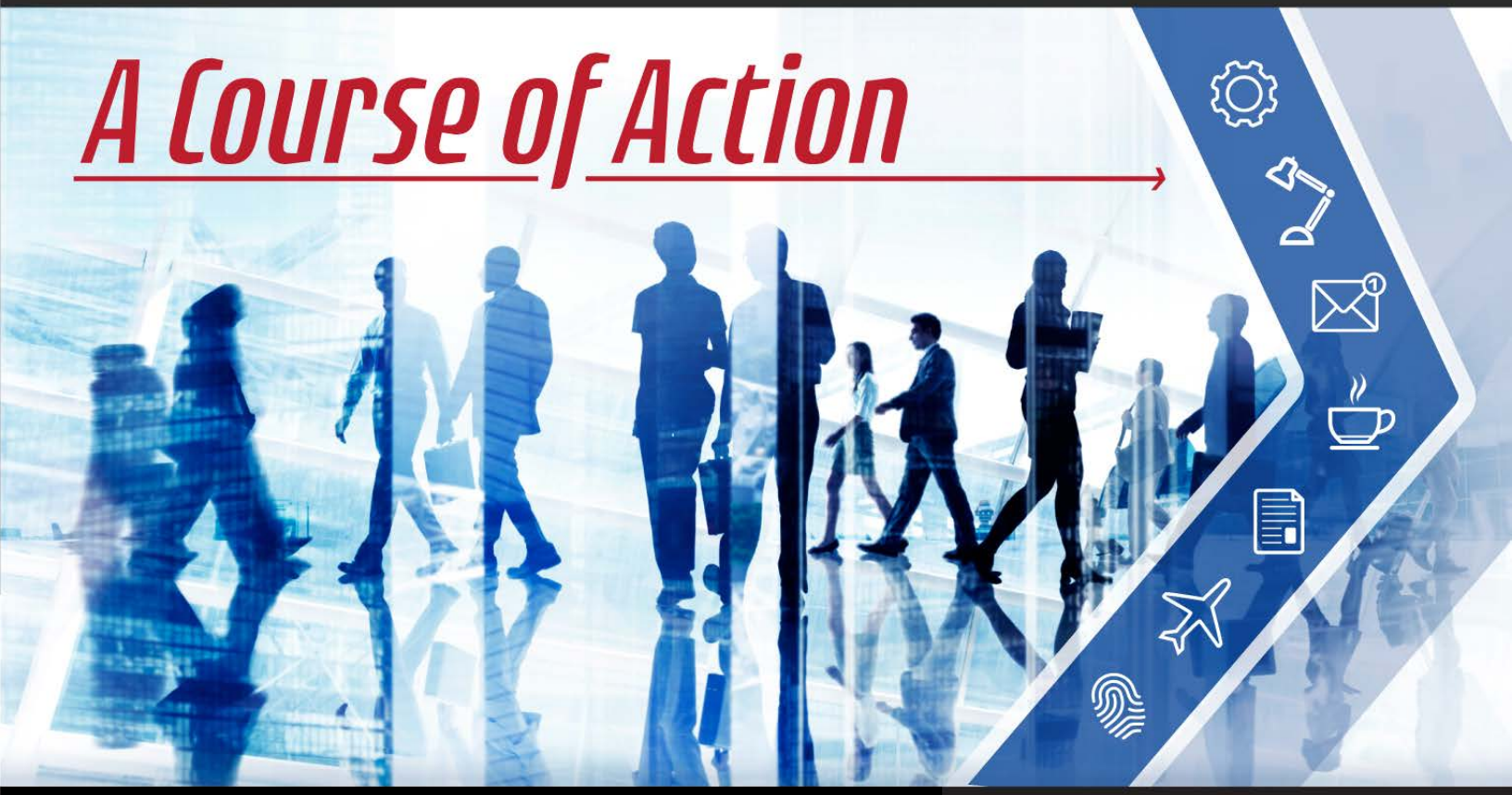
VA Privacy and Information Security Awareness and Rules of Behavior



Text-Only Course Transcript

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

Purpose of This Document

This text-only course transcript was designed to accommodate users in any of these 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 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) 2018 (i.e., October 2017 through September 2018).

You should take the online version of this course if possible. However, if you complete the course using this text-only transcript, you must do the following:

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

   NOTE: There are two versions of the ROB, one for Organizational Users and one for Non-organizational Users. You must initial each page, and then, sign the Acknowledge and Accept section for the user group that applies to you. 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 are able to 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.

Topic 1: Course Introduction

1.1 Welcome

Welcome to *VA Privacy and Information Security Awareness and Rules of Behavior: A Course of Action*.

1.2 Why Are You Taking This Course?

Everyone who comes in contact with VA sensitive information and information systems at VA has a duty to protect privacy and ensure information security. VA must comply with federal laws about privacy and information security. Technology makes it possible for you to use VA information and information systems nearly anytime and anywhere.

This course will help you be more aware of how to protect VA sensitive information and determine what course of action to take whenever privacy or security might be at risk. You must complete this training to use or gain access to VA information or information systems. To maintain your access, you must complete this training each year. In fact, completing this training is one of the Rules of Behavior (ROB) you are required to follow.

Those who must take this training include Organizational and Non-organizational users.

1.3 Who Must Take This Course?

There are two types of users that must take this course, Organizational users and Non-organizational users.

IMPORTANT! User definitions have changed. Please review the definitions to confirm your user type.

Organizational users: VA employees, contractors, researcher, students, volunteers, and representatives of Federal, state, local, or tribal agencies not representing a Veteran or claimant.

Non-organizational users: All information system users other than VA users 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.

Exceptions

Health professions trainees (i.e., student, intern, resident, or fellow) are not required to complete this course. First-time trainees 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).

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

1.4 General Rules That Apply to Both User Groups

Each year when you complete this mandatory training, you review requirements and rules and finish by accepting the ROB. Here are two general rules that apply to both types of users in every situation.

Organizational and Non-Organizational Users

- I will comply with all federal VA information security, privacy, and records management policies.
- I will understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action.

1.5 General Rules for Organizational Users

Here are a few more general rules for Organizational users. Keep these in mind at all times, so you can choose the best course of action. Be sure to read and follow the rules presented throughout the course that apply to your user type.

Organizational Users

- I will have NO expectation of privacy in any records that I create or in my activities while accessing or using VA information systems.
- I will report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor or designee immediately upon suspicion.
- I will secure mobile devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)).
- I will keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information, regardless of work location. I will protect GFE from theft, loss, destruction, misuse, and emerging threats.
    - I will complete mandatory security and privacy awareness training within designated time frames.

1.7 VA Sensitive Information

These are types of VA sensitive information that must be protected:

- Sensitive Personal Information (SPI) is information pertaining to an individual that is maintained by VA. This includes education, financial transactions, medical history, and criminal or employment history. Used synonymously with Personally Identifiable Information (PII), it a way to distinguish or trace one's identity.
- Personally Identifiable Information (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. Some examples include name, home address and phone number, Social Security number, and date of birth.
- Protected Health Information (PHI) includes health records or payment information linked to a specific person. A few examples include patient medical records, patient diagnoses or test results, and patient payment history.
- Regulatory or program-specific information is information that may not be released or may only be released in certain situations. It is information that would not normally be released to the public. Some examples include pricing information submitted to VA by vendors during bid processes, facility or computer room diagrams, documentation of IT systems, and operational business reports.

1.9 Private and Secure Records Management

Like privacy and information security, records management has rules and actions that are required for users of VA information in any media.

This course includes a few key definitions and concepts for managing records securely.

Watch for the records icon (shown below) throughout the course to identify content about records management. You can find a summary of records requirements at the end of the course, and you can review records training available on the TMS.

1.10 Let's Get Started

Most of the course comprises short scenarios with a choice about what to do to protect VA sensitive information and systems. Correct and incorrect feedback provides details related to what you should and should not do in each situation. Additionally, the corresponding ROB are provided as reinforcement of the concepts.

Topic 2: At Your Desk

2.1 Introduction

This section presents situations that usually occur at your desk or workstation**.**

When you've completed this topic, you can recall how to take the best course of action to protect privacy and ensure information security.

Read each scenario and consider the best response. Then, read the ROB that support the correct choice.

2.2 Secure Use of Software

Scenario

While surfing the Internet, you discover a free trial available for a new software product. It sounds like it would help you fend off spyware attacks. You'd like to try it before you request permission to purchase.

Is it okay to go ahead and download the free trial to your VA computer?

Consider the best response:

- **Yes –** It's okay since it's free, and it's only temporary, and you know how to download software because you often do it at home.
- **No –** Downloading this trial anti-spyware software would violate at least three privacy and security Rules of Behavior.

The correct answer is **No**. You must not download software from the Internet. Downloading software yourself violates at least three ROB and could even create a security risk.

Only authorized Office of Information and Technology (OI&T) personnel should install software on your government-furnished equipment. They can make sure you are not bringing viruses or other threats into VA systems and help prevent unexpected security problems.

Only OI&T personnel can perform maintenance on IT equipment, including installation or removal of hardware or software.

Rules of Behavior

Organizational Users:

- I WILL NOT download software from the Internet, or other public available sources, offered as free trials, shareware, or other unlicensed software to a VA-owned system.

- I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA.
- I will permit only those authorized by OI&T to perform maintenance on IT equipment including installation or removal of hardware or software.

2.3 Managing Passwords

Scenario

You have trouble remembering your many VA passwords, so you've decided to try storing them in the notes application (app) on your VA-issued mobile device. There are a lot of requirements for creating VA passwords, so you list those in the notes app, too. You aren't including specific labels with the passwords, so only you will be able to figure it out. You believe it is a safe and convenient method to keep your VA passwords handy.

Is this an acceptable practice?

Consider the best response:

- **Yes –** Using the notes app on your VA-issued mobile device poses no privacy or security risks.
- **No –** Using the notes app on your VA-issued mobile device is risky and violates the ROB.

The correct answer is **No**. Storing VA passwords using the notes app on your VA-issued mobile device would violate at least three ROB. Password requirements include minimum requirements to ensure security when creating or storing passwords. Be sure to review the password requirements when you create new passwords to be sure you meet minimum standards.

You should only store passwords and verify codes in an encrypted file. Putting passwords in the notes app is not secure. You also should not store your password on a piece of paper under your keyboard.

And you must be the only person who can decrypt the file. VA Organizational users must only use VA-approved apps for any storage of sensitive data, including passwords. VA-approved apps are vetted to ensure they protect VA data at rest or in-flight.

Rules of Behavior

Organizational and Non-Organizational Users:

- I will use passwords that meet the VA minimum requirements.
- I will protect my passwords, verify codes, tokens, and credentials from unauthorized use and disclosure.
- I WILL NOT store my passwords or verify codes in any file 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. I will not hardcode credentials into scripts or programs.

2.4 System Access

Scenario

You recently changed jobs within VA. Your new supervisor has coordinated getting access to the new software and systems you need. You liked having access to hospital admissions databases in your old job because you could be "in the know" about people. Today, you noticed that you can still get into one of the old databases, even though you don't need to use it in your new job.

Is it okay for you to continue to view the old database?

Consider the best response:

- **Yes –** If your password still works, it must be okay.
- **No –** You would be violating at least two ROB if you continue to access the old systems.

The correct answer is **No**. You must notify your supervisor or designee any time you have access to a system you no longer need. When you change jobs within VA, your new supervisor determines the systems you need for your new job and coordinates with IT to get you access. If you no longer have a job-related reason to keep access to the systems you used before, you cannot use them. The ROB state that you can only have access to VA computer systems that you are authorized to use for your assigned duties.

Rules of Behavior

Organizational Users:

- I will follow established procedures for requesting access to any VA computer system and for notifying my VA supervisor or designee when the access is no longer needed.
- I will only use my access to VA computer systems and/or records for officially authorized and assigned duties.

2.5 Systems You're Authorized to Use

Scenario

My favorite neighbor is hospitalized at the local VA medical center. My coworker has access to patient information; today, she left her desk but her computer screen was still showing the patient database. So I used her computer to look up my neighbor's condition.

Did I violate any ROB?

Consider the best response:

- **Yes –** You did not have a work-related need to know, and your action was a breach of your neighbor's privacy.
- **No –** Everybody is naturally curious and if you don't tell anyone else, there's no harm done.

The correct answer is **Yes**. Your curiosity about people is no excuse for a breach of privacy, and it's not worth risking disciplinary action! You did not have a work-related need to know, and your action was a breach of your neighbor's privacy. Our concern for others is part of why we work at VA. However, in this case, concern went a little too far.

This example is a violation of several ROB. First, if you aren't authorized to use a system, you can't use it, especially if it isn't on your computer. You should only access devices, systems, and records that you are officially authorized to use in your job, and your coworker should have locked her computer or logged off if it was the end of her workday. Everyone should know that computers must be locked when leaving the area and logged off at the end of the workday.

Viewing your neighbor's sensitive personal information is a privacy incident with potentially severe consequences for you, including disciplinary actions. Don't do it!

Rules of Behavior

Organizational Users:

- I will only use VA approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions.
- I will log out of all information systems at the end of each workday.
- I will logoff or lock any VA computer or console before walking away.

2.6 Disposing of Old Flash Drives

Scenario

You received a voicemail from an individual who said he is a system administrator with OI&T. He asked you to leave your USB flash drive on your desk when you leave today because OI&T is providing new, more secure drives; they will swap the devices overnight so you don't have to worry about being at your desk.

Should you leave the drive out overnight?

Consider the best response:

- **Yes –** Everyone should comply with OI&T requests.
- **No –** Drives should be secured when not in use and should only be given to authorized personnel.

The correct answer is **No**. It might not be easy to tell if the caller is really from OI&T. This could be a scam. Flash drives and other storage devices should never be surrendered to anyone other than authorized OI&T personnel.

Even though all VA-issued storage devices are protected by encryption, do not leave the drive on your desk where anyone walking by could pick it up. Leaving the device on your desk may not seem so risky. However, it would violate at least two ROB. As a precaution, ask your supervisor and other teammates if they received a similar call, and then report the voicemail to your Information Security Officer (ISO). Always report suspicious voicemails like this one to your Information Security Officer (ISO).

Rules of Behavior

Organizational Users:

- I WILL NOT surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee.
- I will secure mobile devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)).

2.8 Overriding Security Controls

Scenario

Duane was in the middle of a busy workday when he received a warning that VA's security software would be upgrading his equipment. His coworker offered to run a program that will override the update and disable the security configuration controls so Duane could continue to work without the interruption of an upgrade. Duane refused the offer.

Did he do the right thing?

Consider the best response:

- **Yes –** The coworker's offer is a violation of ROB.
- **No –** The upgrade will take up too much of his time and cause him to miss work deadlines.

The correct answer is **Yes**. You should never try to avoid a security upgrade. Duane correctly protected VA systems by refusing the offer. There may be a slight disruption to his day, but, in the end, running the upgrade is the right thing to do. However, his coworker's offer clearly violates the ROB and could result in disciplinary action or other penalties and fines.

VA security software and controls are in place to protect VA sensitive information. An override like this violates several ROB. VA's security software and controls are in place to protect VA sensitive information. And you must never attempt to probe your computer system to exploit system controls. If you override these protections or try to probe computer systems, you risk exposing VA information.

Rules of Behavior

Organizational and Non-Organizational Users:

- I WILL NOT attempt to override, circumvent, alter or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff.
- I WILL NOT disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store or use VA information.
- I WILL NOT attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data.

2.9 Summary

When you are using VA systems, you are required to follow the ROB to protect VA information and information systems. Keep this list in mind:

- Always log out of your computer at the end of the workday and lock or log off any time you need to walk away from your desk.
- Always protect your passwords. This means that you must follow the required minimum standards and, as needed, store your passwords where no one else can access them.
- Only use devices and systems you are authorized to use for your assigned duties. Let your supervisor know when you no longer need access.
- Only OI&T personnel can perform maintenance, including the installation of software. Only surrender equipment to OI&T.

Topic 3: Using Email

3.1 Introduction

This section presents situations that usually occur when using email**.**

When you've completed this topic, you can recall how to take the best course of action to protect privacy and ensure information security.

Read each scenario and consider the best course of action. Then, read the ROB that support the correct choice.

3.2 Use VA Email and Do Not Auto-Forward

Scenario

Edward is a member of a project team delivering services to VA under a contract. He finds it inconvenient to log in to the VA email system and prefers to use his company's email system. He is planning to set up an auto-forward option so his VA email will be sent to his company account.

Is this a violation of the ROB?

Consider the best response:

- **Yes –** Auto-forwarding creates risk of exposing unencrypted VA sensitive information.
- **No –** Since Microsoft Outlook has this feature, it is safe to use.

The correct response is **Yes**. This violates at least two ROB. Many contract employees have both a VA email address and another business address. Since Edward has a VA email address, he must use it. When you use VA email, backup copies are kept so that VA can track business actions and manage federal records.

If you auto-forward messages, some responses may not be tracked by VA, which risks violating records management requirements. VA systems have safeguards in place to help protect information; outside email systems do not have the same VA safeguards.

Rules of Behavior

Organizational Users:

- I will use VA e-mail in the performance of my duties when issued a VA e-mail account.
- I WILL NOT auto-forward e-mail messages to addresses outside the VA network.

3.3 Limited Personal Use of VA Equipment

Scenario

You recently started a side business selling household items online and decide to use your VA email to receive customer messages throughout the day. You also want to check your website regularly, so you set it up as a favorite on your VA GFE.

Is this acceptable as "limited personal use" of VA equipment?

Consider the best response:

- **Yes –** You won't get many messages; you just want to stay on top of it.
- **No –** This is an inappropriate personal use of VA equipment.

The correct answer is **No**. This example describes activities that are not allowed. VA policy permits employees to have limited personal use of VA-furnished office equipment under certain conditions; however, the use must involve minimal additional cost to VA, must be performed on non-work time, must not interfere with the VA mission or operations, and must not violate standards of ethical conduct. You may not use VA equipment to operate a business either during or outside of your normal business hours. By the way, if your VA work involves using systems of another federal agency, personal use of those systems is never allowed. See VA Directive 6001 for a list of uses that are not allowed.

Rules of Behavior

Organizational Users:

- I WILL NOT engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.

3.4 Encrypting Emails

Scenario

Camille has been reminded several times to encrypt her emails. She has trouble remembering when she should and shouldn't encrypt. She decides to set up Outlook to automatically encrypt every email.

Is this the right way to use encryption for emails?

Consider the best response:

- **Yes –** She doesn't have time to decide about every email.
- **No –** She is overusing encryption.

The correct answer is **No**. It is important to encrypt emails that contain VA sensitive information, but there's no need to encrypt every message. In fact, that goes against the ROB. It is up to you to determine which emails should be encrypted.

There are some exceptions. VBA normally defaults the email setting to auto-encrypt to reduce the number of potential incidents related to encryption by VBA users. However, VBA users are still required to unencrypt emails that do not contain sensitive information.

Contact the VA National Service Desk for any questions about encryption.

Rules of Behavior

Organizational Users:

- I will encrypt email, including attachments, which contain VA sensitive information. I will not encrypt email that does not include VA sensitive information or any email excluded from the encryption requirement.

3.5 Casual Disclosure of Sensitive Information

Scenario

Garrett works as a receptionist at a VA substance abuse treatment center. A friend who works in the public information office of a nearby university wants to do a human-interest article about VA's substance abuse treatment programs. The friend asks for names of some Veterans to interview. Garrett quickly emails the names and phone numbers of three patients he knows are students.

Did he do the right thing?

Consider the best response:

- **Yes –** His VA clinic has an opportunity for some good publicity from a trusted reporter, and he is helping make it happen.
- **No –** There are especially stiff penalties for disclosing any sensitive information about the diagnosis or treatment of drug or alcohol abuse.

The correct answer is **No**. Garrett has violated several rules about disclosure of VA sensitive information.

Always ask for your supervisor's advice and approval before responding to a request for information if it is beyond the normal duties of your job, especially if VA sensitive information is involved. In his job, Garrett is not authorized to respond to news media.

He has also violated laws that prohibit disclosing VA sensitive information about certain diagnoses, including treatment for drug or alcohol abuse, HIV, or sickle cell anemia. Be especially careful when anyone asks you for patient information in these treatment categories as there are severe penalties for inappropriate disclosure.

Releasing this type of protected health information could cause serious harm to the Veterans or to VA. For more information, see Title U.S.C. 7332: Confidentiality of Certain Medical Records.

Rules of Behavior

Organizational Users:

- I will obtain approval prior to public dissemination of VA information via e-mail as appropriate.
- I WILL NOT make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to, e-mail, instant messaging, online chat, and web bulletin boards or logs.
- I WILL NOT disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals.

- 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. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk.

3.6 Summary

When using email, it is important to follow the ROB to protect VA information. Keep the following in mind:

- Always use your VA email account, if you are issued one. Be sure to keep personal use to a minimum.
- Never auto-forward VA emails to another email account. This will cause confusion and records management challenges.
- Never disclose information you are not authorized to share. Always ask for your supervisor's advice and approval before responding to a request for information if it is beyond the normal duties of your job, especially if PII or PHI is involved. This includes a list of very specific health conditions.
- Always encrypt emails that contain any type of VA sensitive information.

Topic 4: In VA Public Spaces

4.1 Introduction

This section presents situations that usually occur in VA public spaces**.**

When you've completed this topic, you can recall how to take the best course of action to protect privacy and ensure information security.

Read each scenario and consider the best course of action. Then, read the ROB that support the correct choice.

4.2 Providing Access Based on Need to Know

Scenario

You need to post a report to a Microsoft SharePoint site that is restricted to your project team. The report includes a list of individuals and their Social Security numbers.

Is this a violation of the ROB?

Consider the best response:

- **Yes –** It is a violation because you can't be sure every role on the project team has the need to know this information.
- **No –** It is not a violation because members of the project team can all be trusted with the information.

The correct answer is **Yes**. VA allows the use of certain web-based collaboration tools, including Microsoft SharePoint, to enable people to work together and share business information. While VA SharePoint is a secure tool, you are responsible to ensure that anything you post there is only viewed by those with a need to know. Access to the site may change without your knowledge, which could accidentally disclose sensitive information to some individuals who do not have a need to know.

First, determine if the group's need to know is better served by encrypting and emailing documents containing VA sensitive information rather than sharing them on the SharePoint site.

SharePoint administrators (or managers) need to limit access to files and folders that contain sensitive information on SharePoint to those with a need to know. Access lists need to be reviewed periodically to ensure all who are listed are still qualified for access.

Rules of Behavior

Organizational Users:

- I will only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information.

4.3 Wireless Access

Scenario

Joe often hosts meetings at his VA facility with a group of contractors who have Citrix Access Gateway (CAG) access to the VA network. He sometimes uses a personal wireless access point and connects it to his laptop and an open network jack in the meeting room. The group connects to his personal wireless access point to view a database on the VA network.

Does Joe's use of wireless technology comply with the ROB?

Consider the best response:

- **Yes –** He is in compliance since all participants are users with CAG access.
- **No –** Joe has violated at least two rules.

The correct answer is No. It appears Joe has violated two of the rules for using wireless technology. The ROB state that you will not set up a wireless access point unless you are explicitly authorized; it sounds like Joe uses his personal access point as needed, without getting permission. The ROB also state that you cannot have a VA network connection and a non-VA network connection physically connected to any device at the same time; connecting his wireless router to both his laptop and the VA network jack does not comply with this rule.

The solution? Get permission before using any type of Internet server or wireless access point. Alternatively, check whether your facility offers VA-approved guest access to facilitate contractor access.

- I WILL NOT host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner, local Chief Information Officer (CIO) or designee, and approved by my Information Security Officer (ISO). SOURCE: AC-18
- I WILL NOT have a VA network connection and a non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any device at the same time unless the dual connection is explicitly authorized.

4.4 Connecting Non-GFE to a Facility Network

Scenario

Mark is a contractor visiting his VA Project Manager at a VA facility for a day of meetings. He usually works remotely and does not have a VA-furnished computer. He has his company computer with him, along with a PIV credential reader. He has the Facility Chief Information Officer's (CIO) permission to use remote access capabilities to connect to the VA Intranet as needed whenever he visits the facility.

Is Mark obeying the ROB?

Consider the best response:

- **Yes –** Mark received permission from the Facility CIO before using remote access when visiting the facility.
- **No –** Mark should never use a non-VA computer when he visits a VA facility.

The correct answer is **Yes**. Although Mark is a contractor, he is still an organizational user. Because his company-owned computer uses VA-approved software to access the VA network and he obtained the CIO's permission in advance, Mark has met the requirements needed to connect his non-GFE equipment to VA's network while visiting a VA facility.

Rules of Behavior

Organizational Users:

- I will only use VA-approved solutions for connecting non-VA-owned systems to VA's network.
- I will obtain approval prior to using remote access capabilities to connect non-GFE equipment to VA's network while within the VA facility.

4.5 Using Other Federal Agencies' Information Systems

Scenario

Denise is on an interagency committee that requires her to enter information into a Department of Defense (DoD) system.

Does she have to take the DoD privacy and security training in order to use the DoD systems even if she has already taken VA's privacy and security training?

Consider the best response:

- **Yes –** Every agency has its own policies, so she must take any training that is required.
- **No –** If she has taken VA's training, it should be about the same for any other agency.

The correct answer is **Yes**. Each federal agency has its own ROB and required privacy and security training before getting access to its systems. You must complete any required training and sign and abide by the entity's specific ROB.

If you follow the other agency's terms of the system, you can use it for your specific duties. However, personal use is prohibited.

Rules of Behavior

Organizational Users:

- I will only use other Federal government information systems as expressly authorized by the terms of those systems; personal use is prohibited.
- I will sign specific or unique ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity's ROB to conduct VA business. While using their system, I must comply with their ROB.

4.6 Summary

Keep the following in mind when you are sharing information:

- Only provide sensitive information to those who need to know to complete their duties.
- Never host, set up, administer, or operate any type of Internet access without explicit authority.
- Only connect non-VA equipment to VA networks using VA-approved solutions. And only use remote access capabilities to connect GFE to VA's network while within the VA facility.

Topic 5: Handling Paper

5.1 Introduction

This section presents situations that usually occur when handling paper.

When you've completed this topic, you can recall how to take the best course of action to protect privacy and ensure information security.

Read each scenario and consider the best course of action. Then, read the ROB that support the correct choice.

5.2 Using Minimum Necessary Information

Scenario

Ruth is a clinic administrator. She creates a weekly report about how much time it takes to see patients at the clinic. The data report includes a line number for each patient, the diagnostic codes for the visit, and sign-in/sign-out times. No patient identifiers are included for each line.

Does this approach protect VA sensitive information?

Consider the best response:

- **Yes –** Only the minimum necessary information is listed.
- **No –** Personal information is disclosed.

The correct answer is **Yes**. The report protects VA sensitive information because it contains the minimum necessary information for the business purpose and contains no information that risks disclosing any personal information.

Rules of Behavior

Organizational Users:

- I will protect Sensitive Personal Information (SPI) aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function.

5.3 Securing Documents When Not in Use

Scenario

Francis has been working with patient information all day. He's been reviewing electronic and printed reports that include sensitive information. He logs off his computer and leaves for the day, with his paper files neatly stacked on his desk and his office door unlocked.

Is this a violation of the ROB?

Consider the best response:

- **Yes –** He left sensitive information on his desk and did not lock the door.
- **No –** He logged off his computer.

The correct answer is **Yes.** This is a violation of the ROB. While Francis did secure his computer, he did not secure the printed materials on his desk and he did not lock the door.

He should have secured the reports in a locked desk drawer. Maintain a clean desk policy to ensure you do not leave VA sensitive information on your desk during the day or when you leave for the day.

Administrations may have differing guidance. VBA does not authorize materials containing sensitive information to be locked away. This is to prevent claims folders from being locked in someone's cabinet or desk drawer.

Always check with your supervisor or Records Management Officer for the procedure at your facility.

Rules of Behavior

Organizational Users:

- I will ensure that all printed material containing VA sensitive information is physically secured when not in use (e.g., locked cabinet, locked door).

5.4 Secure Faxing

Scenario

A patient would like you to fax her files to a non-VA clinic. The receiving clinic's fax machine is in a room that is secured with badge entry.

Is it okay to fax the file?

Consider the best response:

- **Yes –** The area is secure with badge entry.
- **No –** The information may still be at risk.

The correct answer is **Yes**. In this case, the recipient's fax machine is in a secured area requiring badge entry, so the fax may be sent safely. Be sure to follow the appropriate procedures if sending a fax is the only solution. The ROB provide additional guidance.

Rules of Behavior

Organizational Users:

- I will 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 included.
- I will transmit individually identifiable information via fax only when no other reasonable means exist, and when someone is at the machine to receive the transmission or the receiving machine is in a secure location.

5.5 Summary

When you work with paper documents, keep the following in mind:

- List only the minimum necessary VA sensitive information to perform a legitimate business function.
- Secure printed materials that contain sensitive information by using the clean desk policy. If it contains sensitive information, lock it away.
- If you must fax, follow standard procedures when faxing. This includes using a cover sheet, double-checking the fax number, and confirming delivery.

Topic 7: Exercise Caution to Prevent Incidents

7.1 Introduction

This section provides a high-level overview of when to use extra caution to make a big difference. Think about:

- The most common, high-impact security incidents you can help prevent
- The priorities the Inspector General has identified
- Best practices for records management for everyone
- Best practices and recertification for users of VA-provided Apple (iOS) mobile devices

Knowing the basics and using best practices will help you make good choices to prevent incidents and protect VA and Veterans.

7.2 Who to Ask

If you have general questions about a real-life situation, you can always ask your supervisor or call the VA National Service Desk. Or:

- If your question is about privacy, ask your Privacy Officer (PO).
- If your question is about information security, ask your Information Security Officer (ISO).
- If your question is about records, ask a Records Officer.

Use the Locator information found in the Resources to help you identify your PO or ISO.

7.3 Most Common or High-Impact Incidents

VA tracks the number and impact of privacy and security incidents. The goal is to identify patterns and prevent future incidents. Take a close look at this list of incidents that most commonly put VA and Veterans at risk. Always use the ROB to guide your actions to prevent incidents like these.

- Mishandling of sensitive paper documents
- Mismailings
- Missing or stolen equipment
- Pharmacy items/Consolidated Mail Outpatient Pharmacy (CMOP) mismailed
- Lost mobile phone
- Policy violation
- Lost PIV cards or credentials
- Internal unencrypted emails
- Unauthorized access or disclosure

- IT equipment inventory missing

7.4 IG Report

The VA Office of the Inspector General (IG) annually reviews VA's progress in achieving security program goals. Sometimes the IG points out weaknesses that can be addressed by better communication or training.

Examples include more awareness of risks when using social media and more awareness of how to prevent phishing attacks.

7.5 No Use of Personal Email for VA Business

VA established a policy in 2015 that prohibits using personal email for VA business (VAIQ #7581492: *Use of Personal Email*). If you use your personal email for VA business, you are putting VA at risk.

Personal email is not properly encrypted and potentially exposes VA sensitive information. Using personal email also potentially violates the requirement to maintain copies of emails that are considered federal records.

The policy allows for limited use of personal email in emergency situations with approval from the ISO. However, in these situations, you must send these personal emails to your records management contact within 20 days.

7.6 Secure Management of Records

Here are privacy and information security ROB to keep in mind for records management.

Organizational users:

- I will comply with all federal VA information security, privacy, and records management policies.
- I will have NO expectation of privacy in any records that I create or in my activities while accessing or using VA information systems.

7.9 Summary

Keep the following in mind when exercising caution to prevent incidents:

- Know who to contact when there's an incident
- Be aware of the common, high-impact security incidents
- Keep the IG's priorities in mind

Topic 8: Summary and Rules of Behavior

8.1 Conclusion

Recall privacy and security ROB:

- Whenever you use VA systems and networks
- When you have conversations about patients or Veterans
- When you send and receive emails
- When you handle any material containing VA sensitive information
- When you handle records.

That's right, remember the ROB all the time, everywhere.

8.2 Acknowledge, Accept, and Comply With the ROB

Working for VA, you may access and use VA information systems or you may come in contact with VA sensitive information. This means you must accept responsibility for protecting privacy and ensuring information security. The ROB are the minimum compliance standards for VA personnel in all locations. If your location has rules that are stricter than the information security rules, you must obey them.

Read all of the ROB closely. By accepting and acknowledging the ROB, you are agreeing to uphold all of the behaviors stated in the rules. Many, but not all, of the ROB have been explained in this course.

To complete this training, you must review, initial, and sign the appropriate ROB for your user type.

NOTE: There are two versions of the ROB, one for Organizational Users and one for Non-organizational Users. You must initial each page, and then, sign the Acknowledge and Accept section for the user group that applies to you.

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

Non-Organizational Users 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 and signed the ROB document, you must submit the document to your supervisor or designee for documentation of course completion.

8.3 Congratulations

Congratulations! Once you have signed and submitted the ROB, you will have successfully completed *VA Privacy and Information Security Awareness and Rules of Behavior: A Course of Action*.

Upon completion of this course, you should be prepared to protect privacy, ensure the security of VA sensitive information, and comply with the Rules of Behavior.

Appendix A: Department of Veteran Affairs Information Security Rules of Behavior for Organizational Users

1. COVERAGE

a. Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) provides the specific responsibilities and expected behavior for organizational users and non-organizational users of VA systems and VA information as required by 0MB Circular A-130, Appendix Ill, paragraph 3a(2)(a) and VA Handbook 6500, *Managing Information Security Risk: VA Information Security Program.*

b. *Organizational users* are identified as VA employees, contractors, researchers, students, volunteers, and representatives of Federal, state, local or tribal agencies not representing a Veteran or claimant.

c. *Non-organizational users* are identified as all information system users other than VA users 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 on-boarding power of attorney/private attorneys.

d. VA Information Security ROB 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 VA Information Security ROB provides the minimal rules with which individual users must comply. Authorized users are required to go beyond stated rules using "due diligence" and the highest ethical standards.

2. COMPLIANCE

a. Non-compliance with VA ROB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include restricting access, suspension of access privileges, reprimand, demotion and suspension from work. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may result in criminal sanctions.

b. Unauthorized accessing, uploading, downloading, changing, circumventing, or deleting of information on VA systems; unauthorized modifying VA systems, denying or granting access to VA systems; using VA resources for unauthorized use on VA systems; or otherwise misusing VA systems or resources is strictly prohibited.

c. VA Information Security Rules of Behavior (ROB) does not create any other right or benefit, substantive or procedural, enforceable by law, by a party in litigation with the U.S. Government.

3. ACKNOWLEDGEMENT

a. VA Information Security ROB must be signed before access is provided to VA information systems or VA information. The VA ROB must be signed annually by all users of VA information systems or VA information. This signature indicates agreement to adhere to the VA ROB. Refusal to sign VA Information Security ROB will result in denied access to VA information systems or VA information. Any refusal to sign the VA Information Security ROB may have an adverse impact on employment with VA.

b. The ROB 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 Acknowledgement and Acceptance For Other Federal Government Agency users, documentation of a signed ROB will be provided to the VA requesting official.

4. INFORMATION SECURITY RULES of BEHAVIOR

Access and Use of VA Information Systems

I Will:

- Comply with all federal VA information security, privacy, and records management policies. SOURCE: PM-1
- Have NO expectation of privacy in any records that I create or in my activities while accessing or using VA information systems. SOURCE: AC-8
- Use only VA-approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. SOURCE: AC-6
- Follow established procedures for requesting access to any VA computer system and for notifying my VA supervisor or designee when the access is no longer needed.
  SOURCE: AC- 2
- Only use my access to VA computer systems and/or records for officially authorized and assigned duties. SOURCE: AC-6
- 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 walking away. SOURCE: AC-11
- Only use other Federal government information systems as expressly authorized by the terms of those systems; personal use is prohibited. SOURCE: AC-20
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network.
  SOURCE: AC-20

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data. SOURCE: AC-6
- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8
- Have a VA network connection and a non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any device at the same time unless the dual connection is explicitly authorized. SOURCE: AC-17 (k)

- Host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner, local Chief Information Officer (CIO) or designee, and approved by my Information Security Officer (ISO). SOURCE: AC-18

Protection of Computing Resources

I Will:

- Secure mobile devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)). SOURCE: AC-19

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee. SOURCE: MP-4
- 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: CM-3

Electronic Data Protection

I Will:

- Only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA. SOURCE: Sl-3
- Safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using FIPS 140-2 validated encryption (or its successor) unless it is not technically possible. This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)). SOURCE: SC-13
- Only use devices encrypted with FIPS 140-2 (or its successor) validated encryption. VA owned and approved storage devices/media must use VA's approved configuration and security control requirements. SOURCE: SC-28
- Use VA e-mail in the performance of my duties when issued a VA email account. SOURCE: SC-8
- Obtain approval prior to public dissemination of VA information via e- mail as appropriate. SOURCE: SC-8

I Will Not:

- Transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption. SOURCE: AC- 18
- Auto-forward e-mail messages to addresses outside the VA network. SOURCE: SC-8
- Download software from the Internet, or other public available sources, offered as free trials, shareware; or other unlicensed software to a VA- owned system. SOURCE: CM-11
- Disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store or use VA information. SOURCE: CM- 10

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames, and complete any additional role-based security training required based on my role and responsibilities. SOURCE: AT-3
- I Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. SOURCE: AU-1
- 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: MA-2
- Permit only those authorized by OI&T to perform maintenance on IT components, including installation or removal of hardware or software. SOURCE: MA-5
- Sign specific or unique ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity's ROB to conduct VA business. While using their system, I must comply with their ROB. SOURCE: PL-4

Sensitive Information

I Will:

- Ensure that all printed material containing VA sensitive information is physically secured when not in use (e.g., locked cabinet, locked door). SOURCE: MP-4
- Only provide access to sensitive information to those who have a need- to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. SOURCE: UL-2
- 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. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk. SOURCE: UL-2
- Obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)). SOURCE: UL-2
- Protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use encryption products approved and provided by VA to protect sensitive data. SOURCE: SC-13
- Transmit individually identifiable information via fax only when no other reasonable means exist, and when someone is at the machine to receive the transmission or the receiving machine is in a secure location. SOURCE: SC-8
- Encrypt email, including attachments, which 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: SC-8
- Protect Sensitive Personal Information (SPI) aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function. SOURCE: SC-28

_____

- Ensure fax transmissions are sent to the appropriate destination. This includes double checking the fax number, confirming delivery, using a fax cover sheet with the required notification message included. SOURCE: SC-8

I Will Not:

- Disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals. SOURCE IP-1
- Allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance by my VA supervisor, ISO, and Information System Owner, local CIO, or designee. SOURCE: AC-20
- Make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to, e-mail, instant messaging, online chat, and web bulletin boards or logs. SOURCE: SC-8

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements.
  SOURCE: IA-5 (1)
- Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure. SOURCE: IA-5 (h)

I Will Not:

- Store my passwords or verify codes in any file 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. I will not hardcode credentials into scripts or programs. SOURCE: IA-5 (1) (c)

Incident Reporting

I Will:

- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor or designee immediately upon suspicion. SOURCE: IR-6

5. ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of these Rules of Behavior VA information Security Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of VA Information Security Rules of Behavior.

_____	_____
Print or type your full name	Signature Date
_____	_____
Office Phone	Position Title