

VA Privacy and Information Security Awareness and Rules of Behavior

A Course of Action



FY18 Text-Only Course Transcript

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



Table of Contents

Purpose of This Document.....	iv
Using Hyperlinks Within This Document	iv
Topic 1: Course Introduction	1
1.1 Welcome	1
1.2 Why Are You Taking This Course?	1
1.3 Who Must Take This Course?	1
1.4 General Rules That Apply to Both User Groups.....	2
1.5 General Rules for Organizational Users.....	2
1.6 General Rules for Non-Organizational Users	2
1.7 VA Sensitive Information	3
1.8 Mandatory Training for Users of VA-Furnished Mobile Devices	3
1.9 Private and Secure Records Management.....	4
1.10 Let's Get Started	4
Topic 2: At Your Desk	5
2.1 Introduction	5
2.2 Secure Use of Software	5
2.3 Managing Passwords	6
2.4 System Access.....	7
2.5 Systems You're Authorized to Use.....	8
2.6 Disposing of Old Flash Drives	9
2.7 Auto-populating Internet Sites	10
2.8 Overriding Security Controls.....	11
2.9 Summary.....	12
Topic 3: Using Email	13
3.1 Introduction	13
3.2 Use VA Email and Do Not Auto-Forward	13
3.3 Limited Personal Use of VA Equipment	14
3.4 Encrypting Emails.....	15
3.5 Casual Disclosure of Sensitive Information	16
3.6 Summary.....	17
Topic 4: In VA Public Spaces.....	18
4.1 Introduction	18



4.2 Providing Access Based on Need to Know	18
4.3 Wireless Access	19
4.4 Connecting Non-GFE to a Facility Network	20
4.5 Using Other Federal Agencies' Information Systems	21
4.6 Summary	22
Topic 5: Handling Paper	23
5.1 Introduction	23
5.2 Using Minimum Necessary Information	23
5.3 Securing Documents When Not in Use	24
5.4 Secure Faxing	25
5.5 Summary	25
Topic 6: Working Away From VA	26
6.1 Introduction	26
6.2 Encryption of Devices and Equipment	26
6.3 Encryption	27
6.4 Working Remotely	28
6.5 Permission for Remote Access	29
6.6 Telework	30
6.7 International Travel	31
6.8 Summary	32
Topic 7: Exercise Caution to Prevent Incidents	33
7.1 Introduction	33
7.2 Who to Ask	33
7.3 Most Common or High-Impact Incidents	33
7.4 IG Report	34
7.5 No Use of Personal Email for VA Business	34
7.6 Secure Management of Records	34
7.7 Recertification for Users of VA-Provided Mobile Phones (iPhones)	35
7.8 More Reminders for Mobile Device Users	35
7.9 Summary	36
Topic 8: Summary and Rules of Behavior	37
8.1 Conclusion	37
8.2 Acknowledge, Accept, and Comply With the ROB	37
8.3 Congratulations	38
Appendix A: Department of Veteran Affairs Information Security Rules of Behavior for Organizational Users	A-1



Appendix B: Department of Veteran Affairs Information Security Rules of Behavior for Non-Organizational Users	B-1
Appendix C: Glossary	C-1
Appendix D: Privacy and Information Security Resources	D-1



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](#).

1.6 General Rules for Non-Organizational Users

Here are a few more general rules for Non-organizational users. Keep these in mind as 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.

Non-Organizational Users:

- 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) on VA information systems to a VA ISO, local CIO, and Information System Owner immediately upon suspicion.
- I will have NO expectation of privacy in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes.
- I will protect Government Furnished Equipment (GFE) from theft, loss, destruction, misuse, and 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.

1.8 Mandatory Training for Users of VA-Furnished Mobile Devices

Users of VA-issued mobile devices must complete mandatory security training before receiving the device and must refresh their training each year.

Completing this Annual Privacy and Information Security Awareness training meets the annual recertification requirement for users of VA-issued mobile devices.

The mobile icon (shown below) appears throughout the course to identify content that supports the mobile device recertification requirement. You are also encouraged to review *Mobile Training: Security of Apps on iOS Devices*, TMS #3926744.





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.

Non-Organizational Users:

- 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.
- I will if authorized to directly connect to a VA system, 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 GFE or VA IT components, 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.

Non-Organizational Users:

- I WILL NOT divulge a personal username, password, access code, verify code, or other access credential to anyone.

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.

Non-Organizational Users:

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

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.

Non-Organizational Users:

- I will follow VA policies and procedures for handling Federal Government IT equipment and sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

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)).

Non-Organizational Users:

- I WILL NOT swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee.

2.7 Auto-populating Internet Sites

Scenario

When using her personal smartphone, Sue allows her usernames and passwords to save and automatically populate on her favorite social media sites. This allows her to log in without typing her password.

Can she use this same type of automatic log-in for her VA-issued mobile device and VA systems?

Consider the best response:

- **Yes** – This approach will be convenient and efficient.
- **No** – This approach creates unacceptable risks for VA devices and systems.

The correct answer is **No**. Never risk exposing VA's sensitive information. Using automatic log-in to social media sites on your VA mobile device risks enabling others to access VA systems. It may be easier to automatically log in to [social media](#) sites on a personal smartphone, but if you hardcode credentials like this to auto-populate your log-in for VA networks, you risk exposing VA's sensitive information. You also violate the ROB.

VA has [two-factor authentication](#) to reduce risk by controlling access to information systems. VA system users use the [Personal Identity Verification \(PIV\) card/credential](#) to gain access to VA facilities and information systems. Be careful to protect your PIV credential from being lost or stolen.

Rules of Behavior

Organizational and Non-Organizational Users:

- I WILL NOT hardcode credentials into scripts or programs.





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

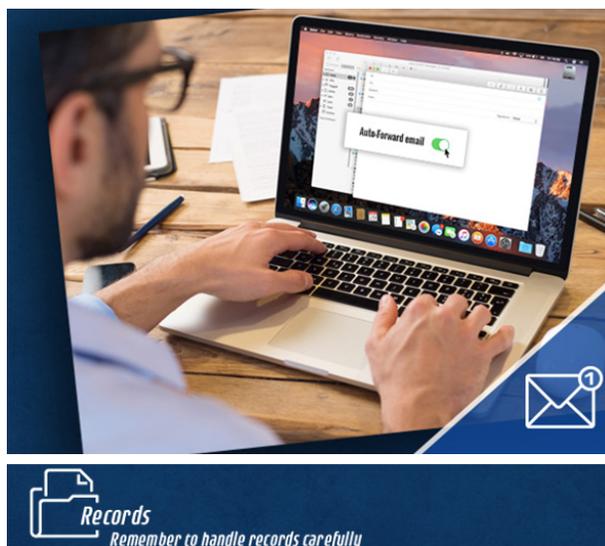
Scenario

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:

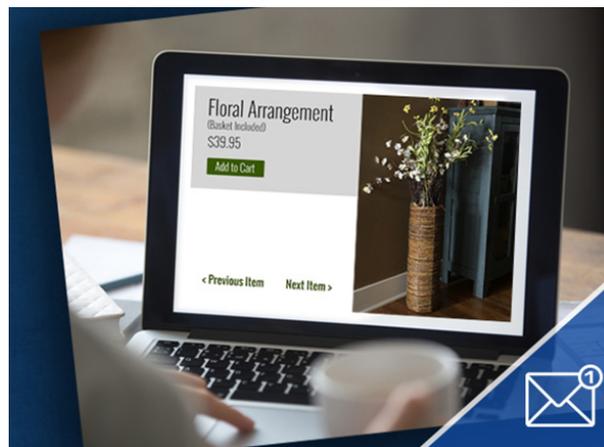
- **Yes** – You won’t get many messages; you just want to stay on top of it.
- **No** – This is an inappropriate personal use of VA equipment.

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.

Non-Organizational Users:

- I WILL NOT disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia by VA without appropriate legal authority. Unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals, and includes criminal penalties.

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.

Rules of Behavior

Organizational Users:

- 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.

Non-Organizational Users:

- I WILL NOT use personally-owned equipment on-site at a VA facility to directly connect to the VA network, or connect remotely to the VA network unless approved prior to use (i.e., approval from VA ISO or Change Management Agent).



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.

Non-Organizational Users:

- I will only use VA-approved solutions, software, or services for connecting non-VA-owned systems to VA's network either remotely or directly.



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.

Non-Organizational Users:

- I will complete any additional role-based security training required based on my role and responsibilities.
- I will sign specific or unique ROBs as required for access or use of specific VA systems or non-VA systems.



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 6: Working Away From VA

6.1 Introduction

This section presents situations that usually occur when working away from VA.

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.

6.2 Encryption of Devices and Equipment

Scenario

Jeff is a contract employee working remotely, and he does not use VA-furnished devices or equipment. He does have access to a few databases containing VA sensitive information.

Is he required to have his equipment and devices encrypted?

Consider the best response:

- **Yes** – All devices and equipment that may be used to access VA sensitive information must be encrypted.
- **No** – Encryption requirements do not apply to contractors who do not use GFE.



The correct answer is **Yes**. Contract employees are able to use non-VA equipment. Encryption is not required because those non-VA government-furnished systems are prevented from storing VA sensitive information locally to the machine by the VA Citrix Access Gateway StoreFront remote access solution.

Rules of Behavior

Organizational Users:

- I will 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)).



6.3 Encryption

Scenario

Kathy is a VA employee who works remotely three days each week. She does not work with VA sensitive information in her job. She uses a VA laptop and a VA flash drive.

Is she required to have her equipment and devices encrypted with [Federal Information Processing Standard \(FIPS\) 140-2 validated encryption](#)?

Consider the best response:

- **Yes** – All VA-furnished devices must be encrypted.
- **No** – Devices only need encryption if they will contain sensitive information.



The correct answer is **Yes**. In Kathy's situation, since she is using GFE issued by VA IT, it has been encrypted before she receives it. Whether she will use sensitive information in her job is not a deciding factor. All VA devices and equipment must be encrypted with FIPS 140-2 encryption. This is true even if you do not use the devices to contain or transmit sensitive information.

Kathy can find out what requirements pertain to her equipment and devices by asking her project supervisor or the ISO assigned to her project.

Rules of Behavior

Organizational Users:

- I will 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.
- I WILL NOT transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption.
- I will 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.
- I WILL NOT 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.



6.4 Working Remotely

Scenario

Jon is a VA employee taking classes for an advanced degree. He sometimes works remotely from the university library. Another student asks Jon to show him how to remotely access a database.

Jon shows Marcus how he logs in to get behind the VA firewall. He does not share his password or share his PIV credential.

Did Jon do anything wrong?

Consider the best response:

- **Yes** – He showed Marcus how to use VA's remote access mechanisms.
- **No** – He didn't show Marcus his password.



The correct answer is **Yes**. While it's good that Jon protected his password and his PIV credential, he violated the ROB because he showed Marcus how to use VA's remote access mechanisms. Always protect information about VA's remote access procedures. VA's remote access mechanisms are considered VA sensitive information and must not be shared with others.

Rules of Behavior

Organizational and Non-Organizational Users:

- I will protect information about remote access mechanisms from unauthorized use and disclosure.

Organizational Users:

- I WILL NOT access non-public VA information technology resources from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.

Non-Organizational Users:

- I WILL NOT access non-public VA information systems from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.



6.5 Permission for Remote Access

Scenario

You need to provide patient documents for a doctor across town. The files are too large to send via email. You talk with your supervisor and get her approval to place the sensitive information on a VA-owned encrypted USB drive. You will immediately and carefully hand-deliver the USB drive to the doctor yourself so that the information doesn't get into the wrong hands.

Does this action comply with the ROB?

Consider the best response:

- **Yes** – As long as you have your supervisor's approval, you can deliver the sensitive information using a USB drive in this situation.
- **No** – You should never use a USB drive to transport VA sensitive information.

The correct answer is **Yes**. This action complies with the ROB because you received approval from your supervisor to deliver the sensitive information using a USB drive.

Rules of Behavior

Organizational Users:

- I will 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)).





6.6 Telework

Scenario

A representative from OI&T requests an appointment to inspect your remote work location. He will also scan your GFE while he visits.

Is this something you should comply with?

Consider the best response:

- **Yes** – It is part of the telework agreement.
- **No** – My work location is secure; it is not necessary to inspect it.

The correct answer is **Yes**. Whether you think your work location is secure or not, an OI&T representative may request to inspect your remote location. Based on the telework agreement, you must agree to the request.

Additional information regarding telework can be found in *VA Handbook 5001/26 Hours of Duty and Leave (Telework)* and in the *VA Telework Training Module for Employees* on the TMS.

Rules of Behavior

Organizational Users:

- I will provide authorized OI&T personnel access to inspect the remote location pursuant to an approved telework agreement that includes access to VA sensitive information.
- I will have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.

Non-Organizational Users:

- I will 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.





6.7 International Travel

Scenario

You have an opportunity to visit family for a month in Australia. You'd like to work a few days so you don't have to take a full month of leave, so you'll need to bring your VA laptop and mobile device.

Should you contact your supervisor to discuss this?

Consider the best response:

- **Yes** – There may be challenges with traveling.
- **No** – You'll be working the same number of hours, just in a different location.



The correct answer is **Yes**. International travel can be risky. That risk increases when you travel with VA GFE. At a minimum, you must get permission from your supervisor or ISO prior to international travel if you plan to bring your GFE. Your supervisor, ISO, local CIO, and Information System Owner must be notified if you plan to take your GFE with you. They will also need to approve your request to access the VA network from a foreign country.

While you travel, take extra precautions and be more aware of your surroundings. When you return, you must contact your supervisor. You may need to provide your GFE to OI&T for inspection.

While you travel, take extra precautions and be more aware of your surroundings. When you return, you must contact your supervisor. Be aware, you may need to provide your GFE to OI&T for inspection.

Rules of Behavior

Organizational Users:

- I will notify my VA supervisor or designee prior to any international travel with GFE mobile device (e.g. laptop, PDA) and upon return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.
- I will 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.
- I will safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel).
- I WILL NOT access VA's internal network from any foreign country designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner.



Non-Organizational Users:

- I WILL NOT access any VA information system from any foreign country unless approved by a VA ISO, local CIO, and Information System Owner.

6.8 Summary

Keep the following in mind when working away from VA:

- Always use encryption products approved by VA to protect sensitive data.
- Never transmit VA sensitive information via wireless technologies unless they have validated encryption.
- Always safeguard VA mobile devices that contain VA information using validated encryption.
- Never access non-public VA information on publicly available devices.
- Never reveal information about VA's remote access mechanisms.
- Use extra caution when handling sensitive information, and obtain approval when working with sensitive information remotely.
- Always contact your supervisor before and after international travel.
- Never access VA's internal network from a foreign country without approval from your VA supervisor and other VA officials.
- Always follow telework agreements including allowing for inspections and providing GFE to be scanned and serviced by VA authorized personnel.



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.

Non-organizational users:

- I will comply with all federal and VA information security, privacy, and records management policies.

The term records has a very broad definition in the [Federal Records Act](#) of 1950. In general, any materials that document the transaction of VA business are potentially records. VA has [designated Records Management Officials](#) who manage federal records across VA administrations and facilities. Federal records must be kept and stored according to requirements of a [records control schedule \(RCS\)](#).



Remember:

- Work with your designated Records Management Official if you are creating, transporting, storing, or disposing of materials that may be records.
- You need to be sure VA sensitive information is protected.
- Be aware that VA business-related email and [text messages](#) may be records and exercise caution before deleting them.
- To increase your knowledge about how to handle records at VA, locate records training on the TMS.

7.7 Recertification for Users of VA-Provided Mobile Phones (iPhones)



Do you have a VA-provided mobile phone (e.g., iPhone)? If **NOT**, you may skip this section.

Here are the actions you must take to protect VA-provided mobile devices:

Secure Use

- Enroll your GFE mobile device in AirWatch before downloading any apps
- Use apps from the VA App Catalog. They have been deemed safe for use with VA sensitive information and for conducting VA business
- Download apps from the Apple App Store **ONLY** if you are not receiving or inputting VA sensitive information
- Never put VA sensitive information in public apps
- Enable and use Wi-Fi for automatic updates
- Never allow access requests

When you accept the Rules of Behavior at the end of this course, you are also accepting that you have received annual refresher training for your VA mobile device.

For any additional information, please review the *Mobile Training: Security of Apps on iOS Devices* course (TMS 3926744).

7.8 More Reminders for Mobile Device Users



If you do **NOT** have a VA-provided mobile device, you may skip this section.

More Reminders

Here are a few more reminders to be sure you are using VA-provided mobile devices securely:



- Treat the personal information of others the same as you would treat your own. Protect it!
- Follow all of the VA ROB and report any suspected or identified incidents to the National Service Desk
- Limit your personal use of the VA-issued device as stated in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology
- Connect to VA securely using an approved Virtual Private Network (VPN), e.g. CAG or AnyConnect

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
- Follow the ROB and best practices for records management and using VA-provided mobile devices
- Recertify to use your VA-provided Apple (iOS) mobile devices



Topic 8: Summary and Rules of Behavior

8.1 Conclusion

Recall privacy and security ROB:

- Whenever you use VA systems and networks
- When you travel
- When you work from a non-VA location
- 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 use your mobile devices and laptop computers
- 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 OMB Circular A-130, Appendix III, 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: SI-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

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. I will protect GFE from theft, loss, destruction, misuse, and emerging threats. SOURCE: AC-17
- Obtain approval prior to using remote access capabilities to connect non-GFE equipment to VA's network while within the VA facility. SOURCE: AC-17
- Notify my VA supervisor or designee prior to any international travel with a GFE mobile device (e.g. laptop, PDA) and upon return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return. SOURCE: AC-17
- Safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel). SOURCE: AC-17
- Provide authorized OI&T personnel access to inspect the remote location pursuant to an approved telework agreement that 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 GFE mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened. SOURCE: AC-19

I Will Not:

- Access non-public VA information technology 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 designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner. 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 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



Appendix B: Department of Veteran Affairs Information Security Rules of Behavior for Non-Organizational Users

1. COVERAGE

Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) for Non-Organizational Users provides the specific responsibilities and expected behavior for non-organizational users of VA systems and VA information as required by 38 U.S.C. § 5723(f)(5), OMB Circular A-130, Appendix I, §§ 4(h) (6-7) and VA Handbook 6500, Managing Information Security Risk: VA Information Security Program.

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 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.

VA information is 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 (e.g., 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 is the responsibility of the recipient.

The VA 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 simply provides the minimum standards with which individual users must comply, and VA facilities and other agency components may issue standards for protection that exceed the ROB. In addition, authorized users are required to go beyond stated rules using due diligence and the highest ethical standards.

2. COMPLIANCE

Non-compliance with the VA ROB for Non-Organizational Users may be cause for suspension or removal of access to VA information or information systems. Such a suspension would not prevent the authorized disclosure of records to an individual; however, it may prevent disclosure through a particular method, e.g., by suspending of access through a VA information system. Depending on the severity of the violation and management discretion, consequences may include restricting access or suspension of access privileges. Theft, conversion, or unauthorized access, disposal, or destruction of Federal property or disclosure of information may result in criminal sanctions.

Accessing, uploading, downloading, changing, circumventing, or deleting of information on VA systems without authorization; modifying VA systems, denying or granting access to VA systems



without authorization; using VA resources for unauthorized purpose on VA systems; or otherwise misusing VA systems or resources is strictly prohibited and may result in criminal sanctions.

The VA ROB for Non-Organizational Users 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**

The VA ROB for Non-Organizational Users must be signed before access is provided to VA information or information systems and annually thereafter by non-organizational users of VA information or information systems. This signature indicates agreement to adhere to the ROB. Refusal to sign the ROB will result in denial of access to VA information or information systems.

The VA ROB for Non-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 Acknowledgement and Acceptance.

4. **INFORMATION SECURITY RULES of BEHAVIOR**

Access and Use of VA Information Systems

I Will:

- Comply with all federal and VA information security, privacy, and records management policies. SOURCE: VA Handbook 6500 Control PM-1
- Have NO 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: VA Handbook 6500 Control AC-8
- Follow established procedures for requesting access to any VA information system and for notifying VA when the access is no longer needed. SOURCE: VA Handbook 6500 Control AC-2
- Only use my access to VA computer systems and/or records for officially authorized purposes. SOURCE: VA Handbook 6500 Control AC-6
- Only use VA-approved solutions, software, or services for connecting non-VA-owned systems to VA's network either remotely or directly. SOURCE: VA Handbook 6500 Control AC-20, AC-17

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data. SOURCE: VA Handbook 6500 Control AC-6
- Use personally-owned equipment on-site at a VA facility to directly connect to the VA network, or connect remotely to the VA network unless approved prior to use (i.e., approval from VA ISO or Change Management Agent). SOURCE: VA Handbook 6500 Control AC-20



Protection of Computing Resources

I Will:

- Protect Government Furnished Equipment (GFE) from theft, loss, destruction, misuse, and threats. SOURCE: VA Handbook 6500 Control AC-17
- Follow VA policies and procedures for handling Federal Government IT equipment and sign for items provided to me for my exclusive use and return them when no longer required for VA activities. SOURCE: VA Handbook 6500 Control CM-8(4)

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee. SOURCE: VA Handbook 6500 Control 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: VA Handbook 6500 Control CM-3

Electronic Data Protection

I Will:

- If authorized to directly connect to a VA system, only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA. SOURCE: VA Handbook 6500 Control SI-3

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: VA Handbook 6500 Control 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: VA Handbook 6500 Control CM-10

Remote Access

I Will:

- Protect information about remote access mechanisms from unauthorized use and disclosure. SOURCE: VA Handbook 6500 Control AC-17

I Will Not:

- Access non-public VA information systems from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library. SOURCE: VA Handbook 6500 Control AC-17
Access any VA information system from any foreign country unless approved



by a VA ISO, local CIO, and Information System Owner. SOURCE: VA Handbook 6500 Control AC-17

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames. SOURCE: VA Handbook 6500 Control AT-3
- Complete any additional role-based security training required based on my role and responsibilities. SOURCE: VA Handbook 6500 Control 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: VA Handbook 6500 Control AU-1
- 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: VA Handbook 6500 Control MA-2
- Permit only those authorized by OI&T to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software. SOURCE: VA Handbook 6500 Control MA-5
- Sign specific or unique ROBs as required for access or use of specific VA systems or non-VA systems. SOURCE: VA Handbook 6500 Control PL-4

Sensitive Information

I Will Not:

- Disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia by VA without appropriate legal authority. Unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals, and includes criminal penalties. SOURCE: VA Handbook 6500 Control IP-1, 38 U.S.C. § 7332

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. SOURCE: VA Handbook 6500 Control IA-5(1)
- Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure. SOURCE: VA Handbook 6500 Control IA-5(h)



I Will Not:

- Store my VA 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. SOURCE: VA Handbook 6500 Control IA-5
- Hardcode credentials into scripts or programs. SOURCE: VA Handbook 6500 Control IA-5(1)(c)
- Divulge a personal username, password, access code, verify code, or other access credential to anyone. SOURCE: VA Handbook 6500 Control AC-17

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) on VA information systems to a VA ISO, local CIO, and Information System Owner immediately upon suspicion. SOURCE: VA Handbook 6500 Control IR-6



5. ACKNOWLEDGEMENT AND ACCEPTANCE

- a. I acknowledge that I have received a copy of the VA Information Security Rules of Behavior for Non-Organizational Users.
- b. I understand, accept, and agree to comply with all terms and conditions of the VA Information Security Rules of Behavior for Non-Organizational Users.

Print or type your full name

Signature Date

Office Phone

Position Title



Appendix C: Glossary

NOTE: If you select a URL or a hyperlink to an Intranet or Internet location from the Resources, you will leave the course. You may have to relaunch the course to return.

A

Active Directory Rights Management Service (RMS) Encryption—VA-approved, FIPS-140-2 certified encryption tool. The tool limits who can see email and Microsoft-based documents. RMS is a form of information rights management used on Microsoft Windows that uses encryption to limit access to items such as Word, Excel, PowerPoint, Outlook, InfoPath, and XPS documents and the operations authorized users can perform on them. The technology prevents the protected content from being decrypted except by specified people or groups, in certain environments, under certain conditions, and for certain periods of time. Specific operations like printing, copying, editing, forwarding, and deleting can be allowed or disallowed by content authors for individual pieces of content. Source: Microsoft and VHA Handbook 1907.01

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Availability—Ensuring timely and reliable access to and use of information. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

B

Breach—The loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing SPI, 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 May or may not be a breach under the HIPAA Privacy and Security Rules, which define “breach” as the unauthorized acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Under these Rules, breach of PHI excludes a. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the covered entity or business associate and does not result in further use or disclosure; b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and c. Any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



C

Citrix Access Gateway (CAG)—Citrix Access Gateway (CAG) is a virtual private network (VPN) that allows remote access to VA internal resources. Access to CAG requires two-factor authentication through required use of a PIV card reader or SafeNet MobilePASS token. Source: VA FSS Bulletin No. 270, VA Remote Access: Citrix Access Gateway (CAG): Two-Factor Authentication Implementation Schedule

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Clean Desk Policy—The organization will provide secure methods of conducting business while maintaining the ability to work effectively. The clean desk policy will present a positive image to our customers, present the opportunity to reduce the use of paper, and aid in accounting for and fortification of sensitive information. Source: 2013 Privacy Program Manual

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Confidentiality—Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Contractors—People who agree to supply VA with goods or services at a certain price. Contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the ROB and complete security awareness and privacy training prior to receiving access to the information systems. Source: Adapted from VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

D

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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



Disclosure—The communication of VA knowledge or facts, in any medium, without proper authority, or in an improper manner. Disclosure is to reveal or share information. 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 6502.1

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

E

Employees—People who work for VA in return for pay. Employees are all individuals who are employed under Title 5 or Title 38, United States Code, as well as individuals whom the Department considers employees, such as volunteers, without compensation employees, and students and other trainees. Source: Adapted from VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Encryption—The process of changing plaintext to ciphertext for the purpose of security or privacy. Encryption hides text in secret code. 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. Public Key Infrastructure (PKI) is an encryption architecture, which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. Source: Adapted from World Wide Web Consortium Glossary and VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

F

Facebook—A web-based collaborative tool used to facilitate collaboration, outreach, communication, and information sharing. Source: Adapted from VA Directive 6515

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Federal Information Processing Standard (FIPS) 140-2—Security Requirements for Cryptographic Modules is a U.S. government computer security standard that outlines requirements for approving cryptographic modules. Source: Adapted from NIST Standards, <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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 NIST SP 800-63-2

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Federal Records Act—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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Flickr—A web-based photo and video host service. Flickr allows users to store, sort, search, and share photos and videos online through social networking sites. Source: Adapted from <http://dictionary.cambridge.org/dictionary/english/flickr>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Freedom of Information Act (FOIA)—A law that gives people the right to see federal government records. FOIA provides that any person has a right of access to federal agency records, except to the extent that such records are protected from release by a FOIA exemption or a special law enforcement record exclusion. It is VA's policy to release information to the fullest extent under the law. Source: Adapted from <https://www.foia.gov/>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

G – N/A

H

Health Information Technology for Economic and Clinical Health Act (HITECH)—Enacted as part of the American Recovery and Reinvestment Act of 2009, HITECH was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. Source: <https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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 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: <http://www.hipaa.com/>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

I

Identity Theft—A fraud committed using the identifying information of another person. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Information Security—A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Instagram—A web-based photo sharing site. Users share images, graphics, photos, and short videos with friends. Source: Adapted from <http://dictionary.cambridge.org/dictionary/english/instagram>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Instant message (IM)—An electronic message sent in real time via the Internet and, therefore, immediately available for display on the recipient's screen. Source: <http://www.dictionary.com/browse/instant-message>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Integrity—Guarding against improper information, modification, or destruction and includes ensuring information non-repudiation and authenticity. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



J – N/A, K – N/A

L

Limited Personal Use—Limited personal use refers to 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 governments, 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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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. 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 800-83 Revision 1 (July 2013) and VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Microsoft Outlook Calendar—Microsoft Outlook Calendar is the calendar and scheduling component of Outlook and is fully integrated with email, contacts, and other features. Source: Adapted from Microsoft

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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 standard requires only the minimum necessary sensitive personal information (SPI) to perform a legitimate business function. Source: Adapted from <https://www.hhs.gov> and VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



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, on-board 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: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

N

Network and Security Operations Center (NSOC)—Responsible for protecting VA information by monitoring, responding to, and reporting cyber threats and vulnerabilities; managing Internet gateways; conducting Enterprise network monitoring; and providing value-added network and security management services as requested. Source: Adapted from https://vaww.portal2.va.gov/sites/infosecurity/nsoc/SitePages/VA_NSOC.aspx

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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.

SOURCE: This definition is based on the Information Security Rules of Behavior for Organizational Users policy (VAIQ #7823189), effective September 15, 2017. It supersedes previous definitions of this term stated in the Organizational Users ROB.

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

O

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. SOURCE: This definition is based on the Information Security Rules of Behavior for Organizational Users policy (VAIQ #7823189), effective September 15, 2017. It supersedes previous definitions of this term stated in the Organizational Users ROB.

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Password Requirements—Passwords must contain at least eight non-blank characters. They must contain characters from 3 of the following 4 categories: English upper case characters, English lower case characters, Base 10 digits, and non-alphanumeric special characters. Six of the characters must not occur more than once in the password. System administrator and service accounts must contain at least 12 non-blank characters and use 3 of the 4 categories as outlined above. When changing a password, four characters must be changed from the old password to the new password. The same password should not be used if it has been used within the past two years. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Penalties—Failure to follow the rules and report incidents, may result in facing penalties, having to pay fines, losing your job (if you are an organizational user), or even facing prison time. Privacy Act penalties include up to \$5,000 in fines and a year in prison per violation. HIPAA violations may result in fines from \$100 to \$1.5 million and jail time. FISMA noncompliance can result in loss of funding and contracts. Unlawful disclosure of medical records and documents or information contained within can result in up to \$5,000 in fines for a first offense and up to \$20,000 for a subsequent offense (38 CFR § 5701, 5702, and 7332). Mishandling records can also result in penalties. The maximum penalty for the willful and unlawful destruction, damage, or alienation of federal records is a \$2,000 fine, 3 years in prison, or both (36 CFR § 1228.102). If you steal, change, or destroy federal property or information, you could face many penalties under various other laws, such as fines of up to \$250,000 and up to 10 years in prison.

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Personal Identity Verification (PIV) card/credential—An ID card that receives, stores, recalls, and sends data securely. The PIV card is an ID card issued by a federal agency that contains a computer chip, which 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.va.gov/pivproject/>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



Personally Identifiable Information (PII)—Any information which can be used to distinguish or trace an individual's identity, such as his or her name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be PII. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Phishing—Efforts to steal personal data. Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means. Source: NIST SP 800-83 Revision 1 (July 2013)

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Privacy—Keeping data away from the view of other people. Privacy is freedom from unauthorized intrusion of Personally Identifiable Information (PII) and an individual's interest in limiting who has access to personal health care information. Source: Partners Healthcare Glossary of Common Terms, Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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 <http://www.justice.gov/opcl/privacyact1974.htm>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Prohibited activities—Using VA-issued devices for inappropriate actions. Prohibited activities include, but are not limited to, uses that cause congestion, delay, or disruption to any system or equipment; use of systems to gain unauthorized access to other systems; the creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings; use for activities that are illegal, inappropriate, or offensive to fellow employees or the public; the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials; the creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, or other illegal or prohibited activities; use for commercial purposes or "for profit" activities or in support of outside employment or business activities, such as consulting for pay, sale or administration of business transactions, or sale of goods or services; engaging in outside fundraising activity,



endorsing any product or service, or engaging in any prohibited partisan activity; participating in lobbying activity without authority; use for posting agency information to external news groups, bulletin boards, or other public forums without authority; use that could generate more than minimal expense to the government; and the unauthorized acquisition, use, reproduction, transmission, or distribution of privacy information, copyrighted, or trademarked property beyond fair use, proprietary data, or export-controlled software or data. Source: Adapted from VA Directive 6001

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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 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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Public Key Infrastructure (PKI) encryption—VA-approved software that is used to hide text in secret code and secure the delivery of electronic services to VA employees, contractors, and business partners. PKI encryption is part of an overall security strategy that combines hardware, software, policies, and administrative procedures to create a framework for transferring data in a secure and confidential manner. PKI encryption is a critical component to safeguard networked information systems and assets and to conduct business securely over public and private telecommunication networks. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Q – N/A

R

Records—(1) In general, the term records (A) includes all recorded information, regardless of form or characteristics, made or received by a federal agency 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 United States Government or because of the informational value of data in them; and (B) does not include library and museum material made or acquired and preserved solely for reference or exhibition purposes; or duplicate copies of records preserved only for convenience. For purposes of paragraph (1), the term “recorded” information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. The Archivist’s determination whether recorded



information, regardless of whether it exists in physical, digital, or electronic form, is a record as defined in subsection (a) shall be binding on all federal agencies. Source: § 3301

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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. A Records Control Schedule is required by statute. All VA records and information must be identified by records series and be listed in the aforementioned Records Control Schedule. Source: Adapted from VA Handbook 6300.1

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Regulatory or program-specific information—Information that VA may not release or may release only in very limited, specified situations. This category of information, which normally would not be released to the public (5 U.S.C. Section 552—the Freedom of Information Act), may include certain critical information about VA's programs, financial information, law enforcement or investigative information, procurement information, and business proprietary information. Source: VA Privacy Service

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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: Adapted from VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Rules of Behavior (ROB)—A set of Department rules that describes the responsibilities and expected behavior of users of VA information systems or VA information. Source: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

S

Sensitive Personal Information (SPI)—The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) 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. NOTE: The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information." Source: Adapted from VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



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 Revision 2 (May 2015)

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Spoofing—Spoofing refers to sending a network packet that appears to come from a source other than its actual source. Source: NIST SP 800-48

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

T

Text messages—The sending of short text messages electronically, especially from one cell phone to another. Source: www.merriam-webster.com

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Twitter—Allows people to stay connected through the exchange of short messages. Twitter is a real-time information network that connects users to the latest stories, ideas, opinions, and news about what they find interesting. Users can find the accounts they find most compelling and follow the conversations. Source: Adapted from Twitter

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



Two-factor authentication—Multifactor Authentication requires the use of two or more 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); or (iii) something you are (e.g., biometric). Source: VA Handbook 6500. Second definition: The process of establishing confidence in the identity of users or information systems through two factors. The two factors are something the user knows and something the user has. Source: Adapted from NIST Special Publication 800-63-2, Electronic Authentication Guideline

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

U – N/A

V

VA Confidentiality Statutes—(Title 38 U.S.C. 5701, 5705, 7332) Statutes requiring VA to keep medical claims, information, and health records private. (1) Title 38 U.S.C. 5701: VA Claims Confidentiality Statute is a statute that states VA must keep claims private. VA Confidentiality Statute 38 U.S.C. 5701 provides for the confidentiality of all VHA patient claimant and dependent information with special protection for names and home addresses. (2) Title 38 U.S.C. 5705: Confidentiality of Medical Quality Assurance Records is a statute that states VA shouldn't disclose medical quality assurance program information without permission. VA Confidentiality Statute 38 U.S.C. 5705 provides for the confidentiality of Healthcare Quality Assurance (QA) records. Records created by VHA as part of a designated medical quality assurance program are confidential and privileged. VHA may only disclose this data in a few, limited situations. (3) Title 38 U.S.C. § 7332: Confidentiality of Certain Medical Records is a statute that states VA must keep health records containing drug abuse, alcohol abuse, HIV, and sickle cell anemia private. VA Confidentiality Statute 38 U.S.C. § 7332 provides for the confidentiality of VA created, individually identifiable drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or sickle cell anemia. This statute prohibits use or disclosure with only a few exceptions. VHA may use the information to treat the VHA patient who is the record subject. VHA must have specific written authorization in order to disclose this information, including for treatment by a non-VA provider. Source: Adapted from www.memphis.va.gov/docs/VHA_Privacy_Trng.pdf

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

VA sensitive information—VA sensitive information/data is all Department information and/or data, on any storage media or in any form or format, which 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 various confidentiality provisions. Source: Adapted from 38 U.S.C. Section 5727 and VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.



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: VA Handbook 6500

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

W

Wi-Fi—A system of accessing the Internet from remote machines, such as laptop computers that have wireless connections. Source: www.dictionary.com

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

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 <http://compnetworking.about.com/cs/wireless/f/whatiswireless.htm>

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

X – N/A

Y

YouTube—The name of a website on which users can post, view, or share videos. Source: Adapted from YouTube (n.d.) and Dictionary.com (accessed May 15, 2017)

Select Alt+<left arrow> on your keyboard to return to your previous place in the main document.

Z – N/A



Appendix D: Privacy and Information Security Resources

NOTE: If you select a URL or a hyperlink to an Intranet or Internet location from the Resources, you will leave the course. You may have to relaunch the course to return.

[Table 1. VA Phone Numbers](#)

[Table 2. VA Web Links](#)

[Table 3. VA TMS Courses](#)

[Table 4. Privacy and Information Security Laws and Regulations](#)

[Table 5. Selected VA Privacy Handbooks and Directives](#)

[Table 6. Additional Selected VA Handbooks and Directives](#)

[Table 7. VA Forms and Memorandums](#)

Table 1. VA Phone Numbers
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
VA National Service Desk (to request computer, network, or access support or to report security incidents to the Network Security Operations Center [NSOC]) (855) 673-4357. Select option 6 for Computer, Network, or Access Support, and then select option 4 for NSOC.
Table 2. VA Web Links
FSS Health Information Security Division (HISD) SharePoint site for Medical Device Protection Program (MDPP) guidance* https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/HISD.aspx
ITWD's role-based training* http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Pages/default.aspx
Locator to identify ISOs* and POs https://vaww.portal2.va.gov/sites/infosecurity/index.aspx
Office of Information Security Portal* https://vaww.portal2.va.gov/sites/infosecurity/index.aspx



Table 2. VA Web Links

<p>PIV Card Project</p> <p>http://www.va.gov/PIVPROJECT/index.asp</p>
<p>Remote access solutions*</p> <p>https://vpnportal.vansoc.va.gov/Default.aspx</p>
<p>Rights Management Service (RMS)*</p> <p>http://vaww.help.portal.va.gov/</p>

* Only accessible on the VA Intranet

Table 3. VA TMS Courses

<p>Available at https://www.tms.va.gov/</p>
<p>TMS ID 10203, Privacy and HIPAA Training</p>
<p>TMS ID 336914, An Introduction to Rights Management Service—RMS</p>
<p>TMS ID 1256927, Getting Started with Public Key Infrastructure</p>
<p>TMS ID 1367006, VA Telework Training Module for Employees</p>
<p>TMS ID 2626967, Social Networking and Security Awareness</p>
<p>TMS ID 3591967, Identity Theft and Prevention</p>
<p>TMS ID 3926744, Mobile Training: Security of Apps on iOS Devices</p>

Table 4. Privacy and Information Security Laws and Regulations

<p>Freedom of Information Act (FOIA)</p> <p>Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions.</p> <p>https://www.foia.gov/</p>
<p>Health Information Technology for Economic and Clinical Health Act (HITECH)</p>



Table 4. Privacy and Information Security Laws and Regulations

Describes when and how hospitals, doctors, and certain others may safely exchange individuals' health information. It also limits the use of personal medical information for marketing purposes and increases fines for unauthorized disclosures of health information.

<https://www.healthit.gov/policy-researchers-implementers/health-it-legislation>

Health Insurance Portability and Accountability Act (HIPAA)

Establishes requirements for protecting privacy of personal health information.

<https://www.hhs.gov/hipaa/index.html/>

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

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>

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.

http://www.dhs.gov/files/programs/gc_1281971047761.shtm

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)

<http://www2.ed.gov/policy/gen/leg/fra.html>



Table 4. Privacy and Information Security Laws and Regulations

United States Code (U.S.C.): Veterans Confidentiality Statutes

Title 38 U.S.C. § 5701: Confidential Nature of Claims

<https://www.gpo.gov/fdsys/pkg/USCODE-2014-title38/html/USCODE-2014-title38-partIV-chap57-subchapl-sec5701.htm>

Information about any claims processed by VA must be kept confidential.

Title 38 U.S.C. § 5705: Confidentiality of Medical Quality Assurance Records

<http://www.gpo.gov/fdsys/pkg/USCODE-2011-title38/pdf/USCODE-2011-title38-partIV-chap57-subchapl-sec5705.pdf>

Information generated during a medical quality assurance program may not be disclosed except when authorized.

Title 38 U.S.C. § 7332: Confidentiality of Certain Medical Records

<http://www.gpo.gov/fdsys/pkg/USCODE-2000-title38/pdf/USCODE-2000-title38-partV-chap73-subchapl-sec7332.pdf>

Health records with respect to an individual's drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or sickle cell anemia are extremely sensitive.

Table 5. Selected VA Privacy Handbooks and Directives

Available at: <https://www.va.gov/vapubs/>

VA Directive 6066, Protected Health Information (PHI)

VA Directive 6300, Records and Information Management

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 Managing Privacy Act System of Records

VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses

VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program and Appendix D, VA National Rules of Behavior

VA Handbook 6500.1, Electronic Media Sanitization

VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information

VA Handbook 6502, VA Enterprise Privacy Program



Table 5. Selected VA Privacy Handbooks and Directives

VA Handbook 6502.1, Privacy Event Tracking
VA Handbook 6502.4, Privacy Act Review
VA Handbook 6512, Secure Wireless Technology
VA Handbook 6609, Mailing of Personally Identifiable and VA Sensitive Information
Available at: https://www.va.gov/vhapublications/index.cfm
VHA Directive 1605, VHA Privacy Program
VHA Handbook 1605.01, Privacy and Release of Information
VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information
VHA Handbook 1173.08, Medical Equipment and Supplies
VHA Handbook 1907.01, Health Information Management and Health Records

Table 6. Additional Selected VA Handbooks and Directives

Available at: https://www.va.gov/vapubs/
VA Directive 0701, Office of Inspector General Hotline Complaint Referrals
VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program
VA Directive 6515, Use of Web-Based Collaboration Technologies
VA Handbook 5011/5, September 22, 2005, Hours of Duty and Leave
VA Handbook 5011/26, August 9, 2013, Hours of Duty and Leave (Telework)
VA Handbook 5021/3, Employee/Management Relations
VA Handbook 5021.6, Employee/Management Relations, Appendix A
VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology
VA Handbook 6500, Appendix F, VA System Security Controls
VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



Table 7. VA Forms and Memorandums

Available at: http://vaww.va.gov/vaforms/
VA Form 0244, Records Transmittal and Receipt
VA Form 0740, New Telework Request Agreement, Aug 2013
VA Form 7468, Request for Disposition of Records
VAIQ 7581492, Use of Personal Email
VAIQ 7633050, Mandatory Use of PIV Card Authentication for VA Information System Access
VAIQ 7714283, Modified VA Information Security Rules of Behavior, August 2016
VAIQ 7772935, Information Security Rules of Behavior for Non-Organizational Users, April 5, 2017
VAIQ 7823189, Updated VA Information Security Rules of Behavior, September 15, 2017