfill the requirements in Title 32 Code of Federal Regulations Part 2002 (32 C.F.R. 2002) and Executive Order 13556. The CUI Program will change marking practices and clarify safeguarding and dissemination controls to help you better understand your role in the protection of CUI.

  For more information regarding the CUI Program, refer to the CUI intranet site. You can also email the CUI team. A link to this site and the email address can be found in Resources.

  When it's time for you to transition to CUI practices, you will be formally notified and trained.

  Source: 32 C.F.R Part 2002 and Executive Order 13556

- **VA Sensitive Information** is any information that has not been cleared for public release and has been collected, developed, received, transmitted, used, or stored by VA or by a non-VA entity in support of an official VA activity. VA Sensitive Information may be a type of CUI, and if so, must follow the VA's CUI guidance.

  Source: VA Directive 6500

- **SPI**, with respect to an individual, means any information about the individual maintained by an agency, including the following:
  - Education, financial transactions, medical history, and criminal or employment history
  - Information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records; used to reference Federal Tax Information, Personally Identifiable Information, and Protected Health Information.

  FTI, PII, PHI, and CHD all fall into this category.

  Source: 38 U.S.C. § 5727, VA Handbook 6500.2, OMB Circular A-130, VA ESO - Payment Card Industry SharePoint

  - **FTI** includes tax returns or data about those returns that can come directly from the Internal Revenue Service (IRS) or other secondary sources like other federal agencies.

    Source: VA Handbook 6500.2

  - **PII** is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

    Source: OMB Circular A-130

- **PHI**, as defined by the HIPAA Privacy Rule, is individually identifiable health information transmitted or maintained in any form or medium by a covered entity, such as VHA. This is another subcategory of SPI.

  Note: VHA uses the term PHI to define information that is covered by HIPAA but, unlike individually identifiable health information, may or may not be covered by the Privacy Act of 1974 or Title 38 VA Confidentiality Statutes as updated. In addition, PHI excludes employment records held by VHA in its role as an employer. Please see Resources for more on the updates to Title 38 section 7332.

  Source: 45 CFR § 160.103; VA Directive 6066

- **Credit Cardholder Data (CHD)** is financial data involved in processing, storing, and transmitting the payment card transactions of Veterans, their families, and VA employees. This data must be safeguarded to comply with the Payment Card Information Data Security Standard (DSS). Please visit the VA Enterprise Security Operations (ESO) Payment Card Industry SharePoint for additional PCI DSS guidance. The link to this SharePoint site can be found in Resources.

  Source: 38 U.S.C. § 5727; VA Handbook 6500.2; OMB Circular A-130; VA ESO - Payment Card Industry SharePoint

1.5 Organizational and Non-Organizational Users

There are two types of authorized users at VA: Organizational Users and Non-Organizational Users.

Organizational Users are VA employees, contractors, researchers, students, volunteers, and representatives of federal, state, local, or tribal agencies not representing a Veteran or claimant.

Non-Organizational Users are any information system users not clearly identified as an Organizational User. This includes people with a Veteran or claimant power of attorney.

You need to be aware of the impacts of data breaches, which are considered severe privacy incidents. These impacts can include loss of trust in VA and exposure of Veterans', colleagues', and employees' data. Stay diligent in following VA's ROBs, which are the minimum compliance standard for all VA staff.

Think of the ROBs as the blueprints that provide guidance for Organizational and Non-Organizational Users on how to protect VA sensitive information and safeguard VA systems. This guidance will help you accomplish your day-to-day duties securely. You reduce the risk of compromising privacy and information security when you follow the best practices laid out by the ROBs.

1.6 General Rules of Behavior (ROBs)

The VA Rules of Behavior (ROBs) are sets of rules that outline the responsibilities and expected behaviors of people who use VA information systems. Most ROBs apply to specific situations like accessing VA computer resources or working remotely. Other ROBs are more general.

Be sure to read and follow the rules that apply to your user type. Many of these rules are presented during the course. They will help you determine the right course of action when you have challenges.

The ROBs will be presented at the end of the course for you to acknowledge and accept. Select each user type to review some general ROBs that apply to everyday behavior.

Organizational Users ROBs

These are general ROBs that pertain to everyday behavior expected of Organizational Users:

- I WILL comply with all Federal statutes, regulations and policies applicable to VA information security, information privacy/disclosure and records management. (SOURCE: PM-10)
- I WILL NOT have any expectation of privacy in any information I access, create, receive or maintain, or in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. (SOURCE: AC-10)
- I WILL complete mandatory security and privacy awareness training within designated time frames and complete any additional role-based security training required for my roles and responsibilities. (SOURCE: AT-3)
- I WILL understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)
- I WILL sign VA Information Security ROBs required for access or use of specific VA systems. (SOURCE: AC-8)
- I WILL comply with any requirement to sign a non-VA entity's ROB to conduct VA business. (SOURCE: PM-10)
- I WILL obtain approval from the Office of Public and Intergovernmental Affairs before establishing a VA social media account. (SOURCE: AC-22)

Non-Organizational Users ROBs

These are general ROBs that pertain to everyday behavior expected of Non-Organizational Users:

- I WILL comply with all Federal statutes, regulations, and policies applicable to VA information security, information privacy/disclosure, and records management policies. (SOURCE: PM-10)
- I WILL NOT have any expectation of privacy in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. (SOURCE: AC-10)
- I WILL complete mandatory security and privacy awareness training within designated time frames. (SOURCE: AT-2)
- I WILL understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)
- I WILL sign specific VA Information Security ROBs required for access or use of specific VA or non-VA systems. (SOURCE: AC-8)
- I WILL obtain approval from the Office of Public and Intergovernmental Affairs (OPIA) before establishing a VA social media account.

1.7 What to Expect and Course Completion

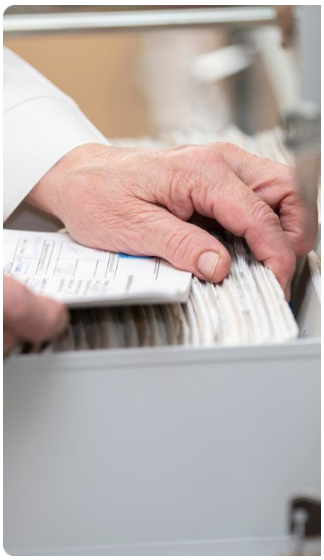
During this course, you can expect to gain a better understanding of your roles and responsibilities for protecting VA information and information systems. You will also learn how you can help with records management. In addition, this course may satisfy the annual mobile device training requirement, if you have completed this course at the time the mobile device is requested. Most importantly, you will explore how the ROBs apply in your day-to-day work as you use your problem-solving skills to promote VA's mission of service to the Veteran.

Practical, realistic scenarios that put privacy and security at risk are presented during this course. For each scenario, you will have the chance to identify the best action to take. Then you'll get feedback to help you understand the best action to take as well as the related ROBs that apply to the situation.

After reviewing all the topics in the course, you will select your user type and then print, initial each page of, and sign the ROB. This is required to achieve completion credit for this course. After completing these requirements, contact your supervisor or Contracting Officer Representative (COR) to submit the signed ROB and to coordinate with your local Talent Management System (TMS) Administrator to ensure you receive credit for completion.

Topic 2: Handling VA Information

2.1 Introduction and Objectives



Veterans, their families, and your colleagues depend on you to show good judgment when you access or handle VA sensitive information. Treat the information of others and VA with the same care that you would your own, laying the groundwork for a stronger, safer tomorrow.

When you have completed this topic, you will be able to do the following:

- Recognize your role in protecting VA information that you handle
- Identify common problems when handling VA information.

This topic will provide you with situations and information on properly handling VA sensitive information as we work together to construct a secure future for VA.

2.2 Protecting and Disclosing VA Sensitive Information

It is your duty to protect VA sensitive information, such as SPI, which includes personal information and health information. This information can be as simple as names and addresses or as significant as a medical diagnosis combined with another identifier, like a Social Security number.

The requirements and safeguards in place do not apply only to Veterans, but also to your fellow VA colleagues, contractors, and anyone else who uses VA systems and services.

A key part of protecting VA sensitive information is following best practices for information disclosure. Disclose VA sensitive information only at the right times to the right people. This includes sending information to other federal agencies and partners, whether by email or regular mail. Before disclosing or releasing information, you must be authorized by law to do so for official business purposes. The intentional theft of VA sensitive information is a constant threat that employees must be aware of at all times, including when working remotely and using web-based collaboration tools like Microsoft Teams and SharePoint. When using these tools, take care not to share SPI with employees, contractors, or others who aren't authorized to receive it. Also ensure that the appropriate access controls and user permission reviews are in place. If you are unsure, check with your supervisor, Information System Security Officer (ISSO), or Privacy Officer (PO) before sending the information.

Unless authorized by the head of the agency, Social Security numbers should not be used as the primary identifier for Veterans or included on documents sent by mail. VA has developed regulations to determine exemption requirements for Social Security numbers on documents sent by mail. For a list of these exemptions, visit the Social Security Number Reduction page on the VA Privacy Service site. A link to this page can be found in Resources.

Before using, mailing, or collecting Social Security numbers or any other form of SPI, you should talk to your PO and supervisor. They will help decide whether there is a business need that meets the policy

for acceptable use in accordance with VA Handbook 6507.1, *Acceptable Uses of the Social Security Number (SSN) and the VA SSN Review Board*. Then, consult with your local ISSO to ensure that all proper security controls are in place.

2.3 Scenario: Reducing the Use of Social Security Numbers

Scenario

You are preparing to send out pre-populated letters to several hundred Veterans. You notice that full Social Security numbers have been printed on the letters. What should you do?

Determine the best answer from the options provided.

A. The automated system included Social Security numbers on the letters, so they must be important. Go ahead and mail everything out.

B. Social Security numbers should not be included on mailed documents unless authorized. Contact your PO for guidance before sending.

Feedback

The correct answer is B.

Per the Social Security Number Fraud Prevention Act of 2017 and related policies, SSNs should not be included on any documents sent by mail or used as the primary identifier for Veterans, employees, or VA staff unless authorized by the head of the agency in accordance with regulations.

If the use of Social Security numbers is not required to fulfill an official function or mission, it should be eliminated as part of the ongoing reduction and removal effort.

Wherever possible, try to use alternative identifiers, such as date of birth, address, phone number, and others. Talk to your PO and supervisor for further guidance.

Note that some documents will continue to be mailed and pre-populated with full Social Security numbers due to legal requirements and business needs. VA has developed regulations to determine exemption requirements for Social Security numbers on documents sent by mail. For a list of these exemptions, visit the Social Security Number Reduction page on the VA Privacy Service site. A link to this page can be found in Resources.

Additional guidance is outlined in the Paperwork Reduction Act (PRA), Consolidated Appropriations Act, OMB Memorandum 17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information*, and 38 U.S.C. § 5101 of VA Regulatory Identification Number (RIN) 2900-AR19-Final Rule.

For information on the privacy requirements of these acts, reach out to the VA Privacy Service. For information on data requests and survey requirements, reach out to the Office of Research & Development and the Office of Enterprise Integration. These offices can help you decide whether there is a business need grounded in law that meets the guidelines for acceptable use as defined in Directive 6309, *Collections of Information* and Directive 6507, *Reducing the Use of Social Security Numbers*.

Rules of Behavior

Organizational Users

I WILL comply with all Federal statutes, regulations and policies applicable to VA information security, information privacy/disclosure and records management. (SOURCE: PM-10)

I WILL protect VA sensitive information aggregated in lists, databases or logbooks and include only the minimum necessary VA sensitive information to perform a legitimate business function. (SOURCE: AC-21)

Non-Organizational Users

I WILL comply with all Federal statutes, regulations, and policies applicable to VA information security, information privacy/disclosure, and records management policies. (SOURCE: PM-10)

2.4 Proper Handling of Information

There are three formats of VA information: physical (e.g., paper), electronic, and verbal. Here are some best practices for keeping VA sensitive information secure:

- Always store paper documents containing VA sensitive information securely when not in use.
- Make sure to clear your work area and secure any documents containing VA sensitive information before screensharing, turning on video, or leaving the room. These guidelines apply whether you're working remotely or onsite.
- When mailing sensitive documents, make sure that the envelopes are addressed correctly and contain only contents intended for that recipient to avoid mismailing incidents.
- Before faxing sensitive documents, confirm that the connection is secure, verify the fax number, and ensure that an authorized person is on the receiving end.
- Store electronic files and documents containing VA sensitive information on properly secured shared drives.
- Be careful where and when you talk about VA sensitive information. For example, discussing VA sensitive information in the elevator or at lunch in a cafeteria is a privacy and security risk. You never know who might be listening. To avoid these situations, make sure you are in an area where you can't be overheard (e.g., a meeting room) when discussing sensitive information.
- Be careful when you are speaking with Veterans in person or on the phone. If you are speaking in person, take precautions so that your conversation can't be overheard by others. If you are speaking with a Veteran over the phone, verify they are in a location where they can give you sensitive information without being overheard.

2.5 Scenario: Preventing Mismailing

Scenario

You're preparing to mail out sensitive documentation to Veterans. As you stuff the last envelope, you realize that the recipient information on the front doesn't match the documentation inside. What should you do?

Determine the best answer from the option provided.

A. You may have accidentally included the wrong documentation in other envelopes as well. Go back and check each one to avoid a privacy incident.

B. It's probably an isolated issue. Update the incorrect address quickly and then send everything out.

Feedback

The correct answer is A. When manually preparing documents for mailing, you should always be cautious. Take the time to make sure the name on each envelope matches the name on the documentation inside the envelope. Also, make sure that only necessary information appears on the envelope for mailing purposes. These same guidelines apply when mailing electronic forms of VA sensitive information as well, such as Digital Video Discs (DVDs) or other media storage devices.

Mismailing is one of the top ten reported privacy incidents that continue to affect VA. It carries the potential for identity theft, invasion of privacy, and loss of trust in VA's ability to protect the sensitive information entrusted to us. Use only officially authorized methods and approved systems for transferring and mailing sensitive documents on behalf of VA, as outlined in VA Directive 6609, *Mailing of Sensitive Personal Information*. If there is an incident or a suspected incident, report it to your supervisor, your local ISSO, and the PO.

Note that you should exercise the same care when sending fax communications. Before transmitting VA sensitive information over fax, you should ensure that there's no other way to send the information securely. You should also verify the fax number and confirm that an authorized person is on the receiving end.

Rules of Behavior

Organizational Users

I WILL transmit VA sensitive information via fax only when no other reasonable means exist and when either someone is at the receiving machine to receive the transmission or the receiving machine is in a secure location. (SOURCE: AC-19)

I WILL NOT make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

Non-Organizational Users

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

2.6 Records Management Awareness

VA business records are managed according to federal regulations. As a VA employee, it is your responsibility to know proper records management to comply with the Federal Records Act of 1950.

Federal records come in many formats. You should become familiar with what could be a record.

Determining whether a particular document is a record or nonrecord does not depend on whether it is an original or a copy. For example, several copies of a single form may each have record status if each serves a separate administrative purpose and is maintained in a different filing system. A single set of publications should be designated as a record copy, as distinguished from copies found elsewhere or stocks of the same publication. Documentary materials are records when they meet both of the following criteria:

- They were made or received by a federal government agency while transacting agency business, and
- They are appropriate for preservation either as evidence of the agency's organization, functions, and activities or because of the value of the information they contain. Source: *Records Management for Everyone* (VA TMS ID: 4192704).

Consult with your supervisor or Designated Records Management Official if you are creating, transporting, storing, or disposing of materials that might be records. A Records Control Schedule (RCS) describes the requirements needed to maintain and dispose of federal records.

VA records may also include emails, text messages, or messages sent via Microsoft Teams, so be careful about deleting them. Refer to Memorandum VAIQ 09726796, *Proper Use of Email and Other Messaging Applications,* for more guidance.

There are specific ROBs that apply to records management. They are as follows:

- I WILL comply with all Federal statutes, regulations and policies applicable to VA information security, information privacy/disclosure and records management. (SOURCE: PM-10)
- I WILL recognize that access to certain databases has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. (SOURCE: SC-28)
- I WILL NOT have any expectation of privacy in any information I access, create, receive or maintain, or in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. (SOURCE: AC-10)

Note that VA is launching a new Electronic Health Record (EHR) system to store and track patient medical information. The new system connects VA medical facilities with the Department of Defense,

the U.S. Coast Guard, and participating community care providers, allowing clinicians to easily access a Veteran's full medical history in one location. The VA EHRM Integration Office manages deployment of the new system. (Source: VA EHRM Intranet site)

This ongoing transition will affect the way that sensitive health records are handled and accessed, so it's important to stay aware of the latest policies and guidance. Visit the Electronic Health Record Modernization Integration Office (EHRM-IO) intranet site for information on program management and oversight of the EHRM implementation effort. The intranet site address can be found in Resources. To learn more about records management, you're encouraged to take *Records Management for Everyone* (VA TMS ID: 4192704). You can also search for other related courses on VA's TMS.

2.7 Summary

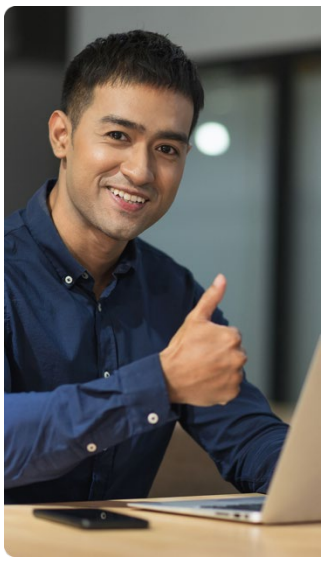
VA sensitive information comes in many formats, and you must be careful when handling it. Otherwise, you may face consequences, including fines or suspension. It is not always easy, but it is necessary to take such precautions to protect Veterans, their families, and other VA system users, including employees and contractors.

You should follow the blueprint for handling VA sensitive information with these best practices:

- Protect all VA sensitive information, in any format (i.e., physical, verbal, electronic), as if it were your own.
- Securely safeguard and handle paper and electronic documents to avoid unauthorized disclosure of sensitive information.
- Verify that names and addresses match and that only the content for the intended recipient is included when mailing sensitive information.
- Know what a record is and understand your responsibilities for records management.

Topic 3: Protecting VA Electronic Resources

3.1 Introduction and Objectives



It is your responsibility to track, protect, and care for all VA electronic devices and resources that you access or that are issued to you. This includes protecting the information on those devices, which is covered in Topic 5: Safeguarding VA Electronic Information.

When you have completed this topic, you will be able to do the following:

- Recall steps to protect VA electronic resources
- Recognize procedures for reporting theft or misuse of VA devices
- Identify best practices and recertification for users of VA-provided mobile devices.

In this topic, you will find situations that deal with proper use and maintenance of VA devices and equipment, information about best practices, and annual training for users of VA-issued mobile devices.

3.2 VA-Issued Electronic Resources

Like many workplaces, VA issues equipment so employees can perform their daily duties based on their job requirements. Equipment includes laptop or desktop computers, mobile phones, and tablets. Protect these resources as you would your own. Only VA-approved devices are allowed on the VA network.

Keep in mind that the Office of Information and Technology (OIT) has implemented the VA IT One + One Device Policy, which limits employees to no more than one IT computing device. Your supervisor or COR will determine which device is more appropriate: a desktop for office use or a laptop for home or travel use if business needs dictate a more portable solution. If you have mobility needs, you can be provided with a VA-issued mobile device as well as one computing device, with supervisor permission. The End User Class Matrix provides guidelines on device class selection. A link to this matrix can be found in Resources. (Source: VA Directive 6011, *VA IT One + One Device Policy*)

The following are some basic guidelines for VA-issued devices:

- If you need repair or maintenance for your VA-issued equipment, use only those authorized by OIT to repair your equipment.
- If you experience theft or loss of VA-issued devices, report it as soon as it is discovered to your supervisor, local ISSO, and PO.
    - If you don't know the name of your local ISSO or PO, you can check the PO/ISSO locator website. A link to this site can be found in Resources.

  - You should also contact the VA Police in the case of suspected theft or other physical security threats.
- If you find VA equipment unattended, notify your local ISSO or the VA Police.
  - You should also report any Veteran-owned personal devices that are left on VA property and turn them in to the VA Police upon discovery. These devices may be configured to access, or could contain, sensitive information.
- If you need to travel with a VA-issued device or transport it outside a VA-protected environment, make sure that you comply with security measures and obtain any necessary approvals, such as an Authority to Transport. VA-issued devices should never be taken out of the country or on personal travel without permission.

If you are relocating or changing job roles within VA, you should coordinate the details of the move with the proper authorities to ensure that your equipment is accounted for. If you are leaving your current duty station within VA, remember to coordinate with your local OIT office to return your equipment and devices or transfer them to your new OIT servicing area. If you leave VA, you must work with your supervisor to return and out-process all VA devices, equipment, badges, and records. Contractors must also turn in VA-issued electronic resources at the end of the contract.

There are criminal penalties for the unlawful removal of federal records. Before separating from VA, you must transfer custody of all federal records to your supervisor or COR. You must also remove any encryption or security measures from the files and documents so your supervisor or COR can access them.

Remember that you are not allowed to divulge any information that you had access to during your time with VA. (Sources: 18 U.S.C. 2071, VA Form 10-0708)

3.3 Scenario: Loss or Misuse of VA Equipment

Scenario

You need to make an important business call but can't find your VA-issued device. It's not in any of the usual places. What should you do first?

Determine the best answer from the options provided.

A. Give yourself some time to find the missing device before alarming anyone. It's probably somewhere nearby.

B. Report the loss to your supervisor, ISSO, and PO immediately or as soon as able.

Feedback

The correct answer is B.

If you lose or misplace a Government-Furnished Equipment (GFE) device, you should contact your supervisor, ISSO, and PO as soon as you're able. You should also contact the VA Police in the case of suspected theft or other physical security threats.

Additionally, make sure that you follow administration-specific reporting guidelines. For example, those who work in VHA medical centers should report incidents occurring after hours to their Administrator of the Day (AOD).

If a security incident occurs outside of business hours, reach out to the Enterprise Service Desk (ESD) for immediate response. Contact information for the ESD is available in Resources. The ESD is open 24/7 and can take appropriate measures until you're able to report to your supervisor, ISSO, and PO. In some cases, VA technicians may be able to locate lost devices. They can also remotely wipe or disable stolen phones and laptops to avoid unauthorized disclosure of VA sensitive information.

Upon receiving a new VA-issued mobile device, you'll be prompted to set up a secure Personal Identification Number (PIN) code shortly after activation, which helps avoid disclosure of VA sensitive information on lost or stolen phones.

Note that VA mobile devices should never be taken out of the country without permission. If you need to travel with GFE, make sure that you put in a request and receive the appropriate approvals.

Remember, it's your responsibility to protect VA assets from theft, loss, fraud, and abuse. Never leave your work devices (e.g., laptops, mobile phones, tablets) unattended, even on VA property. If you do need to step away, ensure that devices are appropriately locked down or stowed away out of sight.

Physical security is very important, especially for devices that are connected to medical systems or diagnostic equipment.

Although most VA devices are encrypted and set to lock, they may still contain sensitive information that could be accessed and used for identity theft or other harmful purposes. Check the status of your devices regularly to ensure that appropriate protections are in place.

If you find someone else's VA equipment unattended, notify your local ISSO or the VA Police.

The loss, theft, or misuse of GFE is a serious issue that should be reported as soon as it's discovered, in accordance with the ROBs.

Rules of Behavior

Organizational Users

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

I WILL secure mobile devices (e.g., laptops, tablets, smartphones) and portable storage devices (e.g., compact discs, digital video discs, universal serial bus flash drives). (SOURCE: PE-4)

I WILL report suspected or identified information security incidents, including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

Non-Organizational Users

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

I WILL report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant alert messages (security and privacy) on VA information systems to the enterprise service desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

3.4 Software Downloads

Install only software that is VA-approved and compliant with software licensing and copyright restrictions on VA-issued devices. Do not download software from the internet to your VA-owned systems unless you have been authorized to do so. This includes free trials and open-source software.

Downloading unauthorized third-party software could expose VA systems and endpoints to malicious threats or cyberattacks. You can help increase security by only downloading VA-approved software and ensuring that the latest antivirus updates are installed. If you begin receiving antivirus alerts or suspect that malicious software has been downloaded, report the incident to your supervisor, ISSO, and PO immediately.

For more information about approved software, please visit Resources for the link to the VA Technical Reference Model (TRM). If you need specific software to do your work that is not VA-approved, you should discuss it with your supervisor and submit a ticket through the ESD. They will route your request to the proper authority.

3.5 VA-Issued Mobile Device Security

Before being issued a VA mobile device, you must take *Mobile Training: Security of Apps on iOS Devices* (VA TMS ID: 3926744). Afterward, you must fulfill the annual refresher training requirement by completing this course.

Here are some best practices for securely using your VA-issued mobile device:

- Enroll GFE mobile devices in Workspace ONE® before downloading any apps.
- Use only VA-approved apps from the VA App Catalog to send, receive, or store VA sensitive information. Go to Resources for a link to view the allow list of apps that have been approved for VA business.
- To download apps that will NOT be used for handling VA sensitive information or interacting with the VA system—such as hotel, airline, and weather apps—use approved public app stores.
- Never download apps from any third-party source other than an approved app store. The link to the deny list of apps that are blocked from VA phones is available in Resources. Downloading unapproved applications on VA mobile devices is not allowed.

- If you are notified of a malicious app or other threat on your device, take the recommended steps to remove or correct it. VA's mobile security tool Lookout monitors all VA mobile devices, alerting users whenever a threat is detected. Non-compliant devices may be removed from the network.
- Remember, VA sensitive information stored on a VA-issued mobile device must be encrypted.
- Enable and use Wi-Fi for automatic Operating System (OS) updates.
- Never allow remote access requests from anyone other than an authorized VA official.

For more detailed information, review VA Handbook 6500.10, *Mobile Device Security Policy*.

3.6 Handling VA-Issued Mobile Devices

Mobile phones and tablets/iPads are becoming standard devices for daily work, just like laptops. The two greatest conveniences of mobile devices, size and mobility, are also their greatest weaknesses. That's because their size and mobility make them easy to steal, lose, or misuse.

VA uses a mobile device management system to centrally manage all VA-issued mobile devices. While the risk of data breaches and privacy incidents on VA mobile devices is low, you should stay aware and vigilant. Loss or theft of mobile devices and equipment can have negative privacy and security impacts, such as the compromise of VA sensitive information.

When switching duty stations, it's important to coordinate with your local OIT office to return your equipment and devices or transfer them to your new OIT servicing area.

If you have a VA mobile device, review the guidance below:

- Follow all mobile-specific VA ROBs for your user type as agreed to and report any suspected or actual incidents to your local ISSO or PO.
- Follow all guidance for accessing apps from the VA App Store (hosted by VA Mobile), the VA App Catalog, and public app stores.
- Do not use text messaging or third-party Short Message Service (SMS) apps not offered in the VA App Catalog to conduct VA business or send VA sensitive information unless specifically approved by the appropriate authorities. Contact your local ISSO or PO for more information.
- Observe limited personal use of the device as stated in VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*.
- If you are leaving VA or transferring to a new duty station, coordinate with your local OIT office to return your equipment and devices or transfer them to your new OIT servicing area.

3.7 Scenario: GFE, Personal Devices, and Personal Use

Scenario

It's the middle of the workday, and your personal mobile device battery is running low. Would it be ok to charge the device by plugging it in to one of your GFE laptop's Universal Serial Bus (USB) ports?

Determine the best answer from the options provided.

A. Sure. Where's the harm? It's just a quick charge.

B. No. You should keep GFE separate from personal property.

Feedback

The correct answer is B. You should never plug personal smart watches, phones, tablets, printers, or other devices into GFE such as laptops, desktop computers, or VA-provided docking stations. Remember, personally owned mobile devices are not allowed to be connected to the VA network or used to store or communicate VA data. Even charging the device creates a risk of unauthorized access, data theft, or harm to VA systems.

Note that this guidance applies to wireless connections, such as Bluetooth, as well as physical connections via USB.

Most unauthorized connections to USB ports will be blocked based on the configuration of the GFE. However, this isn't always the case and is not a guaranteed fail-safe. If you have a business need to connect a blocked device to VA-issued equipment, contact the ESD to determine the appropriate method for submitting a request.

Keep GFE and sensitive information safe, secure, and separate from personal devices and information.

This also means that you should avoid using GFE to access social media or other personal sites unless it's for a work-related purpose. You should always observe limited personal use of VA-issued devices in compliance with VA Directive 6001. Note that unapproved sites will be blocked by the firewall. However, even if a site is approved, that doesn't mean you can use it in ways that interfere with your duties or go against policy. Misuse of approved sites will be handled on a case-by-case basis by your supervisor.

Rules of Behavior

Organizational Users

I WILL keep Government-furnished equipment (GFE) and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

I WILL limit the personal use of social media/networking sites, in accordance with VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology. (SOURCE: AC-8)

Non-Organizational Users

I WILL keep GFE and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

I WILL limit the personal use of social media/networking sites, in accordance with VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology. (SOURCE: AC-8)

3.8 Summary

Just as you handle VA sensitive information with care, you must also make smart choices to protect the devices and resources that store and process that information.

Topic 4: Accessing VA Information

4.1 Introduction and Objectives

VA information systems can be accessed in many ways but should be accessed only by those who have a valid need-to-know and the proper credentials. Knowing how to do so securely is important to maintain the integrity of the system.

When you have completed this topic, you will be able to do the following:

- Identify common situations and methods used when protecting access to VA information systems
- Recognize the steps to protect access to VA information and systems.

In this topic, you will find situations that deal with accessing VA systems and information properly and how to protect your access to such systems and information.

4.2 Need-to-Know and Minimum Access

The need-to-know principle means you should have access only to information, programs, and systems that you need to perform your official duties. Also, you should have access only to the minimum necessary information. Remember, never provide access to information to anyone who doesn't have an authorized need-to-know. This practice helps support the federal strategy of Zero Trust.

VA is moving toward the federal strategy of Zero Trust, per OMB-M22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. With this strategy, no actor, system, network, or service operating outside or within the security perimeter is trusted. Anything or anyone attempting to establish access must always be verified to protect the organization against growing threats. The Zero Trust strategy also helps guide risk management practices for the cybersecurity supply chain. For more information, please visit Resources for the link to the Zero Trust First Cybersecurity Strategy.

In addition, employees must validate the need-to-know for information managed by their office. For example, if your office maintains a Microsoft Teams or SharePoint site, you have a responsibility to ensure that access is limited to those who have a need-to-know, per VA Directive 6515, *Use of Web-Based Collaboration Technologies*.

If you have access to a system you no longer need or more access than you need, this violates the need-to-know principle. Having access you no longer need increases your risk of being an insider threat. This could expose VA sensitive information; invade the privacy of Veterans, colleagues, and employees; and cause possible risk to VA. Let your supervisor know when you no longer need access to a system so that you can be removed from it. This helps keep your risk of being an insider threat low.

Typically, your access will need to be updated whenever you change jobs within VA. Work with your supervisor, ISSO, Records Management Officer, and PO to take care of system access and any physical records you have before changing jobs, retiring, or leaving VA.

4.3 Scenario: Need-to-Know

Scenario

While checking in patients at a VA medical facility, a coworker shows you a lookup tool you can use to verify Veteran appointment times. You realize that this tool contains sensitive information you don't need access to for your job, such as treatment, payment, and health records. What should you do?

Determine the best answer from the options provided.

A. Let your supervisor know that you and your coworker have access to information that exceeds your need-to-know.

B. Continue using the tool. You can just ignore the information you don't need.

Feedback

The correct answer is A.

You should let your supervisor and the appropriate authorities know if you have access to information, programs, or systems that you don't need.

Following the need-to-know principles helps protect the privacy of Veterans and reduces your risk of being an insider threat.

To ensure that you have access to only the minimum necessary information, work with your supervisor, ISSO, Records Management Officer, and PO. They will help take care of your system access and physical records before you change jobs or leave the organization.

Also, never provide access to VA sensitive information unless the requesting party has a verified need-to-know for official business purposes. Even if the requesting party is an authorized entity, you should still reach out to the appropriate authorities, such as your supervisor, local ISSO, or local PO, to verify that they have a need-to-know. If they do, provide only the minimum necessary information through a properly encrypted email or other VA-approved method.

If you maintain or provide access to sensitive records, such as medical diagnoses or treatments, without the appropriate legal authority, you are in violation not only of the VA ROB but also of federal law. There must be a valid, professional, duty-related reason for you to share access with anyone, whether they are inside or outside the organization. In cases when an external party is requesting information, direct them to the facility’s Release of Information Office, Freedom of Information Act Officer, or PO for assistance.

Rules of Behavior

Organizational Users

I WILL only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties. (SOURCE: AC-21)

I WILL ensure responsible practices whenever Veteran data is accessed or used in accordance with VA policy and guidance. (SOURCE: AC-21)

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

Non-Organizational Users

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

4.4 Identification and Authentication

You use your VA credentials, also known as a Personal Identity Verification (PIV) card, to access VA facilities, systems, and information.

You provide this identification to show that you are authorized to be in a VA facility, and you use it to authenticate your access to VA systems. This card should be treated like your credit card or passport; it is an important piece of identification for you and is part of VA's standard method for controlling access to information and systems.

The security certificates on your PIV card and your PIN authenticate you to use VA systems. You should secure any PINs, passwords, passcodes, or other forms of authentication you may use; never share this information with others.

See VA Directive and Handbook 6510, *VA Identity and Access Management*, for more detailed information on how VA manages credentials and access to VA systems.

4.5 Scenario: Lost PIV Card

Scenario

You're returning to work after lunch. When you get back to your office, you can't find your PIV card. It isn't in your wallet or your lanyard. What should you do first?

Determine the best answer from the options provided.

A. Notify the local PIV Card Issuing (PCI) Facility, the VA Police, and your ISSO immediately.

B. Give it a day. It will probably turn up soon.

Feedback

The correct answer is A.

For a lost or stolen PIV card, you should notify local PCI Facility personnel, the VA Police, and your ISSO within 4 hours.

For awareness and incident tracking purposes, you should also contact your supervisor and the ESD, which is open 24/7.

The longer the card is missing, the greater the threat of unauthorized access becomes. All lost or stolen credentials must be reported to the PCI Facility within 24 hours of discovery or on the next business day.

While waiting for the card to be replaced, you can contact the ESD for temporary exemption and system access.

Lost PIV cards continue to be one of the most commonly reported security incidents, often occurring in remote environments. For this reason, you should take care to protect your PIV card, passwords, and credentials at all times, securing them just as you would your driver's license or credit cards.

Remember, PIV cards contain your employee identification and system access information. They can be used to access not only VA computers and information, but also facilities and secure areas. Failure to protect your security tokens from loss or theft can have serious consequences.

Rules of Behavior

Organizational Users

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

I WILL report suspected or identified information security incidents, including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

I WILL protect my passwords; verify codes, tokens and credentials from unauthorized use and disclosure. (SOURCE: IA-5)

I WILL maintain possession and display my VA credentials as required by VA policy. (SOURCE: IA-5)

Non-Organizational Users

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

I WILL report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant alert messages (security and privacy) on VA information systems to the enterprise service desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

I WILL protect my passwords, verification codes, tokens, and credentials to prevent unauthorized use and disclosure. (SOURCE: IA-5)

I WILL maintain possession of my identification credential or VA Personal Identification Verification (PIV) card on or about my person while attending to officially authorized and assigned duties. (SOURCE: AC-3)

4.6 Scenario: Securing Workstations

Scenario

You are working with some sensitive documents at your desk. A coworker stops by and asks if you can come assist a Veteran with a pressing issue. You don't want to leave your workstation unsecured, but you also don't want to keep the Veteran waiting. What should you do? Determine the best answer from the options provided.

A. Take the time to remove your PIV card, log off, and stow the sensitive documents securely out of sight.

B. Ask an officemate to keep an eye on your computer while you step away.

Feedback

The correct answer is A.

In order to protect VA sensitive information, you should remove your PIV card and lock your workstation whenever you leave your workstation or computer. At the end of the day or during a shift change, you should also remove your PIV card and log out of all your systems and computers. While most VA computers will lock automatically after a certain period of inactivity, they may remain open long enough for someone to access the network without permission.

Keep in mind that simply removing your PIV card will not automatically lock your computer or—in the case of on-site workers—break the network connection. For remote workers, removing the PIV card may disconnect you, but any sensitive information that is pulled up onscreen or downloaded locally will still be accessible and exposed until timeout. To properly secure your workstation, you should always remove your PIV card and lock your computer before leaving.

Make sure that you follow clean desk guidance to keep your work area clear and protect VA sensitive information when you are not there. This is especially important in shared or hybrid workspaces. If you have a private office, close and lock the door when it’s unattended. Even if you’re working from home, you should make sure to remove your PIV card, lock your computer, and secure them if they're not in use. If you notice any violations—such as an unattended PIV card, exposed VA sensitive information, or unsecured equipment—inform the appropriate supervisor, ISSO, and PO. ISSOs can and will do audits to make sure that staff are following guidelines for securing their workstations and PIV cards.

Rules of Behavior

Organizational Users

I WILL log out of all information systems at the end of each workday. (SOURCE: AC-11)

I WILL log off or lock any VA computer or console before leaving my workstation, whether at a VA location or alternate worksite. (SOURCE: AC-11)

I WILL protect VA sensitive information from unauthorized disclosure, use, modification or destruction and use encryption products approved and provided by VA to protect sensitive data. (SOURCE: AC-19)

I WILL report suspected or identified information security incidents, including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

Non-Organizational Users

I WILL log off or lock any computer or console with access to or displaying VA information before I leave my workstation. (SOURCE: AC-11)

I WILL report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant alert messages (security and privacy) on VA information systems to the enterprise service desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

4.7 Unsecured Wireless Connections

Unsecured wireless networks may be convenient for quickly checking social media updates or personal emails during personal time. However, it is not appropriate to use an unsecured wireless connection to conduct VA business. This includes guest wireless connections. You must go through the proper process to connect to the VA network to avoid data breaches or unauthorized disclosures. Use the approved methodologies to access VA networks, like the Citrix Access Gateway (CAG), Azure Virtual Desktop (AVD), or Remote Enterprise Security Compliance Update Environment (RESCUE). Other remote access modalities include GFE Mobile and the VA Virtual Office (VAVO).

The VA network has the encryption and data protection services required to securely handle sensitive information. VA Directive 6512, *Secure Wireless Technology*, states that sensitive information must NOT be transmitted via wireless technology unless it is properly encrypted to Federal Information Processing Standard (FIPS) 140-2 standards (or its successor, FIPS 140-3) and the wireless technology is operating as intended.

4.8 Scenario: Unsecured Wireless Connections

Scenario

The secure network goes down at your VA facility, but the guest Wi-Fi is still working. You need to send a sensitive document to your supervisor from your GFE work device. What's the safest way to take care of this issue?

Determine the best answer from the options provided.

A. Go ahead and connect to the guest Wi-Fi. You're in a VA facility, so it should be fine.

B. Wait until you can reconnect to a secure access point. Better safe than sorry.

Feedback

The correct answer is B.

Guest and public wireless systems do not have restrictive access controls; they are accessible by anyone. When you connect to unsecured Wi-Fi networks, you increase the risk of privacy incidents and data breaches. To reduce exposure, avoid using guest Wi-Fi or public hotspots to conduct VA business. In cases where you must use guest Wi-Fi, remember that any locally stored VA sensitive information is at risk and any action like uploading or taking screen captures of this data must be avoided. On the VA guest Wi-Fi, you don't know the other users and their intentions. Be mindful and, if possible, use only secure access points. Approved remote access methods include CAG, AVD, and RESCUE.

Rules of Behavior

Organizational Users

I WILL protect VA sensitive information from unauthorized disclosure, use, modification or destruction and use encryption products approved and provided by VA to protect sensitive data. (SOURCE: AC-19)

I WILL NOT transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption and properly authorized to release the data. (SOURCE: AC-18)

Non-Organizational Users

I WILL NOT transmit VA sensitive information via wireless technologies unless the connection uses Federal Information Processing Standards (FIPS) 140-2 (or its successor) validated encryption and properly authorized to release the data. (SOURCE: AC-18)

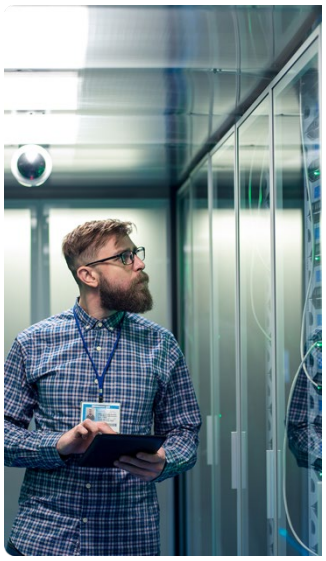
4.9 Summary

Access to VA networks and information is essential for doing your job. It is extremely important that you keep all your forms of access, identification, and authentication safe. This not only protects Veterans but also protects you, your fellow employees, and everyone else on the job site. You must do the following:

- Access only systems and information for which you have the need-to-know to do your job.
- Always secure your PIV card.
- Protect all credentials and passwords you have for VA system access.
- Never conduct official VA business on an unsecured network.

Topic 5: Safeguarding VA Electronic Information

5.1 Introduction and Objectives



Just as information in physical forms (e.g., paper) has information security and privacy risks and concerns, electronic information has its own set of risks and concerns that we must consider when drawing up our privacy and security plans. Electronic information requires constant oversight to protect it from theft or tampering. It's very important to properly safeguard electronic information due to the ease with which it can be accessed, lost, or exposed.

When you have completed this topic, you will be able to do the following:

- Describe best practices for handling electronic VA sensitive information
- Identify potential types of incidents that might expose VA sensitive information.

In this topic, you will find information and scenarios that help you determine how to work with electronic information and how to protect it.

5.2 Transmitting Data Securely

When you need to send VA sensitive information, it must be secure in order to prevent unauthorized access and protect the information.

Encrypted email is one approved method for transmitting VA sensitive information. You must encrypt sensitive emails and file attachments. Sending emails with unencrypted sensitive information can result in security breaches and possible identity theft if the information is accessed by unauthorized individuals.

Faxing is another approved method, if there is no other reasonable means to transmit the information. Before sending VA sensitive information via fax, you should confirm that the connection is secure, that the fax number is correct, and that an appropriate person is on the other end to receive the fax.

5.3 Guidelines for Emailing VA Sensitive Information

Apply the following guidelines when emailing VA sensitive information.

- Encrypt only emails that contain VA sensitive information. Emails not containing sensitive information should not be encrypted.
- Do not put VA sensitive information in the subject line of an email because it cannot be encrypted.

- Use Azure Information Protection (AIP), formerly Azure Rights Management System (RMS), which is the preferred method of encrypting emails containing VA sensitive information.
  - To encrypt an email, complete the following two steps:
    1) Select the **Sensitivity** button from the **Message** tab in the main Microsoft Outlook ribbon.
    2) Then select **Encrypt-Only** from the list of **Legacy Templates**. This template can be used to protect communications to internal and external recipients.
  - For Veterans Benefits Administration (VBA) staff, the email setting normally defaults to auto-encrypt to decrease the risk of unencrypted sensitive emails. However, VBA users are required to adjust the settings to deselect encryption for emails that do not contain sensitive information.
  - For VHA staff, the decision of whether VA sensitive information may be sent via encrypted email using Azure AIP for a specific VHA activity will be made by the VHA Program Office that oversees that activity. For more information, contact the Office of Connected Care Help Desk. Links and contact information can be found in Resources.

Note that patient-provider communication is transmitted by secure messaging through the My HealtheVet portal, which is moving to a new home on VA.gov. The new My HealtheVet portal on VA.gov will provide a single place for Veterans to manage their healthcare needs in the same location where they manage their own VA benefits and services. The new health home will be easy to find, understand and use and will combine tools and features from My HealtheVet and My VA Health (Oracle Cerner) into one unified patient portal.

The VA Health and Benefits mobile app is another tool that Veterans can use to send and receive secure messages to and from their VA health care team.

Take the necessary precautions to prevent loss of VA sensitive information. For more information on these encryption methods, visit Resources.

5.4 Use VA Email for VA Business

Because emails can be considered official records for records management, it is very important that you use your VA email for all official VA business. VA email is set up with safeguards in place to protect VA sensitive information from further transmission, unauthorized access, destruction, or tampering.

Do not auto-forward your VA email to accounts of external email services like Gmail or Yahoo or to contractor accounts. Do not email VA sensitive information to your personal email or other unofficial email accounts, even when working remotely. If external services are used, VA loses the ability to keep full records of business communications.

To ensure best use of government resources, your VA email address should be used for business purposes only. Avoid using your VA email for personal or non-work-related reasons.

For more information, review Memorandum VAIQ 09726796, *Proper Use of Email and Other Messaging Applications.*

If there is a problem or for some reason you cannot use your official VA email, ensure proper recordkeeping by one of the following:

- Copy (cc) your official email address with @va.gov as the domain name so that the message is sent simultaneously to your official account at the moment of transmission.
- Forward a complete copy of the message to your official email address within 20 days of the official transmission.

Remember, DO NOT transmit VA sensitive information via personal email even if you copy (cc) your official va.gov email account.

VA contractors may be allowed to use their corporate email accounts if they do not have access to a VA email account and the security requirements are met. Contact your COR for approval to use corporate email accounts.

5.5 Scenario: Emailing VA Sensitive Information

Scenario

You need to send some sensitive information to certain members of your office mailgroup, but you can't remember who is authorized to receive it. You're also unsure of whether the email needs to be encrypted. What should you do?

Determine the best answer from the options provided.

A. Send the information to the entire group for awareness. They are all VA employees, so there's no need to encrypt the email.

B. Send the information only to those with a verified need-to-know. The email contains sensitive information, so it should be encrypted.

Feedback

The correct answer is B.

You must encrypt sensitive emails and file attachments, as well as making sure that all recipients have a verified need-to-know for official business purposes. Also, do not include sensitive information in the subject line of an email because it cannot be encrypted. Sending emails with unencrypted sensitive information can result in security breaches, privacy incidents, and possible identity theft if the information is accessed by unauthorized individuals.

AIP, formerly Azure RMS, is the preferred method of encrypting emails containing VA sensitive information. To encrypt an email using AIP, complete the following two steps:

1) Select the **Sensitivity** button from the **Message** tab in the main Microsoft Outlook ribbon.
2) Then select **Encrypt-Only** from the list of **Legacy Templates**.

Make sure that you take all the necessary precautions to prevent loss of VA sensitive data in accordance with the ROB. Keep in mind that encryption is necessary only for emails that include sensitive information; non-sensitive messages should not be encrypted.

Rules of Behavior

Organizational Users

I WILL encrypt email, including attachments, that contain VA sensitive information. I will not encrypt email that does not include VA sensitive information, or any email excluded from the encryption requirement. (SOURCE: AC-19)

I WILL ensure responsible practices whenever Veteran data is accessed or used in accordance with VA policy and guidance. (SOURCE: AC-21)

I WILL only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties. (SOURCE: AC-21)

I WILL NOT make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

Non-Organizational Users

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

5.6 Storing and Sharing VA Sensitive Information

You may need to store and share VA sensitive information. Some options include a secured Microsoft SharePoint site within the VA network or a secured shared drive with appropriate permissions to store or share files, with supervisor approval. Microsoft Teams is another tool that is commonly used to store and share information at VA. As with any electronic platform, there are inherent risks in using these tools. You must keep them safe by limiting access to only those individuals with a need-to-know and by giving them only the minimum access they need to perform their job.

Documents containing any sensitive information should be stored and maintained in secured folders with access permissions based on need-to-know. Check with your supervisor and work with your local OIT staff to get your permissions set up. Make sure you monitor access to ensure only individuals with a current need-to-know have access. For guidance on the storage and access of shared sensitive resources, talk to your supervisor, PO, and/or ISSO.

You should also make sure that you regularly check your SharePoint sites, Teams sites, and shared drives to remove VA sensitive information when it's no longer needed. Outdated VA sensitive information should be disposed of according to the RCS. No files containing VA sensitive information should be stored on GFE local hard drives.

Also, do not use personally owned mobile devices to store or communicate VA sensitive information, or to connect to the VA network.

Remember, VA sensitive information may be a type of CUI and, if so, must follow the VA's CUI guidance. As you store and share VA sensitive information, make sure to apply best practices for safeguarding information that is controlled but unclassified. The VA Data Loss Prevention (DLP) Program plays an important role in this process.

The VA DLP Program helps us apply best practices for storing and sharing CUI and other sensitive VA information. The DLP Program strengthens controls and policies, develops technical solutions, and establishes awareness, training, and reporting to prevent the loss and leakage of VA sensitive information across VA and ensures Federal Information Security Modernization Act (FISMA) compliance.

5.7 Scenario: Storing and Sharing VA Sensitive Information

Scenario

You need to send some urgent sensitive information to your coworker, but you don't have your VA-issued device handy. Can you text the information from your personal phone so they'll see it right away?

Determine the best answer from the options provided.

A. Yes. They're authorized to receive the information, so it shouldn't be a problem.

B. No. Use a VA-authorized device to send the necessary information through encrypted email or VA-approved software.

Determine the best answer from the options provided.

Feedback

The correct answer is B.

You should never send VA sensitive information via text message, especially from a personal device. This can lead to a compromise of privacy and is a violation of policy.

Note that even if you're using a VA-issued device and VA-approved application, you should include only the minimum information necessary for authorized, business-related purposes, in compliance with VA policy. Remember, it's your responsibility to ensure responsible practices whenever VA sensitive information is shared or accessed.

Personally owned mobile devices may not be connected to the VA network and may not be used to store or communicate VA sensitive information.

All communication of VA sensitive information must take place on GFE through a VA-authorized application or method, such as encrypted email. For a list of approved mobile applications, consult the VA App Catalog. A link to the VA App Catalog is available in Resources.

Rules of Behavior

Organizational Users

I WILL NOT allow VA sensitive information to reside on non-VA systems or devices unless designated and authorized in advance by all appropriate individuals, including my VA supervisor and Information System Owner. (SOURCE: SC-28)

I WILL NOT make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

I WILL ensure responsible practices whenever Veteran data is accessed or used in accordance with VA policy and guidance. (SOURCE: AC-21)

Non-Organizational Users

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

5.8 Identity Theft

Many people have had to deal with identity theft or the threat of it. At VA, there are several methods used to combat this threat. Using care when handling VA sensitive information is a good start. The following are some tips for preventing identity theft:

- Release information only once the need-to-know is verified and the release is authorized.
- Verify that addresses and names match up for mailings or pharmacy information.
- Secure paper documents in locked drawers or cabinets and store VA sensitive information in appropriately secured or permissioned servers.
- Dispose of VA sensitive information properly when you are finished with it. If you have questions on proper disposal of VA sensitive information, ask your local ISSO, PO, or Records Management Officer for information.

Failure to properly defend against identity theft can have many negative impacts on you, the Veteran, and VA as a whole. Identity thieves may use VA sensitive information to cause financial, personal, and organizational harm. If you need to report possible identity theft, refer to Resources for information on the Identity Theft Help Line.

5.9 Scenario: Mishandling VA Sensitive Information on Shared Drives, Sites, and Tools

Scenario

Your office has set up a SharePoint and Teams site for collaboration purposes. While visiting the site, you notice that some of the shared files contain sensitive information not everyone is authorized to access. What should you do?

Determine the best answer from the options provided.

A. Report the discovery to your PO, ISSO, and supervisor.

B. Make a mental note to avoid those files in the future. You don't want to get in trouble.

Feedback

The correct answer is A.

If you notice an unsecured file, folder, or communication that contains VA sensitive information, report it to your PO, ISSO, and supervisor as soon as possible.

Be especially vigilant when using collaboration tools and sites like SharePoint or Teams. While these tools can make information sharing more convenient and efficient, they also come with risks. Many Microsoft 365 products are interconnected, meaning that files shared in one place may be accessible in others, possibly by those without a need-to-know. This creates the potential for data theft, insider threats, and harm to VA's reputation.

To avoid these issues, VA sensitive information should be stored only on properly secured drives, SharePoint and Teams sites, or other approved platforms with administrative control over all access and permission. To confirm these permissions, contact your supervisor and local OIT staff. They can also help you determine the appropriate sharing rules and site configurations.

As you are handling VA sensitive information across shared sites and drives, make sure that all parties have a need-to-know and that only the minimum necessary access is provided. Staff should be regularly reviewing who has access to SharePoint or Teams sites and removing those who lack a need-to-know. For more information, review the recent required action item for all Teams and SharePoint Owners/Admins. A link to this action item can be found in Resources.

Coordinate with your PO and Records Management Officer when a SharePoint site or secured folder is no longer needed in order to properly dispose of the VA sensitive information stored on it.

Rules of Behavior

Organizational Users

I WILL only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties. (SOURCE: AC-21)

I WILL only post sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place. (SOURCE: AC-21)

I WILL protect VA sensitive information aggregated in lists, databases or logbooks and include only the minimum necessary VA sensitive information to perform a legitimate business function. (SOURCE: AC-21)

I WILL only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties. (SOURCE: AC-21)

I WILL ensure responsible practices whenever Veteran data is accessed or used in accordance with VA policy and guidance. (SOURCE: AC-21)

I WILL NOT make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

Non-Organizational Users

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

5.10 Safeguarding External and Removable Media

External and removable media devices such as thumb drives, external hard drives, and mobile devices can make moving information very convenient. However, this also makes it easy to steal or misuse the information. For this reason, the ports on VA-issued equipment (including conference room laptops and desktops) are locked down by default to prevent access.

If you have been assigned removable or external media, you must treat it like any other VA-issued device, including the following guidelines:

- Protect VA sensitive information on that media.
- Lock up thumb drives or hard drives when not in use. When they are no longer needed or they do not work anymore, return them to your local OIT office for proper disposal.
- If you find external media unattended, turn it in to an ISSO or the VA Police.

If you have a business need to access media ports on VA-issued equipment, contact the ESD.

5.11 Internet and Social Media Awareness and Safety

Data protection software like Trellix, formerly McAfee, provides anti-spyware protection, virus protection, and firewall/intrusion detection on VA-issued computers and technology. These programs run in the background and are kept as up to date as possible by OIT staff to protect VA information. Usually, the data protection software will take care of threats and shut down unauthorized access attempts. However, as threats evolve, the software does not always block every cyberattack or dangerous website.

One of the biggest threats is unsafe web browsing. As you conduct work-based research, there are several things to be aware of concerning cyberattacks and unsafe websites. Select each browsing tip for more information:

- **Examine the URL**. There are indicators about the location and security of the information you are accessing in the URL. Check for "typo-squatting," which occurs when attackers create website URLs that contain common misspellings of legitimate websites (e.g., yayhoo.com instead of yahoo.com).
- **Do not automatically trust sites with HTTPS**. The HTTPS in the URL is not in itself an indication that the site is safe, merely an indication that the site uses encryption for the internet/network traffic to and from the website. Cyberattackers can use sites with Secure Socket Layer (SSL) encryption to mimic legitimate sites. Do not use links sent to you in an email; copy and paste that URL separately into a Google search to make sure it's the legitimate site. You can also check for the lock symbol that appears to the left of the URL. This indicates the site has a security certificate.
- **Beware of malware**. Malware refers to malicious software that's designed to compromise the confidentiality, integrity, or availability of data or systems. Malware is typically downloaded when a user visits an infected website or selects a link in a suspicious communication. Be on the lookout for phishing emails, smishing texts, and other fraudulent messages that urge you to open potentially malicious links or attachments. Also beware of free or enticing offers that seem too good to be true. These may be attempts to scam you into revealing sensitive information or downloading malware. There are many types of malware to be aware of, including viruses, worms, Trojan horses, and ransomware attacks. Ransomware blocks access to your data and sends you a pop-up message that your data is encrypted. Payment will often be demanded for your data to be released back to you. A phone number may be given in order to process that payment to fix the issue. If this occurs, immediately report it to your supervisor, local ISSO, and PO, as well as the ESD and VA Police.

Social media can also pose significant risks. Follow these best practices for social media usage:

- Never post VA sensitive information to social media sites, whether in an official VA capacity or privately.
- Never use social media to speak on behalf of VA, unless you've been authorized to do so.
- Avoid accessing or using social media on GFE unless it's for a work-related purpose. Misuse of these sites will be handled on a case-by-case basis by your supervisor.
- Don't accept connection requests or messages from people you don't know. Social media messages can contain malicious links and attachments, just like phishing emails.
- Refer to VA Directive 6515, *Use of Web-Based Collaboration Technologies*, for more detailed information on the official use of web-based collaboration tools or social media sites. You can find this directive on the VA Publications site. A link to the site is provided in Resources.

Failure to follow best practices for safe internet browsing and social media usage can negatively impact the security of VA systems, endpoints, and electronic information. If you have concerns about a website or your data protection software, contact your local ISSO. Causes for concern might include malware pop-ups, antivirus warnings, or unusual activity on your devices or accounts. Report any suspected or actual cybersecurity incidents immediately to your ISSO, PO, and supervisor.

5.12 Limited Personal Use (VA Directive 6001)

It is expected that there will be some personal use of GFE, whether on phones or laptops. VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*, allows VA employees to use government-issued equipment for personal or non-government purposes under the following conditions:

- It involves minimal additional expense to the government.
- It is performed on the employee's non-work time.
- It does not interfere with VA's mission or operations.
- It does not violate standards of ethical conduct for executive branch employees.

Review VA Directive 6001 for more information on limited personal use, employee non-work time, and unauthorized activities. You can find this directive on the VA Publication site. A link to the site is provided in Resources.

5.13 Summary

Just as you must protect VA sensitive information in physical form, you must also protect VA sensitive information in electronic form, making sure that your practices are up to code. Implement the following best practices to protect the information you handle every day:

- Encrypt emails and attachments containing VA sensitive information.
- Use properly permissioned Microsoft SharePoint and Teams sites and network shared drives to store only the minimum necessary VA sensitive information.
- Be aware of and follow safe web browsing practices to avoid cyberattacks and malware infection.
- Be careful what you post on social media to avoid exposing VA sensitive information.

Reach out to your supervisor, ISSO, or PO if you have questions or need to report an issue or incident.

Topic 6: Working Remotely

6.1 Introduction and Objectives

Now more than ever, many VA employees do not work on-site, but instead work remotely, away from their associated facility. Remote work has its own set of challenges in protecting VA information, systems, and equipment. It's important that you know how to securely access VA information and systems when working remotely. This helps ensure a stable foundation of privacy and security across different environments.

When you have completed this topic, you will be able to do the following:

- Identify proper procedures for securely accessing VA information and systems remotely
- Describe best practices for protecting VA information and systems remotely.

In this topic, you will find situations and information concerning working remotely and best practices for protecting VA systems and information while using them remotely.

6.2 Connecting Remotely to the VA Network With GFE and Non-GFE

Before you can connect remotely to the VA network, you will need to work with your supervisor to meet the requirements. Once approved, you must complete the following required documentation and coursework for telework:

- VA Form 0740, *Telework Agreement*
- Telework Notification Letter – Employee Eligible to Telework
- *Telework Training Module for Employees* (VA TMS ID: 1367006).

There are three primary access methods used to connect remotely to VA systems:

- **AVD** is a cloud Desktop-as-a-Service (DaaS) that VA staff can use to remotely access network resources without the need to first access CAG. It's designed for use from any supported Microsoft operating system, including VA-issued or privately owned Windows 10 or Windows 11 computers. It's a good option for authorized users who need remote access to a standardized VA desktop when not connected to the VA network, either physically or via Virtual Private Network (VPN). Two-factor authentication (e.g., PIV card, CAC, or eToken) is required. Note that there is a project underway to move all Windows device remote users from CAG to the AVD solution. Users will receive direct communications as they are migrated to the new resources and old resources are removed. A link to instructions for downloading the AVD client is included in Resources.

- **CAG** is a remote access solution for Personally Owned Equipment (POE) users without GFE. CAG provides access to a virtual desktop and basic applications like email and MS Teams, as well as common applications used by VA end users. CAG requires the installation of Citrix software, called Receiver, on the end user's device. This allows secure access to internal VA resources for users without GFE. Before accessing CAG, users must request and be approved to access the network remotely. Note that there is a project underway to move all Windows device remote users from CAG to the AVD solution. Users will receive direct communications as they are migrated to the new resources and old resources are removed.
- **RESCUE** is a VPN remote access solution designed for VA-issued and -managed Windows and Macintosh endpoints. RESCUE is the recommended VPN solution for VA GFE devices. It provides security posture checks and ensures VA data is encrypted from the end device to the VA trusted network. RESCUE software is installed on all VA GFE laptops prior to being provided to the user. Before accessing RESCUE, users must request and be approved to access the network remotely.

These tools require two-factor authentication through use of a PIV card, Common Access Card (CAC), or eToken. From there, you can securely connect to the VA network. You must protect your log-in credentials and the process for remote access to VA networks and systems. This applies whether you are in the office, at another remote work location, or at home.

Keep in mind that the VA network is not limited to GFE. Non-GFE can also access network resources with permission. For example, VA employees may use their personally owned computer, or a VA contractor may use their corporate-issued laptop. However, personally owned mobile devices may not be used. Only VA GFE mobile devices (e.g., smartphones, tablets) may be connected to the VA network or used to store or transmit VA data.

If you need to access VA network resources with non-GFE, request access via the Remote Access Self Service Portal. A link to the portal is available in Resources. Contact your supervisor or COR with any questions.

6.3 Protecting VA Sensitive Information When Working Remotely

Working remotely comes with benefits, but it poses unique challenges to protecting VA sensitive information. Before starting a telework or remote schedule, meet with your supervisor. They will help you outline a secure plan of action for setting up your physical work location, transmitting and disposing of sensitive information, and handling records. This plan of action will ensure that you are aware of the requirements and privacy safeguards for working remotely. If you have been approved to print documents containing VA sensitive information while working remotely, you are required to shred them when they are no longer of use. GFE printers and shredders will be assigned as needed by your program office. For more information on remote printing and shredding, consult VA Handbook 5011/36, *Hours of Duty and Leave*.

Keep all GFE and VA information separate from personal items and information. It is a good idea to establish a dedicated work area to keep your personal information away from VA sensitive information. If authorized VA personnel wish to inspect the remote location, you should give them access before the telework agreement is set in place. If you need to store, transport, or use GFE or sensitive information outside a VA protected environment, then an additional approval step is required to obtain an Authority to Transport.

The requirements for GFE transport include a properly completed VA Form 0887, *VA Government Property Loan Form*. The requirements for transportation of VA documents include a completed VA Form 0740, *Telework Request/Agreement*, and a letter of approval from your supervisor. Per VA Directive 7002, you must complete a request to take VA information offsite and obtain approvals from the appropriate administration-specific Directors of the local VA facility in which they are housed.

Safeguard all VA sensitive information regardless of the format or location. Be especially mindful of how you handle VA sensitive information when working remotely. Do not give anyone access to your VA-issued equipment or credentials. This applies to mobile devices as well as other forms of GFE. Do not use your personal or VA-issued mobile devices to attach VA sensitive information to unencrypted emails, share files with those who lack a need-to-know, or take unsecured screenshots of SPI. These actions put VA sensitive information at risk.

Whether you are in the office or working remotely, convenience is never a reason to violate privacy and security policy. If anything happens inadvertently, report the incident immediately to your supervisor, ISSO, and PO.

6.4 Scenario: Disposing of VA Sensitive Information When Working Remotely

Scenario

You're a former full-time teleworker who has recently shifted to a hybrid schedule. While cleaning out your home workspace, you find a box of documents containing VA sensitive information. You no longer have approval to remotely store these papers. How should you dispose of them?

Determine the best answer from the options provided.

A. Throw the papers away. The information is mostly outdated anyway, so security shouldn't be an issue.

B. Return the documents to your official VA office and consult your Records Management Officer for guidance on proper storage or disposal, per an approved RCS.

Feedback

The correct answer is B.

The improper printing, storage, and destruction of papers or documents puts VA sensitive information at risk of being accessed by those who do not have a need-to-know. This would result in a privacy incident or security breach.

Remotely printed or stored documents containing VA sensitive information must be shredded when no longer in use, in accordance with VA and local facility policy.

If you are an authorized full-time teleworker who has been approved for remote printing and storage as part of your assigned job duties, use the GFE shredder assigned to you by your program office.

If you're not a full-time teleworker, you must securely transport documents requiring destruction to your official VA office for proper storage or disposal, in accordance with an approved VA RCS or general RCS. Your Records Management Officer can provide additional guidance and information.

You should never transport or store VA sensitive information offsite unless the appropriate permissions are in place, per your Telework Agreement. If you need to store, transport, or use GFE or sensitive information outside a VA protected environment, then an additional approval step is required to obtain an Authority to Transport. Per VA Directive 7002, you must complete a request to take VA information offsite and seek approval from the Director of the local VA facility.

If you are leaving VA or no longer need to store VA information remotely for official duties, make sure to turn all documents back in to the appropriate authorities.

If you are temporarily unable to follow the policies in VA Directive 6371, *Destruction of Temporary Paper Records*, and VA Handbook 5011/36, *Hours of Duty and Leave*, contact your PO, ISSO, Records Officer, and supervisor for further guidance.

To protect sensitive information while working remotely, you should also make sure to safeguard your VA-issued devices or access, per the ROB.

Rules of Behavior

Organizational Users

I WILL safeguard electronic and physical VA sensitive information while working at home or during travel. (SOURCE: SC-28)

I WILL keep Government-furnished equipment (GFE) and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

Non-Organizational Users

I WILL safeguard electronic and physical VA sensitive information while working at home or during travel. (SOURCE: SC-28)

I WILL keep GFE and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)

I WILL protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

6.5 Scenario: Emailing VA Sensitive Information for Remote Use

Scenario

Your GFE laptop is acting up and you need to take it in for overnight repairs. In the meantime, however, you still have lots to do. Would it be ok to forward some VA sensitive documents to your personal email so you can continue working on them from a home device?

Determine the best answer from the options provided.

A. No. Do not send VA sensitive information to your personal email account. Use a VA-approved method to access the documents remotely.

B. Sure. You need the information for authorized purposes and can't afford to get behind. Go ahead and send the documents to your personal account.

Feedback

The correct answer is A.

Emailing VA sensitive information to a personal account violates privacy and security policy. Also, do not auto-forward email messages to addresses outside the VA network. This raises the risk of someone accessing VA sensitive information without a need-to-know, as well as placing sensitive information outside the VA-protected boundary.

It's also strongly advised that you avoid forwarding VA business calls to a personal phone without permission. Forwarding business calls to a personal phone could disclose VA sensitive information and result in a privacy incident.

To access or share sensitive information while working remotely, you should use only approved methods and channels, such as encrypted internal emails sent over the RESCUE GFE VPN. Note that the same security considerations apply whether you are communicating internally or externally.

Never allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance. Contact your local ISSO or PO for assistance. If you need to remotely access or transmit VA sensitive information from personally owned equipment, connect through CAG or AVD, and use encrypted VA email or other approved means for any transmission purposes. For more information on how to connect remotely using RESCUE, CAG, or AVD, visit the Remote Access Information and Media Portal. Links and access instructions are provided in Resources.

Rules of Behavior

Organizational Users

I WILL keep Government-furnished equipment (GFE) and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)

I WILL safeguard electronic and physical VA sensitive information while working at home or during travel. (SOURCE: SC-28)

I WILL NOT allow VA sensitive information to reside on non-VA systems or devices unless designated and authorized in advance by all appropriate individuals, including my VA supervisor and Information System Owner. (SOURCE: SC-28)

I WILL NOT auto-forward email messages or forward phone calls outside the VA network. (SOURCE: AC-4)

Non-Organizational Users

I WILL keep GFE and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)

I WILL safeguard electronic and physical VA sensitive information while working at home or during travel. (SOURCE: SC-28)

6.6 Collaborating in a Virtual Environment

VA is relying more and more heavily on telework to maintain business operations. Employees and contractors should be aware of information security and privacy best practices for collaborating in a virtual environment, whether for telehealth appointments with Veterans or internal meetings.

There are several VA-supported teleconferencing tools and solutions, including Microsoft Teams, VA Video Connect, and Webex. We use these tools to provide safe, effective, and physically distanced services to Veterans.

- For more information on Microsoft Teams, visit the Resource Center for Office and other Microsoft 365 products.
- For more information on VA Video Connect, visit the Office of Connected Care site.
- For more information on Webex resources, visit the Connectivity and Collaboration Services site.

Links to these VA intranet sites can be found in Resources.

Note that VA has implemented a Transparent Screen Lock (TSL) solution that allows employees to log on to a computer at a VA facility, open an application, and lock the screen so only that application is visible. TSL can be used to conduct secure video conference calls and telehealth appointments without compromising VA sensitive information. For more information on TSL, visit the OIT Desktop and Device Engineering (DDE) SharePoint. A link to this site can be found in Resources.

When conducting or participating in video conference calls and web meetings, you should do your best to reduce unintended information sharing and protect sensitive VA data. Below are some tips to help keep your virtual meetings as private as possible:

- Conduct web meetings only on VA-issued or -approved devices.

- Clear your work area and desktop of any paper or digital documents containing VA sensitive information before starting a screenshare or turning on your video.
- Find a quiet, secure space to hold meetings, away from family members or others who might be physically present when sensitive information is being discussed.
- Set up chat, screen-sharing, and file-sharing privileges before the meeting.
- Limit reuse of meeting access codes.
- Make sure that your video and microphone are turned off when you aren't using them for web conferencing purposes.
- Avoid recording sensitive virtual meetings or Veteran appointments unless authorized to do so. If a recording is needed, make sure to encrypt the audio and secure it with a passphrase.
- Use a dashboard to monitor meeting attendees and ensure that only authorized parties are present.

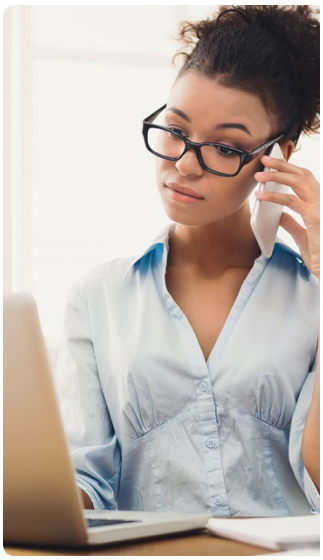
6.7 Summary

Protecting VA systems, equipment, and information while working remotely can be challenging. However, you should take the time to properly and securely set up your workspace and access the VA network. Doing so helps minimize risks of security incidents, data breaches, and privacy incidents. Be sure to follow these foundational best practices:

- Gain appropriate permission and follow procedures to securely gain remote access to the VA network using GFE and non-GFE equipment.
- Work with your supervisor or COR to establish a secure plan of action to protect VA data and sensitive information when working remotely.
- Do not share your VA-issued equipment with anyone.
- Apply best practices and safeguards for collaborating in a virtual environment.

Topic 7: Reporting Incidents

7.1 Introduction and Objectives



If you see something suspicious or what appears to be an incident, you must report it, upholding the principles that create a strong foundation at VA. Incident reporting helps lower the risks of violations and incidents. Make sure you know whom to contact if you suspect there is an incident.

When you have completed this topic, you will be able to do the following:

- Identify privacy and information security incidents
- Recall how to report suspected privacy and information security incidents.

In this topic, you will learn how to recognize and report a potential incident. Along the way, you will have the opportunity to review situations that are, or could lead to, an incident.

7.2 Recognizing a Potential Incident

An incident is an event that threatens to compromise the confidentiality, integrity, and availability of information and the system in which it resides. Incidents come in many different forms, including privacy incidents and data breaches. A privacy incident refers to any unauthorized disclosure of or access to personal information. A data breach is a type of privacy incident involving the release of sensitive data, including VA sensitive information. A data breach could include the theft of sensitive information of thousands of VA employees due to a cyberattack or the disclosure of sensitive information of a single Veteran due to a mismailing incident.

These types of events can threaten information security and privacy. They may also affect Veterans, VA, and you as an employee or associated individual.

You are required to report suspected or actual information security and privacy incidents immediately. Get in touch with your local ISSO or PO and tell them exactly what you saw. In this case, “better safe than sorry” means reporting, even if it turns out not to be an incident.

Examples of suspected incidents that should be reported include the following:

- Finding a folder that contains VA sensitive papers on a copier
- Finding loose mailing labels on the ground that are addressed to patients
- Getting a call from a Veteran stating that they received a Consolidated Mail Outpatient Pharmacy package that should have been sent to someone else
- Seeing someone you do not recognize accessing a VA system
- Receiving an unencrypted email with VA sensitive information from a coworker

- Finding a coworker's PIV card
- Receiving malware alerts after clicking a suspicious link in an external email.

Report any suspected incident, no matter how trivial it seems. Reporting immediately could prevent a small issue from being a big issue later.

7.3 Reporting Incidents

If you notice something out of the ordinary that makes you think an incident has happened or could happen, report it right away to the proper authorities.

The first step is to note the details:

- What happened?
- Where did it happen?
- When did it happen?
- Who was involved?
- Why do you think it might be a violation?

The second step is to report it to the proper authorities:

- You should report suspected or identified incidents to your supervisor, ISSO, and PO immediately. Refer to the PO/ISSO locator website if you don't know the name of your local ISSO or PO.
- If it is after hours and you are unable to contact your supervisor, ISSO, and PO, you may report security incidents to the ESD. If the incident involves privacy, you'll be instructed to contact your PO or AOD as soon as able, based on administration-specific guidelines.
- Contractors should report every incident to their ISSO, PO, and the COR and Project Manager.

All suspected or identified incidents must be reported immediately.

Once an incident is reported, a ticket must be created in the tracking system within one hour. When you are reporting an incident, make sure that the information you provide is accurate and specific. This helps avoid any errors or misunderstandings.

If any additional technology issues occur during the reporting process, reach out to the ESD for immediate assistance.

7.4 Consequences for Causing an Incident

There are different responses for intentional versus unintentional incidents. The consequences are more severe for intentional incidents than for accidental or unintentional incidents.

Consequences for causing incidents can include:

- Suspension of system access

- A reprimand in your personnel file
- Suspension from your job, demotion, or job loss
- Prosecution in civil or criminal courts
- Fines
- Imprisonment.

If you steal, change, or destroy federal property or information, you could face many penalties under various laws, such as:

- Fines of up to $10,000
- Prison for up to 10 years.

There are other types of violations that may also result in penalties. Select each type to learn more:

- **Mishandling records**: Anyone who willfully and unlawfully conceals, removes, mutilates, obliterates, falsifies, or destroys federal records may be fined up to $2,000, imprisoned for up to 3 years, or both. (Source: 18 U.S. Code § 2071)
- **Stealing records**: Anyone who embezzles, steals, sells, conveys, or disposes of federal records without authority may be fined up to $10,000, imprisoned for up to 10 years, or both. (Source: 18 U.S. Code § 641)
- **Violating the Privacy Act**: Anyone who willfully violates the requirements of the Privacy Act will be guilty of a misdismeanor and may be fined up to $5,000. (Source: 5 U.S. Code § 552a)
- **Violating HIPAA**: Those who violate HIPAA regulations may face fines from $100 to $1.5 million and up to 10 years of imprisonment, depending on the type of violation. (Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html)

Additional or more severe penalties may apply for violating laws that safeguard Protected Health Information (PHI).

7.5 Insider Threat and Social Engineering Awareness

Insider threats are a real concern. Everyone at VA should be on the alert for odd behaviors that might indicate a growing insider threat such as:

- Undue and long-term job dissatisfaction
- Attempts to discuss or gain access to information not needed for job role
- Unreported overseas travel or contact with foreign nationals
- Strange or inconsistent working hours
- Unexplained access to financial resources
- Workplace violence, such as bullying or sexually harassing fellow employees

- Repeated violations of security policies, procedures, rules, directives, or practices.

For more information about insider threats, visit the Veterans Affairs Insider Threat Program Awareness and Reporting Tool page. A link to this page is provided in Resources.

You should also be aware of social engineering tactics that attackers may use to gain access to VA systems or information. Common examples include impersonating a legitimate entity (as in phishing emails), diverting attention away from illicit activity, or tailgating authorized parties into a secure physical area.

Always be on the lookout for insider threats and social engineering. Report any suspicious behaviors that you encounter before they turn into serious incidents.

7.6 Scenario: Recognizing Insider Threats and Social Engineering

Scenario

You're working hard to meet a deadline on an important project. One of your coworkers offers to assist; he'll just need you to share your credentials with him so he can access the necessary systems. This sounds suspicious, but you really need the help. What should you do?

Determine the best answer from the options provided.

A. Don't share your access credentials. If your coworker continues making suspicious requests, alert your supervisor, ISSO, or PO to a potential insider threat.

B. Go ahead and provide your access credentials. You'll keep a close eye on him.

Feedback

The correct answer is A.

You should always be mindful of social engineering techniques, watching out for suspicious behaviors from colleagues. Never share your personal username, password, verification codes, or other credentials with anyone. Also, do not provide access to secured records, network drives, or Microsoft SharePoint and Teams sites until you've confirmed that the requester has a valid need-to-know and the correct level of permissions to access the information system. Sharing VA sensitive information with unauthorized volunteers, contractors, Veterans, or staff members is a violation of the ROB.

There are many behaviors that may be warnings of an insider threat, including the following: undue job dissatisfaction, attempts to gain access to information not needed for job role, unreported travel, inconsistent working hours, unexplained wealth, workplace violence, and repeated rule violations.

If you notice anything out of the ordinary, report it to the proper authorities, such as your supervisor, PO, or local ISSO. If you don't know your local ISSO or PO, visit Resources for the link to the PO/ISSO locator. The purpose of reporting is not to get people in trouble. The purpose is to let the authorities know so they can investigate and provide help as needed.

Rules of Behavior

Organizational Users

I WILL understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)

I WILL protect VA sensitive information from unauthorized disclosure, use, modification or destruction and use encryption products approved and provided by VA to protect sensitive data. (SOURCE: AC-19)

I WILL NOT divulge a personal username, password, access code, verification code or other access credentials to anyone. (SOURCE: IA-5)

I WILL report suspected or identified information security incidents, including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

I WILL only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties. (SOURCE: AC-21)

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

I WILL NOT make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

Non-Organizational Users

I WILL understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)

I WILL report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant alert messages (security and privacy) on VA information systems to the enterprise service desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

I WILL NOT disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

I WILL NOT divulge a personal username, password, access code, verification code or other access credentials to anyone. (SOURCE: IA-5)

7.7 Recognizing and Reporting Phishing Attempts

Phishing is a type of scam that uses deceptive email messages to dupe users into revealing personal information or opening malicious links or files. Be on the lookout for warning signs, such as suspicious sender name or email address, non-VA hyperlinks, poor grammar, mistakes in provided information, unusual requests, or offers that seem too good to be true. Note that phishing emails may be developed to look as if they came from inside the VA environment or from another legitimate source. Be extremely vigilant against this growing threat, and make sure to report any suspicious emails to the VA Cybersecurity Operations Center (CSOC) by following these steps.

1) Select the email, but don't open it.
2) Then select the **Report Phishing** button located on the Microsoft Outlook ribbon.
3) Finally, select OK in the pop-up to confirm you want to report the email.

If you can't find the **Report Phishing** button in MS Outlook, visit the Threat Assessment and Analysis Portal Phishing Awareness page for instructions on how to enable or add this functionality. A link to this site can be found in Resources. You can also contact the ESD for assistance.

Note that external emails will not always be flagged, so make sure to double-check the sender's address before taking any action. Also make sure the sender has a valid need-to-know for any requested information, especially if it's personal information like your date of birth, Social Security information, or address. If there is any question about the legitimacy of the request, reach out to an authorized staff member from the appropriate group or team for confirmation.

If you accidentally select a link, open an attachment, or reply to a suspected phishing attempt, immediately report the incident to your local ISSO, PO, and supervisor. They will work with the IT specialist to resolve and monitor the incident in the Privacy and Security Event Tracking System (PSETS). Any antivirus pop-ups or possible malware alerts should also be reported to these parties as soon as you are able. If they aren't available, contact the ESD for immediate action.

Even if there aren't signs of malware, you should still inform your local ISSO and supervisor of any suspicious communications you receive. Remember not to forward or delete phishing attempts. They will be automatically removed from your inbox after selecting the Report Phishing button.

In addition to phishing, you need to be aware of other growing threats such as whaling, spoofing, vishing, and smishing. Smishers may send text messages to your work or personal phone in an attempt to gain access to VA systems or information. If you receive a smishing attempt, report the issue through the yourIT Service Portal. A link to this site can be found in Resources. Your Local Mobility IT Administrator will then work with the Telecom Team to document and resolve the incident.

7.8 Scenario: Recognizing and Reporting Phishing Attempts

Scenario

You receive an email from an unknown address with the subject line: "[External] Your Records Have Been Compromised!" The email includes an urgent message about a recent data breach and urges you to click a link for further instructions. What should you do?

Determine the best answer from the options provided.

A. Don't click the link. The email seems suspect and should be reported using the "Report Phishing" button in Outlook.

B. Click the link. The issue sounds urgent, and you want to learn more.

Feedback

The correct answer is A.

The email may not be legitimate and should be reported as a phishing attempt.

Follow these steps to report a suspicious email to the VA CSOC:

1) Select the email, but don't open it.
2) Then select the **Report Phishing** button located on the Microsoft Outlook ribbon.
3) Finally, select **OK** in the pop-up to confirm you want to report the email.

After reporting the event, the message will be removed from your inbox. You will get a pop-up message confirming that your report was sent to the VA CSOC for analysis. CSOC will then alert the ISSO if there are any security or malware concerns.

When you receive a suspicious communication, pay close attention to details. Be on the lookout for warning signs, such as non-VA hyperlinks, poor grammar, mistakes in provided information, or unusual requests from external addresses or unfamiliar numbers.

Be aware that phishers will often pressure you to take actions like verifying your account, claiming money, or confirming information. They may also use urgent news updates, current world events, and latest trends in the economy to grab your attention.

You should never forward or delete suspicious emails or communications. Also, do not select or open any potentially malicious links or attachments. Doing so may download malware or viruses onto your device, allowing bad actors to harm the VA network. This creates work for the security team and puts VA sensitive information at risk.

Rules of Behavior

Organizational Users

I WILL report suspected or identified information security incidents, including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

I WILL protect VA sensitive information from unauthorized disclosure, use, modification or destruction and use encryption products approved and provided by VA to protect sensitive data. (SOURCE: AC-19)

I WILL NOT make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

Non-Organizational Users

I WILL report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant alert messages (security and privacy) on VA information systems to the enterprise service desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

7.9 Summary

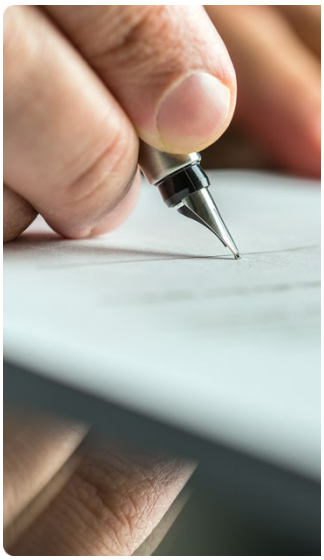
Everyone is responsible for reporting suspicious activities or possible incidents. Be mindful of your surroundings on the job and use your best judgment to identify anything that might threaten the safety and integrity of VA's infrastructure. Follow these best practices for incident reporting:

- Be aware of odd activities in your work area.
- Note the details of the suspicious activity.
- Report the suspicious activity to your supervisor, ISSO, and PO.
- Report any insider threat or social engineering behaviors to your supervisor, ISSO, and PO.
- Report phishing attempts or suspicious communications to VA CSOC.

The purpose of reporting is not to get yourself or colleagues in trouble. Instead, it is to help prevent problems from becoming uncontrollable. By reporting suspected incidents right away, you may be able to prevent a large-scale problem.

Topic 8: Course Summary and ROB

8.1 Course Summary



Everyone at VA has the potential to encounter VA sensitive information. We are all responsible for being diligent about protecting privacy and information security. Knowing the basics, being aware, and following the best practices will help us build a foundation of protection and support for Veterans, VA, and your colleagues.

The ROBs are the minimum compliance standard for all VA personnel in all locations. If you have access to specialized systems or information, you may be required to sign and comply with additional ROBs dealing specifically with those systems or information. This topic will present you with the ROBs required for all VA personnel.

8.2 Acknowledge and Accept ROBs

To complete this training, you must review, initial each page of, and sign and date the appropriate ROB for your user type to acknowledge and accept the ROB. Many, but not all, of the ROB have been explained in this course. By acknowledging and accepting the ROB, you are agreeing to uphold all the behaviors stated in the rules.

Remember there are two versions of the ROB, one for Organizational Users and one for Non-Organizational Users. The following provides the descriptions for each:

- **Organizational Users** are VA employees, contractors, researchers, students, volunteers, and representatives of federal, state, local, or tribal agencies who are authorized to access VA information but do not represent a Veteran or claimant.
- **Non-Organizational Users** are users other than those explicitly categorized as Organizational Users. These include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for onboarding power of attorney/private attorneys.

Once you have initialed the appropriate pages for your user type and signed the ROB document, you must submit the document to your supervisor or COR for documentation of course completion.

8.3 Completion

Contact your supervisor or COR to submit the signed ROB and to coordinate with your local TMS Administrator to ensure you receive credit for completion.

Appendix A: Organizational Rules of Behavior

DEPARTMENT OF VETERANS AFFAIRS (VA) INFORMATION SECURITY RULES OF BEHAVIOR (ROB) FOR ORGANIZATIONAL USERS FISCAL YEAR (FY) 2024

1. COVERAGE

A. This *Department of Veterans Affairs (VA)) Information Security Rules of Behavior (ROB) for Organizational Users* document identifies the specific responsibilities and expected behavior for organizational users of VA information and information systems as required by 38 U.S.C. § 5723(f)(5), Office of Management and Budget Circular A-130, Appendix I, paragraph 4h (6-7), VA Directive 6500, *VA Cybersecurity Program* and VA Handbook 6500, *Risk Management Framework for VA Information Systems – VA Information Security Program*.

B. *Organizational users* are VA employees, contractors, researchers, students, volunteers and representatives of Federal, state, local or tribal agencies authorized to access VA information and information systems for the performance of official duties, but do not represent a Veteran or claimant.

C. *Non-organizational users* are users other than those explicitly categorized as organizational users. The ROB for non-organizational users are identified in VA's *Information Security ROB for Non-Organizational Users* document. These include affiliates and individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for onboarding power of attorney/private attorneys.

D. The ROB provides the minimum requirements that organizational users of VA information and information systems must comply with and does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA's information or information systems. Organizational users may exceed these minimum requirements to protect VA information and information systems when appropriate by exercising due diligence and ethical standards.

2. COMPLIANCE

A. Organizational users are required to comply with the ROB. Non-compliance with the ROB may be cause for disciplinary or adverse actions. Depending on the severity of the violation and management discretion, consequences may include restricting access to VA information or information systems, suspension of access privileges, admonishment, reprimand, demotion, suspension and removal. Theft, conversion or unauthorized disclosure or disposal of Federal property or information may result in criminal sanctions.

_____
Initials

B. Unauthorized access, upload, download, change, circumvention, or deletion of information on VA systems; unauthorized modification of VA systems; denying or granting access to VA systems without authorization; unauthorized use of VA systems or VA information; or otherwise misusing VA systems or resources, is strictly prohibited.

C. The ROB does not create any other right or benefit (substantive or procedural) enforceable by law by a party in litigation with the Government.

3. ACKNOWLEDGEMENT

A. Organizational users must sign the *ROB for Organizational Users* before access is provided to VA information and information systems. This *ROB for Organizational Users* must be signed annually by all VA information and information systems users. This signature acknowledges agreement to comply with the ROB and refusal to sign this ROB will result in denied access to VA information and information systems. Any refusal to sign the *ROB for Organizational Users* may result in the disciplinary or adverse action.

B. The *ROB for Organizational Users* may be signed in hard copy or electronically. If signed using the hard copy method, the user should initial and date each page and provide the information requested under the Acknowledgement and Acceptance section found at the end of this document. For other Federal, state, local and tribal agency users, documentation of a signed VA Information Security ROB will be provided to the VA requesting official.

C. If an individual is both an organizational and a non-organizational user, the individual shall sign both ROBs..

4. INFORMATION SECURITY ROB

Access and Use of VA Information and Information Systems

I Will:

- Comply with all Federal statutes, regulations and policies applicable to VA information security, information privacy/disclosure and records management. (SOURCE: PM-10)
- Use only VA-approved devices, systems, software, services and data that I am authorized to use, including complying with any software licensing or copyright restrictions. (SOURCE: AC-20)
- Follow established procedures for requesting access to any VA computer system and notifying my VA supervisor or designee when the access is no longer needed. (SOURCE: AC-2)
- Only use my access to VA information and information systems for officially authorized and assigned duties. The use of VA information and information systems must not violate any VA policy regarding jurisdiction, restrictions, limitations, or areas of responsibility. (SOURCE: AC-6)

_____
Initials

- Log out of all information systems at the end of each workday. (SOURCE: AC-11)
- Log off or lock any VA computer or console before leaving my workstation, whether at a VA location or alternate worksite. (SOURCE: AC-11)
- Only use other Federal Government information systems as expressly authorized by the terms of those systems; personal use is limited by VA standards. (SOURCE: AC-20)
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. (SOURCE: AC- 17)

I Will Not:

- Have any expectation of privacy in any information I access, create, receive or maintain, or in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. (SOURCE: AC-10)
- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA systems or information. (SOURCE: AC-4)
- Engage in any activity prohibited by VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*. (SOURCE: AC-6)
- Connect information systems to the VA network or engage in sending VA sensitive data outside the VA network without ensuring the system has an authority to operate decision provided by a VA Authorizing Official. (SOURCE: CA-2)
- Have a VA network connection and a non-VA network connection, such as a modem or phone line or wireless network card, physically connected to any device at the same time unless the dual connection is explicitly authorized by my Information System Owner and local Area Manager (AM) or designee. (SOURCE: AC-17)
- Host, set up, administer, or operate any internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner and AM or designee. (SOURCE: AC-17)

Protection of VA-Issued Devices

I Will:

- Secure mobile devices (e.g., laptops, tablets, smartphones) and portable storage devices (e.g., compact discs, digital video discs, universal serial bus flash drives). (SOURCE: PE-4)

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized Office of Information and Technology (OIT) employee. (SOURCE: AC-19)

_____
Initials

- Attempt to override, circumvent, alter or disable security configuration controls unless expressly directed to do so by authorized VA staff. (SOURCE: AC-6)

Data Protection

I Will:

- Only use virus protection software, anti-spyware and firewall/intrusion detection software authorized by VA. (SOURCE: SI-2)
- Safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely. (SOURCE: SC-28)
- Only use VA-owned or approved storage devices encrypted with Federal Information Processing Standards (FIPS) 140-2 (or its successor) validated encryption, consistent with VA's approved configuration and security control requirements to perform VA work. (SOURCE: AC-19)
- Use VA email in the performance of my duties when issued a VA email account. (SOURCE: AC-4)
- Only disseminate VA information to the public when authorized to do so and in the performance of my duties. (SOURCE: PM-10)

I Will Not:

- Transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption and properly authorized to release the data. (SOURCE: AC-18)
- Auto-forward email messages or forward phone calls outside the VA network. (SOURCE: AC-4)
- Download software from the internet, or other publicly available sources, offered as free trials, shareware or other unlicensed software to a VA-owned system. (SOURCE: CM-6)
- Disable or degrade software programs used by VA that install security software updates on computer equipment used to connect to VA information systems or used to create, store or use VA information. (SOURCE: CM-2)

Teleworking and Remote Access

I Will:

- Keep Government-furnished equipment (GFE) and VA information safe, secure and separated from my personal property and information, regardless of work location. (SOURCE: PE-4)
- Protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)

_____
Initials

- Obtain approval prior to using remote access capabilities to connect non-GFE devices to VA's network. (SOURCE: AC-17)
- Secure all appropriate approvals prior to any international telework with a VA mobile device so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international telework and/or inspecting the device or reimaging the hard drive upon return. (SOURCE: AC-17)
- Comply with any security measures, including using a specifically configured device issued for international travel and surrendering the device for inspection or reimaging. (SOURCE: AC-17)
- Safeguard electronic and physical VA sensitive information while working at home or during travel. (SOURCE: SC-28)
- Provide VA authorized personnel access to inspect the remote location as allowed and included in an approved VA telework agreement. (SOURCE: AC-17)
- Protect information about remote access mechanisms from unauthorized use and disclosure. (SOURCE: AC-17)
- Exercise a higher level of awareness in protecting GFE mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened. (SOURCE: SC-28)

I Will Not:

- Access non-public VA information technology (IT) resources from publicly available IT computers, such as remotely connecting to the internal VA network from computers in a public library. (SOURCE: AC-17)
- Access VA's internal network from any foreign country unless all appropriate approvals have been obtained in writing. (SOURCE: AC-17)

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames and complete any additional role-based security training required for my roles and responsibilities. (SOURCE: AT-3)
- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)
- Have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand. (SOURCE: PL-4)

_____
Initials

- Permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software. (SOURCE: AC-6)
- Sign VA Information Security ROBs required for access or use of specific VA systems. (SOURCE: AC-8)
- Comply with any requirement to sign a non-VA entity's ROB to conduct VA business. (SOURCE: PM-10).

Sensitive Information

I Will:

- Ensure responsible practices whenever Veteran data is accessed or used in accordance with VA policy and guidance. (SOURCE: AC-21)
- Ensure that all printed material containing VA sensitive information is physically secured when not in use (e.g., locked cabinet, locked door). (SOURCE: SC-28)
- Only provide access to VA sensitive information to those whom I verify have a need-to-know of this information for their official duties. (SOURCE: AC-21)
- Only post sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place. (SOURCE: AC-21)
- Recognize that access to certain databases has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. (SOURCE: SC-28)
- Act accordingly to ensure the confidentiality and security of sensitive records in a database is commensurate with the increased potential risk. (SOURCE: AC-21)
- Obtain approval from my supervisor to use, process, transport, transmit, download, print or store VA sensitive information remotely (outside of VA-owned or managed facilities (e.g., medical centers, Community-Based Outpatient Clinics, or Regional Offices)). (SOURCE: IP-1)
- Protect VA sensitive information from unauthorized disclosure, use, modification or destruction and use encryption products approved and provided by VA to protect sensitive data. (SOURCE: AC-19)
- Transmit VA sensitive information via fax only when no other reasonable means exist and when either someone is at the receiving machine to receive the transmission or the receiving machine is in a secure location. (SOURCE: AC-19)
- Encrypt email, including attachments, that contain VA sensitive information. I will not encrypt email that does not include VA sensitive information, or any email excluded from the encryption requirement. (SOURCE: AC-19)

_____
Initials

- Protect VA sensitive information aggregated in lists, databases or logbooks and include only the minimum necessary VA sensitive information to perform a legitimate business function. (SOURCE: AC-21)
- Ensure fax transmissions are sent to the appropriate destination. This includes double checking the fax number, confirming delivery and using a fax cover sheet with the required notification message. (SOURCE: AC-21)

I Will Not:

- Disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)
- Allow VA sensitive information to reside on non-VA systems or devices unless designated and authorized in advance by all appropriate individuals, including my VA supervisor and Information System Owner. (SOURCE: SC-28)
- Make unauthorized disclosure of VA sensitive information through any means of communication, including but not limited to, verbal communications, email, text messaging, instant messaging, online chat, social media, websites and collaboration tools/platforms. (SOURCE: AC-19)

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. (SOURCE: IA-5)
- Protect my passwords; verify codes, tokens and credentials from unauthorized use and disclosure. (SOURCE: IA-5)
- Maintain possession and display my VA credentials as required by VA policy. (SOURCE: IA-5)

I Will Not:

- Store my passwords or verify codes in any format on an IT system, unless it has been encrypted using FIPS 140-2 (or its successor) validated encryption and I am the only person who can decrypt the file. (SOURCE: IA-5)
- Hardcode credentials into scripts or programs on an IT system. (SOURCE: AC-3)
- Divulge a personal username, password, access code, verification code or other access credentials to anyone. (SOURCE: IA-5)

Incident Reporting

I Will:

_____
Initials

- Report suspected or identified information security incidents, including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor and the Enterprise Service Desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

Social Media & Networking to Conduct Official VA Business

I Will:

- Use the VA intranet to conduct VA business on social media/networking sites wherever possible. (SOURCE: SC-12)
- Use web-based collaboration and social media tools in accordance with VA Directive 6515, *Use of Web-Based Collaboration Technologies*. (SOURCE: PL-4)
- Limit the personal use of social media/networking sites, in accordance with VA Directive 6001, *Limited Personal use of Government Office Equipment Including Information Technology*. (SOURCE: AC-8)
- Obtain approval from the Office of Public and Intergovernmental Affairs before establishing a VA social media account. (SOURCE: AC-22)
- Ensure that my use of social media to conduct VA business complies with law, guidance, and VA policy. (SOURCE: AC-21)
- Use the VA intranet to conduct VA business on social media/networking sites wherever possible, while ensuring that my use of social media to conduct VA business complies with law, guidance, and VA policy. (SOURCE: SC-28)
- Use my best judgment when interacting on social media about matters related to VA's mission. (SOURCE: PL-4)
- In my capacity as a VA representative, post only information about which I have actual knowledge. (SOURCE: AC-21)
- Identify me and my roles as a VA representative when commenting or providing information on matters related to the VA's mission and ensure that my profile and any related content is consistent with how I wish to present myself to colleagues, Veterans, and the public. (SOURCE: AC-21)
- Only post and use content in accordance with applicable ethics, intellectual property, records and privacy laws, regulations, and policies. (SOURCE: AC-21)
- Use only instant messaging services approved by VA. (SOURCE: AC-21)

_____
Initials

- Publish a disclaimer that the views are my own and do not represent VA, if the content I publish on blogs, wikis or any other form of user-generated media might reasonably be perceived as the position of VA. (SOURCE: AC-22)

I Will Not:

- Comment on VA mission-related legal matters unless I am the VA official spokesperson for the matter and have management approval to do so. (SOURCE: AC-22)
- Comment or provide information on any matter I do not have actual, up-to-date knowledge in my capacity as a VA representative. (SOURCE: AC-22)
- Post VA information protected by the Privacy Act of 1974; 38 U.S.C. §§ 5701, 5705, or 7332; the Health Insurance Portability and Accountability Act (HIPAA) Rules; or against VA policy on any non-VA websites, without legal authority and prior approval by an authorized official. (SOURCE: AC-22)
- Use profanity, make libelous statements, make threats, or use privately created works without the express, written permission of the author. (SOURCE: AC-22)
- Quote more than short excerpts of another person's work unless the source is properly credited. (SOURCE: AC-22)

Identification Persona and Branding

I Will:

- Use display names and branding that are professional, appropriate for the context, and align with VA values and mission. (SOURCE: PL-4)
- Be aware that display names and branding may be visible to external audiences and act accordingly to represent VA positively. (SOURCE: PL-4)
- Follow VA policies and guidelines regarding online identification and branding that may require alignment with specific branding or naming conventions. (SOURCE: PL-4)
- Be reminded that VA reserves the right to take disciplinary action if display names or branding are found inappropriate, misleading, or damaging to its reputation. (SOURCE: PL-4)

I Will Not:

- Use graphical elements in place of names, such as logos, photographs, or custom illustrations that do not meet VA branding guidelines and that are not part of the va.gov design system. (SOURCE:AC-21)
- Use controversial or polarizing display names or branding that could negatively affect VA or create conflicts. (SOURCE: PL-4)

_____
Initials

- Use display names and branding that contains offensive language, can be perceived as discriminatory content or, misrepresents one's identity. (SOURCE: PL-4)
- Use display names and branding that contain personal or sensitive information. (SOURCE: AC-21)

5. ACKNOWLEDGEMENT AND ACCEPTANCE

A. I acknowledge that I have received a copy of *VA Information Security ROB for Organizational Users.*

B. I understand, accept and agree to comply with all terms and conditions of *VA Information Security ROB for Organizational Users.*

C. I will provide a supervisor or appropriate designee a signed copy of this document in a timely manner to ensure awareness and compliance.

D. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights or liabilities created by existing statute or Executive Order relating to (1) classified information; (2) communications to Congress; (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this agreement and controlled.

Print or type your full name	Signature	Date
_____	_____	_____

Office Phone _____ Position Title _____

Appendix B: Non-Organizational Rules of Behavior

DEPARTMENT OF VETERANS AFFAIRS (VA) INFORMATION SECURITY RULES OF BEHAVIOR (ROB) FOR NON-ORGANIZATIONAL USERS FISCAL YEAR (FY) 2024

1. COVERAGE

A. *VA Information Security Rules of Behavior for Non-Organizational Users* identifies the specific responsibilities and expected behavior for non-organizational users of VA information and information systems as required by 38 U.S.C. § 5723(f)(5), Office of Management and Budget Circular A-130, Appendix I, paragraph 4(h) (6-7), VA Directive 6500, VA Cybersecurity Program and VA Handbook 6500, *Risk Management Framework for VA Information Systems – VA Information Security Program.*

B. *Non-organizational users* are users other than users explicitly categorized as organizational users. These include affiliates and individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for on-boarding power of attorney/private attorneys.

C. *Organizational users* are VA employees, contractors, researchers, students, volunteers and representatives of Federal, state, local or tribal agencies authorized to access VA information and information systems for the performance of official duties, but do not represent a Veteran or claimant. The ROB for organizational users is identified in VA's Information Security Rules of Behavior for Organizational Users.

D. VA information is the information under the control of VA or stored on a VA information system. This includes both VA-sensitive and non-sensitive information. Information properly disclosed by VA to a non-organizational user (for example, contents of a Veteran's claims file for purposes of representing a Veteran or claimant) is no longer VA information and its security and confidentiality are the recipient's responsibility.

E. This ROB for Non-Organizational Users does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA's information or information systems. The ROB provides the minimum requirements with which individual users of VA information and information systems agree to comply and VA facilities and other agency components may issue requirements for protection that exceed this ROB.

_____
Initials

2. COMPLIANCE

A. Non-Organizational Users are required to comply with this ROB. Non-compliance with this ROB may result in suspension or removal of access to VA information or information systems. Although such a suspension would not prevent VA from making an authorized disclosure of records to a non-organizational user; a suspension of access may prevent disclosure through a particular method, for example, through a VA information system. Depending on the severity of the violation and management discretion, consequences may include access restriction or suspension of access privileges. Theft, conversion or unauthorized disclosure or disposal of Federal property or disclosure of information may result in criminal sanctions.

B. Unauthorized access, upload, download, change, transmission or deletion of information on VA systems without authorization; unauthorized modification of VA systems; denying or granting access to VA systems without authorization; unauthorized purpose on VA systems; or otherwise misusing VA systems or resources is strictly prohibited and may result in criminal sanctions.

C. This ROB does not create any other right or benefit (substantive or procedural) enforceable by law by a party in litigation with the Government.

3. ACKNOWLEDGEMENT

A. Non-Organizational Users must sign this ROB before access is provided to VA information and information systems. This ROB must be signed annually by all non-organizational users of the VA information or information systems. This signature indicates agreement to comply with this ROB and refusal to sign this ROB will result in denied access to VA information or information systems.

B. This ROB may be signed in hard copy or electronically. If signed using the hard copy method, the user must initial and date each page and provide the information requested under Acknowledgement and Acceptance.

C. If an individual is both an organizational and a non-organizational user, the individual shall sign both ROBs.

4. INFORMATION SECURITY RULES of BEHAVIOR

Access and Use of VA Information and Information Systems

I Will:

- Comply with all Federal statutes, regulations, and policies applicable to VA information security, information privacy/disclosure, and records management policies. (SOURCE: PM-10)

_____
Initials

- Follow established procedures for requesting access to VA information or an information system and notifying VA when the access is no longer needed. (SOURCE: AC-2)
- Only use VA-approved solutions, software, or services for connecting non-VA-owned systems to VA's network remotely or directly. (SOURCE: AC-17)
- Log off or lock any computer or console with access to or displaying VA information before I leave my workstation. (SOURCE: AC-11)
- Only use my access to VA information and information systems for officially authorized and assigned duties. The use of VA information and information systems must not violate any VA policy regarding jurisdiction, restrictions, limitations or areas of responsibility. (SOURCE: AC-6)

I Will Not:

- Have any expectation of privacy in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. (SOURCE: AC-10)
- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive information. (SOURCE: AC-4)
- Use personally owned equipment on-site at a VA facility to directly connect to the VA network or remotely to the VA network unless approved prior to use. (SOURCE: AC-20)
- Copy in any manner or use any technology (such as a mobile device) to copy or otherwise create unauthorized copies of VA information to which I do not have lawful access. (SOURCE: AC-3)
- Connect information systems to the VA network or engage in sending VA sensitive data outside the VA network without ensuring the system has an authority to operate decision provided by a VA Authorizing Official. (SOURCE: AC-3)

Protection of VA-Issued Devices

I Will:

- Protect Government-furnished equipment (GFE) from theft, loss, destruction, misuse, and threats. (SOURCE: PE-4)
- Follow VA policies and procedures for handling Federal Government IT equipment and sign for items provided to me and return them when no longer required for VA activities. (SOURCE PE-6)

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized Office of Information and Technology (OIT) employee. (SOURCE: AC-19)

_____
Initials

- Attempt to override, circumvent, alter, or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff. (SOURCE: AC-6)

Data Protection

I Will:

- If authorized to connect to a VA system, only use virus protection software, anti-spyware and firewall/intrusion detection software authorized by VA. (SOURCE: SI-2)

I Will Not:

- Download or install prohibited software from the internet or other publicly available sources, offered as free trials, shareware or other unlicensed software to a VA-owned system. (SOURCE: CM-6)
- Disable or degrade software programs used by VA that install security software updates on computer equipment and all electronic devices used to connect to VA information systems or used to create, store, or use VA information. (SOURCE: CM-2)
- Transmit VA sensitive information via wireless technologies unless the connection uses Federal Information Processing Standards (FIPS) 140-2 (or its successor) validated encryption and properly authorized to release the data. (SOURCE: AC-18)

Teleworking and Remote Access

I Will:

- Keep GFE and VA information safe, secure, and separated from my personal property and information, regardless of work location. (SOURCE: PS-2)
- Protect GFE from theft, loss, destruction, misuse and emerging threats. (SOURCE: PE-4)
- Obtain approval prior to using remote access capabilities to connect non-GFE devices to VA's network. (SOURCE: AC-17)
- Secure all appropriate approvals prior to any international telework with a VA mobile device so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international telework and/or inspecting the device or reimaging the hard drive upon return. (SOURCE: AC-17)
- Comply with security measures, including using a specifically configured device issued for international travel and surrendering the device for inspection or reimaging. (SOURCE: AC-17)
- Safeguard electronic and physical VA sensitive information while working at home or during travel. (SOURCE: SC-28)

_____
Initials

- Provide authorized VA personnel access to inspect the remote location when approved remote access to VA information and information systems includes access to VA sensitive information. (SOURCE: AC-17)
- Protect information about remote access mechanisms from unauthorized use and disclosure. (SOURCE: AC-17)
- Exercise a higher level of awareness in protecting VA mobile devices or other GFE when traveling internationally as laws and individual rights vary by country and threats against devices with agency information may be heightened. (SOURCE: SC-28)

I Will Not:

- Access non-public VA information systems from publicly available computers, such as remotely connecting to the internal VA network from computers in a public library. (SOURCE: AC-17)
- Access any internal VA information system from any foreign country unless all appropriate approvals have been obtained in writing. (SOURCE: AC-17)
- Access VA's internal network from any foreign country designated as a security risk unless all appropriate approvals have been obtained in writing. This prohibition does not affect access to VA external web applications. (SOURCE: AC-17)

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames. (SOURCE: AT-2)
- Complete any additional role-based security training required based on my roles and responsibilities. (SOURCE: AT-3)
- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action. (SOURCE: AC-10)
- If applicable, have my GFE scanned and serviced by VA authorized personnel; this may require me to return it promptly to a VA facility upon request. (SOURCE: MP-7)
- Permit only those authorized by OIT to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software. (SOURCE: AC-6)
- Sign specific VA Information Security ROBs required for access or use of specific VA or non-VA systems. (SOURCE: AC-8)

Sensitive Information

_____
Initials

I Will Not:

- Disclose information protected by VA's privacy statutes or regulations without appropriate legal authority. Unauthorized disclosure of this information may have an adverse effect on agency operations, agency assets and individuals, including myself. (SOURCE: AC-8)

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. (SOURCE: IA-5)
- Protect my passwords, verification codes, tokens, and credentials to prevent unauthorized use and disclosure. (SOURCE: IA-5)
- Maintain possession of my identification credential or VA Personal Identification Verification (PIV) card on or about my person while attending to officially authorized and assigned duties. (SOURCE: AC-3)
- Display my VA credential or PIV card at all times while at a VA facility inside the provided sleeve, worn above the waist on the outermost garment with the photo visible. (SOURCE: AC-3)
- Turn in my VA credential or PIV card when it is expired or the reason for VA having issued it to me has ended. (SOURCE: AC-3)

I Will Not:

- Store my VA passwords or verify codes in any format on any IT system unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption and I am the only person who can decrypt the file. (SOURCE: IA-5)
- Hardcode credentials into scripts or programs. (SOURCE: AC-3)
- Divulge a personal username, password, access code, verify code or other access credentials to anyone. (SOURCE: IA-5)
- Share my credential personal identification number with any other individual. (SOURCE: IA-5)
- Keep my VA credential or PIV card once it has expired or the purpose for VA having issued it to me has ended. (SOURCE: AC-3)

Incident Reporting

I Will:

- Report suspected or identified information security incidents, including loss or theft of GFE, unauthorized disclosures of VA information, or unauthorized access to a VA information system, as well as anti-virus, antispyware, firewall, or intrusion detection software errors or significant

_____
Initials

alert messages (security and privacy) on VA information systems to the enterprise service desk immediately or as soon as reasonably feasible. (SOURCE: IR-4)

Social Media & Networking to Conduct Official VA Business

I Will:

- Use the VA Intranet wherever possible when using social media/networking sites for officially authorized VA purposes. (SOURCE: SC-12)
- Use web-based collaboration and social media tools in accordance with VA Directive 6515, Use of Web-Based Collaboration Technologies. (SOURCE: SC-28)
- Limit the personal use of social media/networking sites on GFE in accordance with VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology. (SOURCE: AC-8)
- Ensure that my use of social media for officially authorized VA purposes complies with law, guidance, and VA policy. (SOURCE: SC-28)
- Be professional when posting to VA-related social media for officially authorized VA purposes. (SOURCE: AC-22)
- Use my best judgment when interacting on social media about matters related to VA's mission when doing so for officially authorized VA purposes. (SOURCE: PL-4)
- Only post and use content in accordance with applicable ethics, intellectual property, records and privacy laws, regulations and policies. (SOURCE: AC-21)
- Use only instant messaging services approved by VA when using VA furnished equipment. (SOURCE: AC-21)
- Publish a disclaimer that the views are my own and do not represent VA, if the content I publish on blogs, wikis, or any other form of user-generated media might reasonably be perceived as the position of VA. (SOURCE: AC-22)

I Will Not:

- Post VA information protected by the Privacy Act of 1974; 38 U.S.C. §§ 5701, 5705 or 7332; the Health Insurance Portability and Accountability Act (HIPAA) Rules, or VA policy on non-VA websites; without legal authority and prior approval by an authorized VA official. (SOURCE: AC-22)
- Indicate that I represent VA unless officially authorized to do so. (SOURCE: AC-22)

Identification of Persona and Branding

I Will:

_____
Initials

- Use display names and branding that are professional, appropriate for the context and align with VA values and mission. (SOURCE: PL-4)
- Be aware that display names and branding may be visible to external audiences and act accordingly to represent VA positively. (SOURCE: PL-4)
- Follow VA policies and guidelines regarding online identification and branding that may require alignment with specific branding or naming conventions. (SOURCE: PL-4)
- Be reminded that VA reserves the right to take disciplinary action if display names or branding are found inappropriate, misleading or damaging to its reputation. (SOURCE: PL-4)

I Will Not:

- Use controversial or polarizing display names or branding that could negatively affect VA or create conflicts. (SOURCE: PL-4)
- Use display names and branding that contains offensive language, can be perceived as discriminatory content or, misrepresents one's identity. (SOURCE: PL-4)
- Use display names and branding that contain personal or sensitive information. (SOURCE: AC-21)
- Use graphical elements in place of names, such as logos, photographs, or custom illustrations that do not meet VA branding guidelines and that are not part of the va.gov design system. (SOURCE: AC-21)

5. ACKNOWLEDGEMENT AND ACCEPTANCE

A. I acknowledge that I have received a copy of the *VA Information Security ROB for Non-Organizational Users*.

B. I understand, accept, and agree to comply with all terms and conditions of the *VA Information Security ROB for Non-Organizational Users*.

C. I will provide a supervisor or appropriate designee a signed copy of this document in a timely manner to ensure awareness and compliance.

D. These provisions are consistent with and do not supersede, conflict with, or otherwise alter any applicable obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information; (2) communications to Congress; (3) the reporting to an Inspector General of a violation of any law, rule, or regulation or mismanagement, a gross waste of funds, an abuse of authority or a substantial and specific danger to public health or safety; or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by applicable Executive Orders and statutory provisions are incorporated into this agreement and controlled.

Print or type your full name _____

Signature _____

Date _____

Office Phone _____

Position Title _____

Appendix C: Glossary

A

Authorized user – Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

Source: NIST SP 800-53

Availability – The term "availability" means ensuring timely and reliable access to and use of information.

Source: NIST SP 800-53

Azure Information Protection (AIP) – Formerly Azure RMS, AIP is a content-based protection technology that works with AIP-enabled applications such as Office 365's Word, Excel, PowerPoint, and Outlook to help safeguard digital content from unauthorized use—both online and offline, inside and outside of the VA firewall. AIP protects content with a publish license that lives in the header of the file or email no matter where the content resides. This helps VA prevent sensitive information from getting into the wrong hands, either intentionally or unintentionally. AIP is an encryption solution which can be used to send encrypted messages internally and externally, in compliance with FIPS 140-2, HIPPA, and other government regulations.

Source*: Adapted from Azure Information Protection Services User's Guide (Version 2.0)

Azure Virtual Desktop (AVD) – AVD is a cloud Desktop-As-A-Service (DaaS) platform. It provides authorized users connecting with VA-issued or privately-owned Windows 10 or Windows 11 computers access to a standardized VA desktop. Two-factor authentication is required to log in.

Source*: https://raportal.vpn.va.gov/Main1/WVDOverview.aspx

B – N/A

C

Citrix Access Gateway (CAG) – CAG is the recommended remote access solution for personally owned equipment (POE) users. CAG is a method of providing access to VA applications without having to install the application on the POE or join the POE device to the VA network. CAG requires the installation of Citrix software, called Receiver, on the end user's device.

Source: Office of Information and Technology, VA ESE OE Remote Bundle Package Storefront 3.6 End User Guide for Chrome OS version 1.3, March 17, 2017 https://raportal.vpn.va.gov/Main1/

Clean desk guidance – Employees must be conscientious of sensitive information on desktops and other work areas in the course of their daily work. Only sensitive information currently being used should be visible on the desktop and should be protected when dealing with customers. When not being used by staff, sensitive information is protected by covering or securing in a manner to prevent incidental disclosure.

Source: Adapted from VA Medical Center Policy

Confidentiality – The term "confidentiality" means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Source: NIST SP 800-53

Contracting Officer Representative (COR) – Individual designated and authorized in writing by the CO to perform specific technical or administrative functions.

Source: VA Handbook 6500.6

Contractor – An individual under contract for furnishing supplies and/or services to VA who will have access to VA information systems and/or physical access to VA facilities, regardless of frequency or length of time.

Source: VA Handbook 0735

Controlled Unclassified Information (CUI) – Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or disseminating controls. Excludes information that is required to be marked classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Source: 32 C.F.R Part 2002 and Executive Order 13556

Cybersecurity – Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: NIST SP 800-53 and OMB Circular A-130

D

Data breach – The loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

Source: 38 U.S.C. § 5727

Designated Records Management Official – A person designated to serve as the records officer for an organization with oversight responsibilities for the management, retention, and disposition of VA records for his or her respective organization, to include Central Office program offices and respective field facilities that fall under his or her purview. Note that the title of this official may vary from one organization to the next. Other titles include, but are not limited to, Records Officer, Records Liaison Officer, Records Management Officer, Records Management Technician, and Records and Information Management Specialist. This designated official works in cooperation and coordination with the VA Records Officer.

Source: Adapted from VA Handbook 6300.1

Disclosure – Disclosure is to reveal or share information. Unauthorized disclosure refers to the communication of VA knowledge or facts, in any medium, without proper authority or in an improper manner. At VA, the principle of disclosure requires that “VA personnel will zealously guard all personal data to ensure that all disclosures are made with written permission or in strict accordance with privacy laws.”

Source: Adapted from VA Directive 6502, VA Handbook 6500.2

E

Employee – An individual who is appointed in the civil service, engaged in the performance of a federal function under authority of law or an Executive act, and subject to the supervision of an individual or officer acting in an official capacity.

Source: Adapted from 5 U.S.C. § 2105(a)

Encryption – Encryption is the cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.

Source: NIST SP 800-82

Endpoint – Endpoints are physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers. Endpoint security, or endpoint protection, helps protect endpoints from malicious actors and exploits.

Source: https://www.microsoft.com/en-us/security/business/security-101/what-is-an-endpoint

Enterprise Service Desk (ESD) – The single point of contact for IT-related issues for all VA employees. The ESD is made up of five pillars: Tier 1 Agents, Case Management, Process Integration, Access Management, and Knowledge Management. All five pillars work together to increase customer satisfaction and reduce system down time.

Source*: https://dvagov.sharepoint.com/sites/OITECOESDCOM/

F

Federal Information Processing Standard (FIPS) – FIPS are standards and guidelines for federal computer systems that are developed by National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular government requirement. Although FIPS are developed for use by the federal government, many in the private sector voluntarily use these standards.

Source: NIST Compliance FAQs

Federal Information Security Modernization Act (FISMA) – A law that requires VA to have an information security program. Title III of the E-Government Act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Source: Adapted from https://csrc.nist.gov/projects/risk-management/fisma-background

Federal Records Act of 1950 – A law that requires VA to maintain a system of records. The Federal Records Act requires federal agencies to make and preserve records that have adequate and proper documentation of their organizations, functions, policies, decisions, procedures, and essential transactions. These records are federal property and must be maintained and managed according to laws and regulations.

Source: Adapted from VA Handbook 6300.1

Federal Tax Information (FTI) – FTI is any return or return information received from the IRS or any secondary source which is protected by the confidentiality provisions of Internal Revenue Code section 6103.

Source: https://www.irs.gov/privacy-disclosure/safeguarding-federal-tax-information-fti-in-aca-printed-notices

G

Government-Furnished Equipment (GFE) – Equipment in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Equipment means a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for the performance of a contract. Equipment is not intended for sale and does not ordinarily lose its identity or become a component part of another article when put into use. Equipment does not include material, real property, special test equipment, or special tooling.

Source: Adapted from https://www.acquisition.gov/far/part-45

GFE Mobile – GFE Mobile was developed as a solution to support remote users with government furnished Apple iOS and Android tablets and smartphones. This solution enables users with approved government furnished mobile devices to connect remotely to the VA Network.

Source: https://raportal.vpn.va.gov/Main1/

H

Hard drive – A rigid magnetic disk fixed permanently within a drive unit and used for storing data. It could also be a removable cartridge containing one or more magnetic disks.

Source: NIST SP 800-88 Rev.1

Health Insurance Portability and Accountability Act (HIPAA) and HIPAA Privacy Rule (1996) – A law that requires VA to keep a person's health information private. HIPAA establishes requirements for protecting the privacy of personal health information. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the Nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

Source: Adapted from https://www.hhs.gov/hipaa/for-professionals/index.html

I

Identity theft – A fraud committed using the identifying information of another person.

Source: 15 USC 1681a.

Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: FIPS 200; NIST SP 800-53

Information security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Source: 38 U.S.C. § 5727

Information Security Knowledge Service (KS) – VA's official intranet site for enterprise Risk Management Framework (RMF) policy and implementation guides. The KS provides cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forms, and the latest information and developments in the RMF.

Source*: Adapted from
https://dvagov.sharepoint.com/sites/OITOIS/knowledgeservice/pages/home.aspx/

Information System Security Officer (ISSO) – An individual working with the senior agency ISSO, Authorizing Official (AO), or Information System Owner to help ensure the appropriate operational security posture is maintained for an information system or program.

Source: CNSSI-4009 [VA Adapted]

Insider threat – An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

Source: CNSSI 4009

Integrity – The act of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Source: NIST SP 800-53

J – N/A

K – N/A

L

Limited personal use – The acceptable, limited conditions for VA employees to use government office equipment, including information technology, for non-government purposes. Employees may do so when such use involves minimal additional expense to the government, is performed on the employee's non-work time, does not interfere with VA's mission or operations, and does not violate standards of ethical conduct for executive branch employees.

Source: Adapted from VA Directive 6001

Lookout – Lookout Mobile Endpoint Security is a mobile security tool. This enterprise-grade mobile security solution provides comprehensive risk management across mobile devices, including iOS and Android, to secure against application, device, and network-based threats while providing visibility and control over data leakage. Lookout makes it easy to integrate with existing security management services and apply policies for increased visibility and reduced risk.

Source: https://digital.va.gov/marketplace/saas-catalog/

M

Malware – A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. It creates a malicious code that takes the form of a virus, worm, Trojan horse, or other code-based malicious entity that infects a host.

Source: NIST SP 800-61

Microsoft SharePoint – Software used to store documents on an intranet site. It can be used to set up collaborative sites to share information with others, manage documents from start to finish, and publish reports to help make decisions.

Source: Adapted from Microsoft

Minimum necessary – Standard that provides key protection of the HIPAA Privacy Rule. The standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of Protected Health Information. The Privacy

Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity. VA's standard requires only the minimum necessary sensitive personal information (SPI) to perform a legitimate business function.

Source: Adapted from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html

Mobile device – 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, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and e-readers.

Source: NIST 800-53; VAH 6500.10

My HealtheVet – My HealtheVet offers tips and tools to help Veterans partner with their health care team. The support tools on this website are designed to enrich the Veteran experience with My HealtheVet and help Veterans make informed decisions.

Source: Adapted from https://www.myhealth.va.gov/mhv-portal-web/about-mhv

N

Need-to-know – A decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

Source: CNSSI 4009-2015 under need-to-know determination

Network – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Source: NIST SP 800-53

Non-Organizational Users – Users other than those explicitly categorized as Organizational Users. These include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for onboarding power of attorney/private attorneys.

Source: Department of Veteran Affairs Information Security Rules of Behavior for Non-Organizational Users.

O

Office of Information and Technology (OIT) – The mission of OIT is to collaborate with our business partners to create the best experience for all Veterans.

Source: https://digital.va.gov/office-of-information-and-technology/

Organizational Users – VA employees, contractors, researchers, students, volunteers, and representatives of federal, state, local, or tribal agencies who are authorized to access VA information and information systems but do not represent a Veteran or claimant.

Source: Department of Veteran Affairs Information Security Rules of Behavior for Organizational Users.

P

Password – A word or group of characters that is used to gain entry to an electronic system. A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.

Source: NIST IR 7298, Glossary of Key Information Security Terms

Penalty – A punitive measure that the law imposes for the performance of an act that is proscribed or for the failure to perform a required act. Penalty is a comprehensive term with many different meanings. It entails the concept of punishment—either corporal or pecuniary, civil or criminal—although its meaning is usually confined to pecuniary punishment. The law can impose a penalty, and a private contract can provide for its assessment. Pecuniary penalties are frequently negotiated in construction contracts in the event that the project is not completed by the specified date.

Source: West's Encyclopedia of American Law, edition 2.

Personal Identity Verification (PIV) Card/Credential – The PIV card is an ID card issued by a federal agency that contains a computer chip that allows it to receive, store, recall, and send information in a secure method. The main function of the card is to encrypt or code data to strengthen the security of both employees' and Veterans' information and physical access to secured areas while using a common technical and administrative process. The method used to achieve this is called Public Key Infrastructure (PKI) technology. PKI complies with all federal and VA security policies and is the accepted global business standard for internet security. As an added benefit, PKI can provide the functionality for digital signatures to ensure document authenticity.

Source: https://www.osp.va.gov/PIV_Information.asp

Personally Identifiable Information (PII) – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Source: OMB Circular A-130

Personal use – Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Examples of authorized personal use would include employees checking their Thrift Savings Plan or other personal investments, seeking employment, communicating with a volunteer charity organization, or scheduling a medical appointment.

Source: VA Directive 6001

Phishing – A scam by which an internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly.

Source: https://merriam-webster.com/dictionary/phishing

Privacy – Ability of an individual to exercise control over the collection, use, and dissemination of their Personally Identifiable Information (PII).

Source: Adapted from Partners Healthcare Glossary of Common Terms, Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Privacy Act of 1974 – Legislation that states how federal agencies can use personal data. The Privacy Act of 1974 establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of Personally Identifiable Information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the subject individual unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.

Source: Adapted from https://www.justice.gov/opcl/privacy-act-1974

Privacy Officer (PO) – The party responsible for taking proactive measures to help ensure that PII collected by VA is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusions upon individual privacy, thereby minimizing privacy

events. Additionally, it is the defensive duty of a PO to assist in mitigating damage when PII is compromised.

Source: VA Directive 6509 [VA Adapted]

Protected Health Information (PHI) – The HIPAA Privacy Rule defines PHI as individually identifiable health information transmitted or maintained in any form or medium by a covered entity, such as the Veterans Health Administration (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. In addition, PHI excludes employment records held by VHA in its role as an employer.

Source: Adapted from 45 C.F.R. § 160.103; VA Directive 6066

Q – N/A

R

Records – All recorded information, regardless of form or characteristics, made or received by an agency of the U.S. Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them.

Source: https://www.archives.gov/records-mgmt/scheduling/id

Records Control Schedule (RCS) – A document that contains the retention and disposition rulings as approved by the National Archives and Records Administration (NARA) that describes how long scheduled VA records must be maintained before being disposed of. An RCS is required by statute. All VA records and information must be identified by records series and be listed in the aforementioned RCS.

Source: Adapted from VA Handbook 6300.1

Records Management – The managerial activities involved with respect to the creation and receipt, maintenance and use, and disposition of records to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of VA operations.

Source: VA Handbook 6300.1

Remote access – Access to a computer or network that is far away. Remote access is access to an organizational information system by a user, or an information system acting on behalf of a user, communicating through an external network (e.g., the internet).

Source: NIST SP 800-18

Remote Enterprise Security Compliance Update Environment (RESCUE) – Cisco AnyConnect VPN (RESCUE) is designed and recommended to be the sole VPN solution for Government-Furnished Equipment (GFE) devices. RESCUE GFE provides a security posture check and ensures VA data is encrypted from the end device into the VA trusted network.

Source: https://www.oit.va.gov/resources/remote-access/

Rules of Behavior (ROB) – The term "VA National Rules of Behavior" refers to a set of Department rules that describe the responsibilities and expected behavior of personnel with regard to information system usage.

Source: VAIQ 7823189, Updated VA Information Security Rules of Behavior, September 23, 2019

S

Sensitive Personal Information (SPI) – Any information about an individual maintained by an agency, including education, financial transactions, medical history, and criminal or employment history, or information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records. Used to reference Federal Tax Information, Personally Identifiable Information, and Protected Health Information.

Source: 38 U.S.C. § 5727

Social engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Source: NIST SP 800-82

Social media – Web- and mobile-based tools that allow persons and groups to exchange ideas. Social media is specifically designed for social interaction that uses highly accessible and scalable publishing techniques using web-based technologies. Social media uses web-based collaboration technologies to blend technology and social interaction in order to transform and broadcast media monologues into social dialogue, thereby transforming people from content consumers to content producers. Examples of social media include Facebook, Flickr, Instagram, instant messaging, and YouTube. This form of media does not include email.

Source: Adapted from VA Directive 6515

Smishing – Smishing is a social engineering tactic that combines phishing with SMS text messages. Cybercriminals typically use smishing attacks to steal your personal data, such as emails, passwords, and banking information.

Source: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-smishing-attack

System Owner – Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

Source: CNSSI 4009-2015

T

Text messages – Short messages sent electronically, especially from one cell phone to another.

Source: https://www.merriam-webster.com/dictionary/text%20message

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (DoS). Examples of threats include phishing, social engineering, and spoofing.

Source: NIST SP 800-53 rev 5

Two-factor authentication – Two-factor authentication requires the use of two different factors to achieve authentication. The factors are defined as (i) something you know (e.g., password, personal identification number), (ii) something you have (e.g., cryptographic identification device, token), and/or (iii) something you are (e.g., biometric).

Source: VA Handbook 6510, *VA Identity and Access Management*

U – N/A

V

VA App Catalog - A source for internal, non-commercial, and commercial apps that have been deemed safe for use with VA sensitive information and for conducting VA business. All apps that will

send, receive, or store VA sensitive data **must** be downloaded from the catalog. The catalog is accessible only by those with VA-furnished devices that are enrolled in Workspace ONE Enterprise Mobility Management (EMM).

Work with your local IT to get enrolled. Once your device is enrolled, the list of available apps will be visible, including the VA App Catalog. Tap on the VA App Catalog icon to install it.

Source: Adapted from the VA App Catalog

VA App Store – A source for secure VA-developed and third-party apps that expand Veterans' access to care, assist with coordination and communication between Veterans and their VA health care teams, and improve the overall Veteran care experience. These apps can be downloaded by Veterans and the health care professionals who serve them. The website also features health care and wellness apps for caregivers and civilians. The VA App Store is available to all devices and does not require that the devices be enrolled in in Workspace ONE Enterprise Mobility Management (EMM). The apps listed on this store are also available on the Apple App Store. Visit the VA Mobile site to access the VA App Store.

Source: https://mobile.va.gov/

VA Confidentiality Statutes – Statutes requiring VA to keep medical claims, information, and health records private:

- VA Claims Confidentiality Statute (formal title, Confidential Nature of Claims), 38 U.S.C. 5701, implemented by 38 CFR Section 1.500-1.527.
- Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Health Records, 38 U.S.C. 7332, implemented by 38 CFR Section 1.460-1.496.
- Confidentiality of Medical Quality Assurance Review Records, 38 U.S.C. 5705, implemented by 38 CFR Section 17.500-17.511.

Source: Adapted from VHA Directive 1605.01

VA Health and Benefits mobile app – This app allows Veterans to manage their VA health care, benefits, and payments from their mobile phone or tablet. It also allows them to send and receive secure messages to and from their VA health care team.

Source: https://mobile.va.gov/app/va-health-and-benefits

VA Mobile – A team that provides technologies that expand clinical care beyond traditional office visits. VA Mobile's website hosts the VA App Store.

Source: https://mobile.va.gov/

VA Sensitive Information – All Department information and/or data on any storage media or in any form or format that requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

VA sensitive information may also be referred to as Controlled Unclassified Information (CUI).

Source: VA Handbook 6500

VA Virtual Office (VAVO) – VAVO is a highly scalable remote access solution that provides teleworkers, small offices, and mobile users with office-like experiences combining voice, video, wireless (upcoming), and real-time data applications in a secure environment. VAVO requires the purchase of special hardware.

Source: https://raportal.vpn.va.gov/Main1/

Virtual Private Network (VPN) – A virtual network built on top of existing networks that can provide a secure communications mechanism for data and internet protocol (IP) information transmitted between networks.

Source: NIST SP 800-113

Virus – A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Source: NIST SP 800-82

W

Wi-Fi – A system of accessing the internet from remote machines, such as laptop computers, that have wireless connections.

Source: https://www.dictionary.com/browse/wifi?s=t

Wireless network – A network of computers that is not connected by cables. Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber-optic cabling between network devices.

Source: Adapted from https://www.lifewire.com/wireless-computer-networking-816540

Workspace ONE® – VMware Workspace ONE® is an intelligence-driven digital workspace platform that simply and securely delivers and manages any app on any device by integrating access control, application management, and multiplatform endpoint management.

Source: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/vmware-workspace-one-datasheet.pdf

X – N/A

Y – N/A

Z – N/A

Appendix D: Privacy and Information Security Resources

The inclusion of external hyperlinks does not constitute endorsement by VA of the linked website(s), or the information, technologies, or services contained therein. For other than authorized VA activities, VA does not exercise any editorial control over the information you may find at these locations. All links are provided with the intent of supporting the mission of VA. VA does not guarantee the availability or performance of external websites.

VA Information Security Knowledge Service (KS) Site

The VA KS site* is a one-stop shop for all your Risk Management Framework, policy, and implementation guide needs:
https://dvagov.sharepoint.com/sites/OITOIS/knowledgeservice/pages/home.aspx/

VA Publications are available via the KS site.

VA Directives and Handbooks

VA Publications can also be accessed on the VA Publications site*:
https://vaww.va.gov/vapubs/index.cfm

Directives

- VA Directive 0701, *Office of Inspector General Hotline Complaint Referrals*
- VA Directive 0710, *Personnel Security and Suitability Program*
- VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*
- VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*
- VA Directive 6011, *VA IT One + One Device Policy*
- VA Directive 6066, *Protected Health Information (PHI) and Business Associate Agreements Management*
- VA Directive 6300, *Records and Information Management*
- VA Directive 6309, *Collections of Information*
- VA Directive 6500, *VA Cybersecurity Program*
- VA Directive 6507, *Reducing the Use of Social Security Numbers*
- VA Directive 6510, *VA Identity and Access Management*
- VA Directive 6512, *Secure Wireless Technology*
- VA Directive 6515, *Use of Web-Based Collaboration Technologies*

Handbooks

- VA Handbook 0710, *Personnel Security and Suitability Program*
- VA Handbook 5011, *Hours of Duty and Leave*
- VA Handbook 5021, *Employee/Management Relations*
- VA Handbook 6300.1, *Records Management Procedures*
- VA Handbook 6300.4, *Procedures for Processing Requests for Records Subject to the Privacy Act*
- VA Handbook 6300.5, *Procedures for Establishing and Maintaining Privacy Act Systems of Records*
- VA Handbook 6300.6, *Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses*
- VA Handbook 6309, *Collections of Information*
- VA Handbook 6500, *Risk Management Framework for VA Information Systems VA Information Security Program*
- VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*
- VA Handbook 6500.6, *Contract Security*
- VA Handbook 6500.10, *Mobile Device Security Policy*
- VA Handbook 6502, *VA Enterprise Privacy Program*
- VA Handbook 6507.1, *Acceptable Uses of the Social Security Number (SSN) and the VA SSN Review Board*
- VA Handbook 6510, *VA Identity and Access Management*
- VA Handbook 6513, *Secure External Connections*
- VA Handbook 6609, *Mailing of Sensitive Personal Information*

VA Forms and Memorandums

VA Forms Home Page* available at: https://vaww.va.gov/vaforms/

- VA Form 0244, *Records Transmittal and Receipt*
- VA Form 0740, *Telework Request/Agreement*
- VA Form 0887, *VA Government Property Loan Form*
- VA Form 10-0708, *Employees Records Clearance - Revised*
- VA Form 7468, *Request for Disposition of Records*

VA Memorandums available via the KS Site* at:
https://dvagov.sharepoint.com/sites/OITOIS/knowledgeservice/pages/das-ois-memos.aspx/

- Memorandum VAIQ 09726796, *Proper Use of Email and Other Messaging Applications*
- Memorandum VAIQ 7633050, *Mandatory Use of PIV Card Authentication for VA Information System Access*
- Memorandum VAIQ 7687162, *Security of Apps on iOS Training*, August 16, 2016
- Memorandum VIEWS 00236140, *Disabling Network Accounts for Non-Compliance of Mandatory VA Privacy and Information Security Awareness and Rules of Behavior Training (Updated)*, September 12, 2019
- Memorandum VIEWS 02621670, *Prohibited Uses of VA Sensitive Information*, June 11, 2020
- Memorandum VIEWS 10343241, *Updated Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) for Non-Organizational Users for Fiscal Year (FY) 2024,* September 28, 2023
- Memorandum VIEWS 10343126, *Updated Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) for Organizational Users for Fiscal Year (FY) 2024,* September 28, 2023

VHA Publications

VHA Publications available at: https://www.va.gov/vhapublications/index.cfm

VHA Directives

- VHA Directive 1605, *VHA Privacy Program*
- VHA Directive 1605.01, *Privacy and Release of Information*
- VHA Directive 1605.02, *Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information*
- VHA Directive 1907.01, *VHA Health Information Management and Health Records*

VA Web Links

- Azure Virtual Desktop – Download the Client: https://www.oit.va.gov/resources/remote-access/azure-virtual-desktop/
- Controlled Unclassified Information (CUI) Awareness: https://www.youtube.com/watch?v=4Bq9tPxp6WY
- CUI - What is Controlled Unclassified Information?*: https://vaww.crr.oit.va.gov/frac/cui/
- Cybersecurity Awareness Portal*: https://vaww.oit.va.gov/cap/

- CyberHero – Telemedicine is Here and Rapidly Changing the Healthcare Industry*: https://dvagov.sharepoint.com/sites/VACyberHERO/SitePages/Telemedicine-is-Here-and-Rapidly-Changing-the-Healthcare-Industry(1).aspx
- Enterprise Service Desk (ESD)*: https://dvagov.sharepoint.com/sites/OITECOESDCOM/
- Government Employee Outside the U.S. Travel Process: https://yourit.va.gov/sys_attachment.do?sys_id=85dbcf8ddb9c4c187e8a388d7c9619ff
- How do I submit a travel request for travel outside of the United States? (KB0107099)*: https://yourit.va.gov/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3Dcdbda3281baae410bafeeaccac4bcb5e
- IT One + One Device Policy*: https://vaww.oit.va.gov/oit/it-one-device-policy/
- ITWD's Role-Based Training*: https://dvagov.sharepoint.com/sites/OITITWD/rbt/pages/default.aspx
- Locator to identify ISSOs*: https://dvagov.sharepoint.com/sites/OITISSOLocator/default.aspx
- Mobile Documentation > Approved Devices and Apps*: https://dvagov.sharepoint.com/sites/OITMT/shared%20documents/forms/documents.aspx?rootfolder=%2Fsysdesign%2Fcs%2Fmt%2Fshared%20documents%2Fapproved%20devices%20and%20apps&folderctid=0x012000ce74b1c730fd694fa9df56b69e70282500e0245bbf72be8c4f93592e1b9acc2ef3&viewid=59ed2ac5%2D9364%2D4f93%2D93d0%2Db77c4bf53e79&id=%2Fsites%2FOITMT%2FShared%20Documents%2FApproved%20Devices%20and%20Apps
- Mobile Documentation > Procedures*: https://dvagov.sharepoint.com/sites/OITMT/shared%20documents/forms/documents.aspx?%20rootfolder=%2Fsysdesign%2Fcs%2Fmt%2Fshared%20documents
- My HealtheVet patient portal: https://www.myhealth.va.gov/mhv-portal-web/home
- My HealtheVet on VA.gov Transition Timeline*: https://vaww.va.gov/MYHEALTHEVET/VAgov_Transition_Timeline.asp
- Office of Electronic Health Record Modernization*: https://vaww.ehrm.va.gov
- Office of Inspector General (Information Requests): https://www.va.gov/oig/foia/
- Office of Research & Development (ORD) Requirements for Surveys & Interviews: https://www.research.va.gov/resources/oasc.cfm
- Office Service Operations, Enterprise Security Operations (ESO), Specialized Device Security Division*: https://dvagov.sharepoint.com/sites/OITESO/default.aspx
- OIT DDE – What is Transparent Screen Lock (TSL)?*: https://dvagov.sharepoint.com/sites/oitdde/SitePages/Transparent-Screen-Lock-(TSL).aspx

- PIV Badge Office: https://www.osp.va.gov/Badge_Office_Locations.asp or https://www.oit.va.gov/programs/piv/how-to.cfm
- PIV Card Project: https://www.oit.va.gov/programs/piv/
- Privacy Officer Locator Resources*: https://dvagov.sharepoint.com/sites/OITPrivacyHub/SitePages/Privacy-Officer-Locator-Resources.aspx
- Project Help Site > Rights Management Service (RMS)*: https://dvagov.sharepoint.com/sites/OITRMS/EndUserInfo/default.aspx
- Resource Center for Office and other Microsoft 365 products*: https://vaww.oit.va.gov/o365/
- SharePoint Online Web request: https://dvagov.sharepoint.com/sites/OITSharePointPlatform
- Social Security Number Reduction*: https://vaww.oit.va.gov/services/privacy/social-security-number-reduction/
- Technical Reference Model (TRM)*: https://trm.oit.va.gov/TRMHomePage.aspx
- VA App Catalog (Workspace ONE EMM Enrollment Instructions Link)*: https://dvagov.sharepoint.com/sites/OITMT/Shared%20Documents/Forms/Documents.aspx?FolderCTID=0x012000CE74B1C730FD694FA9DF56B69E70282500E0245BBF72BE8C4F93592E1B9ACC2EF3&id=%2Fsites%2FOITMT%2FShared%20Documents%2FTechnical%2FActivating%20iOS%20Device%20with%20WorkSpace%20One%20%28Airwatch%29%20for%20DEP%20Devices%2Epdf&parent=%2Fsites%2FOITMT%2FShared%20Documents%2FTechnical
- VA CSOC Threat Assessment and Analysis Portal*: https://dvagov.sharepoint.com/sites/OITOIS/knowledgeservice/taap/pages/home.aspx
- VA CSOC Threat Assessment and Analysis Portal Phishing Awareness*: https://dvagov.sharepoint.com/sites/OITOIS/knowledgeservice/taap/pages/Phishing-Awareness.aspx
- VA Controlled Unclassified Information (CUI)*: https://vaww.oit.va.gov/services/cui/
- VA Enterprise Security Operation Payment Card Industry SharePoint*: https://dvagov.sharepoint.com/sites/OITESO/pci/default.aspx
- VA Mobile/VA App Store: https://mobile.va.gov/appstore
- VA Mobile – VA: Health and Benefits: https://mobile.va.gov/app/va-health-and-benefits
- VA Mobile – VA Video Connect*: https://dvagov.sharepoint.com/sites/VHACCVAMobile/SitePages/VA-Video-Connect.aspx
- VA Privacy Service: https://www.oprm.va.gov/default.aspx
- VA Privacy Service Privacy Hub*: https://dvagov.sharepoint.com/sites/OITPrivacyHub

- VA Privacy Service - Privacy Principles: https://www.oprm.va.gov/privacy/privacy_principles.aspx
- VA Privacy Service Social Security Number Reduction Overview: http://www.oprm.va.gov/privacy/SSNReduction.aspx
- VA Remote Access Information: https://www.oit.va.gov/resources/remote-access/
- VA Remote Access Information and Media Portal*: https://raportal.vpn.va.gov/Main1/
- VA Sensitive Email Communication Guidance*: https://dvagov.sharepoint.com/sites/OITPrivacyHub/NPOF%20Archive/Forms/AllItems.aspx?id=%2Fsites%2FOITPrivacyHub%2FNPOF%20Archive%2FVA%20Sensitive%20Email%20Communication%20Fact%20Sheet%2Epdf&parent=%2Fsites%2FOITPrivacyHub%2FNPOF%20Archive
- VA SharePoint Platform – Required action for all Teams and SharePoint Owners/Admins*: https://dvagov.sharepoint.com/sites/OITSharePointPlatform/SitePages/Required-action-Teams-SharePoint-Owners.aspx
- Veterans Affairs Insider Threat Program Awareness and Reporting Tool: https://www.osp.va.gov/insider_threat_program_awareness_reporting_tool.asp
- VHA Office of Connected Care Help Desk (OCCHD)
  - Ticketing Support: https://occhdsupport.ironbow.com/
  - System Status: https://status.occhdsupport.ironbow.com
- VHA Office of Regulatory and Administrative Affairs – Paperwork Reduction Act*: https://vaww.va.gov/VHAREGS/pra.asp
- Webex Resources*: https://dvagov.sharepoint.com/sites/OITUCIS/webex/SitePages/Webex.aspx
- yourIT Service Portal: https://yourit.va.gov/va
- Zero Trust First* - Cybersecurity Strategy: https://dvagov.sharepoint.com/sites/OITOIS/KnowledgeService/KSPublications/Forms/AllItems.aspx?id=%2Fsites%2FOITOIS%2FKnowledgeService%2FKSPublications%2FVA%2DOIT%2DZero%20Trust%20First%20Cybersecurity%2DStrategy%2Dv04%2D508c%2Epdf&parent=%2Fsites%2FOITOIS%2FKnowledgeService%2FKSPublications

*Accessible only on the VA intranet.

TMS Courses

The Talent Management System is available at: https://www.tms.va.gov/SecureAuth35/

- *Controlled Unclassified Information (CUI)* (VA TMS ID: 4486102)
- *Getting Started with Public Key Infrastructure (PKI) Manual Enroll* (VA TMS ID: 1256927)

- *Learning Secure Payments and PCI* (TMS ID: NFED 7005709)
- *Mobile Training: Security of Apps on iOS Devices* (VA TMS ID: 3926744)
- *PCI Compliance Essentials* (TMS ID: NFED 8001496)
- *Privacy and HIPAA Focused Training* (VA TMS ID: 10203)
- *Social Networking and Security Awareness* (VA TMS ID: 2626967)
- *VA Telework Training Module for Employees* (VA TMS ID: 1367006)

Federal Web Links:

- AR19-Final Rule - Social Security Number Fraud Prevention Act Implementation: https://www.regulations.gov/document/VA-2021-OTHER-0021-0005
- *Federal Information Security Modernization Act (FISMA):* Requires federal agencies to have a program to assess risk and protect information and information security assets that support agency operations: https://www.cisa.gov/federal-information-security-modernization-act
- *Federal Records Act of 1950*: Describes federal agency responsibilities for making and preserving records and for establishing and maintaining active, continuing programs for the economic and efficient management of the records agency. (Related regulations: 44 U.S.C. Chapters 21,29,31,33 and 35 (Federal Records Act); 36 CFR Chapter XII, Subchapter B - Records Management Part 1220-1238; and OMB Circular A-130 Management of Federal Information: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130trans4.pdf
- H.R. 624 - Social Security Number Fraud Prevention Act of 2017: https://www.congress.gov/bill/115th-congress/house-bill/624/text
- H.R.1625 - Consolidated Appropriations Act, 2018 Section 240: https://www.congress.gov/bill/115th-congress/house-bill/1625/text
- National Institute of Standards and Technology (NIST) Publications: https://www.nist.gov/publications
  - NIST SP 800-114, User's Guide to Telework and Bring Your Own Device (BYOD) Security
- OMB-M22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principle: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
- *Paperwork Reduction Act*: Establishes the governance framework and the general principles, concepts, and policies that guide the federal government in managing information and its related resources, including records: https://www.epa.gov/laws-regulations/summary-paperwork-reduction-act
- *Privacy Act of 1974:* Requires federal agencies to establish appropriate safeguards to ensure the security and confidentiality of the records they maintain about individuals, establishes restrictions on the disclosure and use of those records by federal agencies, and permits

individuals to access and request amendments to records about themselves: https://www.justice.gov/opcl/privacy-act-1974

- *The E-Government Act, Section 208, Privacy Provisions*: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
- *The Freedom of Information Act of 1996*: https://www.govinfo.gov/content/pkg/USCODE-2015-title5/pdf/USCODE-2015-title5-partI-chap5-subchapII-sec552.pdf
- *The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009*: https://www.govinfo.gov/content/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf
- *The Health Insurance Portability and Accountability Act (HIPAA) of 1996*: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf
- *The Paperwork Reduction Act of 1995*: https://www.govinfo.gov/content/pkg/USCODE-2014-title44/pdf/USCODE-2014-title44-chap35.pdf
- *United States Code (U.S.C.):* Veterans Confidentiality Statutes
  - 18 U.S.C. 2071 - Concealment, removal, or mutilation generally: https://www.govinfo.gov/app/details/USCODE-2021-title18/USCODE-2021-title18-partI-chap101-sec2071
  - 38 U.S.C. 5101 - Claims and forms: https://www.govinfo.gov/app/details/USCODE-2021-title38/USCODE-2021-title38-partIV-chap51-subchapI-sec5101
  - 38 U.S.C. 5701 - Confidential nature of claims: https://www.govinfo.gov/app/details/USCODE-2021-title38/USCODE-2021-title38-partIV-chap57-subchapI-sec5701
  - 38 U.S.C. 5705 - Confidentiality of medical quality-assurance records: https://www.govinfo.gov/app/details/USCODE-2021-title38/USCODE-2021-title38-partIV-chap57-subchapI-sec5705
  - 38 U.S.C. 7332 - Confidentiality of certain medical records: https://www.govinfo.gov/app/details/USCODE-2021-title38/USCODE-2021-title38-partV-chap73-subchapIII-sec7332

VA Contact Information

- Identity Theft Help Line to report an identity theft incident involving a Veteran: (855) 578-5492
- Office of Inspector General (IG) Hotline to report fraud, waste, or mismanagement of resources: (800) 488-8244
- Office of Research & Development (ORD): VAResearch@va.gov
- Privacy Hotline: (202) 273-5070
- VA Controlled Unclassified Information Team: CUI@va.gov
- VA Data Loss Prevention Program: VADLPPROGRAM@va.gov

- VA Enterprise Service Desk to request computer, network, or access support or to report security incidents to CSOC: (855) 673-4357
- VA Insider Threat Program: insiderthreatprogram@va.gov or 1-202-461-5900
- VHA Office of Connected Care Help Desk (OCCHD): VHA_OCCHD@va.gov or 1-866-651-3180