

VA Privacy and Information Security Awareness and Rules of Behavior

Taking Your Time To Protect VA



FY20 Text-Only Course Transcript

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



VA Privacy and Information Security Awareness and Rules of Behavior

Contents

Purpose of this Document	5
Using Hyperlinks Within This Document.....	5
Topic 1: Course Introduction.....	6
1.1 Welcome	6
1.2 Organizational and Non-Organizational Users	6
1.3 Who Must Take This Course?.....	6
1.4 Why Do You Have To Take This Course?	7
1.5 What to Expect?.....	7
1.6 Types of VA Sensitive Information	7
1.7 General Rules of Behavior	9
Topic 2: Accessing VA Information.....	10
2.1 Introduction and Objectives.....	10
2.2 Identification and Authentication	10
2.3 Securing Workstations	10
2.4 Lost PIV Card.....	11
2.5 Non-GFE Network Connections.....	12
2.6 Need to Know and Minimum Access.....	12
2.7 Policy Violation.....	13
2.8 Insider Threats	14
2.9 Insider Threat Awareness	15
2.10 Summary.....	16
Topic 3: Handling VA Information	17
3.1 Introduction and Objectives.....	17
3.2 Handling Paper Documents	17
3.3 Protecting Personally Identifiable Information/Protected Health Information.....	18
3.4 Mishandling Information	18
3.5 Preventing Mismatching	19
3.6 Preventing Identity Theft	20
3.7 Complying with Records Management Requirements	20
3.8 Keeping Records Secure	21
3.9 Summary.....	21
Topic 4: Safeguarding Electronic Information	22



VA Privacy and Information Security Awareness and Rules of Behavior

4.1 Introduction and Objectives.....	22
4.2 Transmitting Data Securely.....	22
4.3 Using External/Removable Media.....	22
4.4 Encrypting Email.....	23
4.5 Recognizing Phishing Attempts.....	24
4.6 Recognizing Social Engineering.....	25
4.7 Recognizing Social Media Safety.....	26
4.8 Summary.....	28
Topic 5: Protecting VA Electronic Resources.....	29
5.1 Introduction and Objectives.....	29
5.2 VA-Issued Devices.....	29
5.3 Software Downloads.....	30
5.4 Theft or Misuse of VA Equipment.....	30
5.5 VA-Issued Mobile Phones Re-certification and ROB.....	31
5.6 Mobile Phone Reminders.....	31
5.7 Summary.....	32
Topic 6: Working Remotely.....	33
6.1 Introduction and Objectives.....	33
6.2 Securely Accessing VA Systems Remotely.....	33
6.3 Using Unsecured Wireless Connections.....	33
6.4 Using VA Systems and Accessing Information While on Travel.....	34
6.5 Using Non-Official Email for VA Purposes.....	35
6.6 Summary.....	36
Topic 7: Reporting Incidents.....	37
7.1 Introduction and Objectives.....	37
7.2 Recognizing a Potential Incident.....	37
7.3 Internet Awareness and Safety.....	37
7.4 Reporting Incidents.....	38
7.5 Identifying Points of Contact.....	39
7.6 Recognizing and Reporting an Incident.....	40
7.7 Summary.....	41
Topic 8: Course Summary and Rules of Behavior.....	42
8.1 Summary.....	42



VA Privacy and Information Security Awareness and Rules of Behavior

8.2 Acknowledge, Accept, and Comply with the ROBs	42
8.3 Completion	43
Appendix A: Department of Veterans Affairs Information Security Rules of Behavior For Organizational Users	44
1. COVERAGE	44
2. COMPLIANCE	44
3. ACKNOWLEDGEMENT	45
4. INFORMATION SECURITY RULES OF BEHAVIOR	45
5. ACKNOWLEDGEMENT AND ACCEPTANCE	51
Appendix B: Department of Veterans Affairs Information Security Rules of Behavior For Non- Organizational Users	52
1. COVERAGE	52
2. COMPLIANCE	53
3. ACKNOWLEDGEMENT	53
4. INFORMATION SECURITY RULES of BEHAVIOR	53
5. ACKNOWLEDGEMENT AND ACCEPTANCE	58
Appendix C: Glossary	59
Appendix D: Privacy and Information Security Resources	79



VA Privacy and Information Security Awareness and Rules of Behavior

Purpose of this Document

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

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

This version of the *VA Privacy and Information Security Awareness and Rules of Behavior Text-Only Course Transcript* is valid for fiscal year (FY) 2020 (i.e., October 2019 through September 2020).

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

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



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 1: Course Introduction

1.1 Welcome

Welcome to the *VA Privacy and Information Security Awareness and Rules of Behavior: Taking Your Time To Protect VA* training course.

1.2 Organizational and Non-Organizational Users

There are two types of [authorized users](#) at VA: [Organizational](#) and [Non-Organizational](#) users. Organizational users are VA [employees](#), [contractors](#), researchers, students, volunteers, and representatives of federal, state, local, or tribal agencies who are authorized to access VA information and information systems but do not represent a Veteran or claimant.

Non-organizational users are users other than 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.

The [Rules of Behavior \(ROB\)](#) provide guidance for organizational and non-organizational users on how to protect [VA sensitive information](#) and safeguard VA systems. You reduce the risk of compromising [privacy](#) and [information security](#) when you follow the ROB.

We need to be aware of risks like [data breaches](#) that result in exposure of Veteran data and loss of trust, and stay diligent in following VA's ROB. Taking the time to put the ROB into practice will enable us to accomplish our day-to-day duties securely.

1.3 Who Must Take This Course?

Both organizational and non-organizational users are required to take this course.

Everyone at VA shares the duty to protect privacy and ensure information security to keep the organization in good standing and to uphold the federal laws. Regardless of the role you play at VA, you may come in contact with VA sensitive information and information systems. Because of this, everyone has a duty to protect privacy and ensure information security, including you!

As with any rule, there can be exceptions. If you are a Veterans Health Administration (VHA) health professions trainee (e.g., student, intern, resident, or fellow), you are not required to complete this course. This requirement is fulfilled by the following:

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

VHA employees and contractors who have access to [Protected Health Information \(PHI\)](#) have an additional requirement to complete the Privacy and HIPAA Training (VA TMS ID: 10203). There may be other role-based training needed as well, located on the TMS.



VA Privacy and Information Security Awareness and Rules of Behavior

1.4 Why Do You Have To Take This Course?

You must take this course every year to stay up to date on how to protect VA sensitive information. The more you become familiar with the right way to access VA information and systems, the more time you and your colleagues will save in not having to correct costly errors or recover sensitive documents.

All authorized users must take this course prior to gaining access to VA information or information systems. To maintain user access, you have to take this course annually.

Depending on your role and the information and systems you have access to as a [privileged user](#), you may be required to complete additional role-based information security and privacy training.

1.5 What to Expect?

During this course, you can expect to gain a better understanding of your roles and responsibilities for protecting VA information. You will also learn how you can assist with [records management](#) and, if applicable, complete your mobile phone recertification. Most importantly, you will explore how the ROBs apply to your day-to-day work from the time you arrive at work to the time you leave. You should take the time to model integrity and protect VA information and resources every day!

Practical, realistic scenarios are presented throughout this course. You will have the opportunity to review the situation, then decide the best action to take to avoid an [incident](#) where privacy and security are put at risk.

For each scenario, you'll receive feedback to help you understand the best action to take as well as the related ROBs that apply to the situation. This will prepare you to acknowledge and accept the ROBs at the end of this course.

1.6 Types of VA Sensitive Information

Federal agencies have over 100 different ways of characterizing sensitive unclassified information. This information is now referred to across the federal government as [Controlled Unclassified Information, or CUI](#).

Sensitive information can be defined as information that is protected against unauthorized disclosure. VA handles this information frequently, like medical [records](#) of Veterans, personal and financial records of our employees, and information related to VA's security.

Types of sensitive information include [sensitive personal information \(SPI\)](#), [personally identifiable information \(PII\)](#), [protected health information \(PHI\)](#), and [regulatory or program-specific information](#). You are responsible for keeping all of these types of sensitive information safe, so take the time to become familiar with them.

The following provides more information on the different types of sensitive information:

- **Controlled Unclassified Information (CUI)** – VA is currently implementing the Controlled Unclassified Information (CUI) Program to fulfill the requirements in Title 32 Code of Federal



VA Privacy and Information Security Awareness and Rules of Behavior

Regulations Part 2002 (32 CFR 2002). The CUI Program will change marking practices and clarify safeguarding and dissemination controls to help you better understand your role in the protection of CUI. For more information regarding the CUI Program, refer to the VA CUI Intranet site. A link to this site can be found in Resources.

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

- **Sensitive Personal Information (SPI)** – 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.

Source: 38 U.S.C. § 5727

- **Personally Identifiable Information (PII)** – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. Examples of PII include but are not limited to: 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.

Source: OMB M-07-16

- **Protected Health Information (PHI)** – Defined by The [Health Insurance Portability and Accountability Act \(HIPAA\) Privacy Rule](#) 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 PHI to define information that is covered by HIPAA, but unlike individually identifiable health information, it may or may not be covered by the [Privacy Act of 1974](#) or Title 38 [confidentiality](#) statutes. In addition, PHI excludes employment records held by VHA in its role as an employer.

Source: 45 CFR § 160.103; VA Directive 6066

- **Regulatory or program-specific information** – Information that VA may not release or may release only in very limited, specific 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 \[FOIA\]](#)), 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

VA is still in the process of implementing the CUI Program and developing specific guidance for it. When it is time for you to transition to CUI practices, you will be notified and trained.



VA Privacy and Information Security Awareness and Rules of Behavior

1.7 General Rules of Behavior

The VA National ROBs are a set of Department rules that outline the responsibilities and expected behaviors of personnel regarding information system usage.

Most ROBs apply to specific situations like accessing VA computer resources or working remotely, but others are more general.

Be sure to read and follow the rules that apply to your user type. They will be presented at the end of the course for you to review and then acknowledge and accept.

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 receive, or in my activities while accessing or using VA information systems.
- I WILL complete mandatory security and privacy awareness training within designated time frames and complete any additional role-based security training required for my role and responsibilities.
- I WILL understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action.
- I WILL sign specific 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.
- I WILL obtain approval from the Office of Public and Intergovernmental Affairs (OPIA) before establishing a VA social media account.

Non-Organizational users:

- I WILL comply with all federal and VA information security, privacy, and records management policies.
- 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 complete mandatory security and privacy awareness training within designated time frames.
- I WILL understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action.
- I WILL sign specific ROBs as required for access or use of specific VA systems or non-VA systems.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 2: Accessing VA Information

2.1 Introduction and Objectives

VA information systems can be accessed from a variety of locations using a variety of methods. You need to know how to access systems securely to maintain the [integrity](#) of the system and the VA information that resides on it. That starts as soon as you arrive at work.

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

- Recognize the steps to protect access to VA information systems
- Identify common [threats](#) that can compromise VA information and systems

2.2 Identification and Authentication

When you are at a VA facility, you should have your [Personal Identity Verification \(PIV\) card](#) on you at all times. You need this card throughout the day to access VA-issued computers, systems, and other areas as designated by your duties. The security certificates on your PIV and your Personal Identification Number, or PIN, authenticate you to use VA systems.

You should never share your PIV, PIN, user name, or any other access codes or passwords you may have. If you must store your passwords electronically, use only approved solutions for storing those passwords using approved encryption standards.

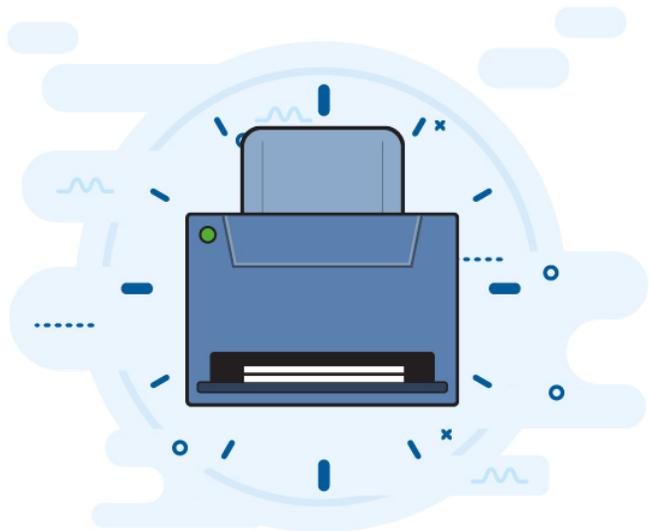
The scenarios in this section will present you with situations that require you to make responsible decisions to protect your accesses to VA network and information systems.

2.3 Securing Workstations

Scenario

You arrive to work in the morning and log in to your computer to check your Microsoft Outlook calendar for upcoming meetings. You realize that you have a meeting in 5 minutes. You must respond to an important email and print out handouts before running to the meeting. You need to step away from your desk to pick up your handouts to make sure they printed correctly, but you'll be right back to finish the email.

What's the first thing you should do to secure your computer before you step away?





VA Privacy and Information Security Awareness and Rules of Behavior

Determine the best answer from the options below:

- A. Everyone in the office knows who you are. You'll be right back, and it shouldn't be a problem if you leave your PIV card in your computer; as long as it's locked it should be fine.
- B. Even if it's just a minute, you should lock your computer and take your PIV card.

Correct Feedback

The correct answer is B.

Never leave PIV cards exposed. Besides providing potential access to VA systems, some PIV cards may provide access to restricted facility locations. Ensure that you only use approved methods to gain access to secured areas.

Additionally, always 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. If you have an office, be sure to lock all doors when you are not there. Also, log out of all information systems at the end of each workday and secure your PIV card.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL log out of all information systems at the end of each workday.
- I WILL log off or lock any VA computer or console leaving my workstation.

2.4 Lost PIV Card

Scenario

You get a text message from a colleague informing you that she has lost her PIV card and she is at the door; she wants you to let her into the building.

What should you do?

Determine the best answer from the options below:

- A. Let her in; it won't hurt this one time.
- B. Tell her that you can contact police security for her or offer to escort her to the PIV Badge Office to report her lost card.

Correct Feedback

The correct answer is B.

Reporting a lost PIV card to your PIV Badge Office prevents any potential unauthorized use and should be done within 24 hours, or the next business day.





VA Privacy and Information Security Awareness and Rules of Behavior

A lost card must be reported to the PIV Badge office, supervisor, and [Information System Security Officer \(ISSO\)](#) to prevent unauthorized use. The longer a card is missing or lost, the more of a threat it becomes for unauthorized entry or access. Report a lost PIV card within 24 hours or the next business day. If you lose your PIV card, contact the [Enterprise Service Desk](#) for a temporary exemption while the card is being located or reproduced.

Make sure you protect your PIV card from unauthorized use. Do not let other people borrow it and do not leave it unattended.

If you find a PIV card, take it to your ISSO or VA police.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users and Non-Organizational Users:

- I WILL protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure.

2.5 Non-GFE Network Connections

The VA network is not limited to just VA-issued equipment. Non-government furnished equipment (non-GFEs) can also access the network with permission. You will need to get approval from your supervisor, the [Contracting Officer's Representative \(COR\)](#), the [Area Manager](#), and [Information Technology and Operations \(ITOPS\)](#). You will also have to use a VA-approved solution to connect.

An example of a VA-approved solution for non-GFE would be Citrix Access Gateway (CAG). Once you have this in place, you can access the VA network with non-GFEs. Be careful not to disclose information about your remote access to unauthorized individuals as this also counts as sensitive information.

One example of non-GFEs on the VA network is contractor laptops. Sometimes, contractors may not be issued VA equipment and must use their corporate laptops for their VA duties.

2.6 Need to Know and Minimum Access

Any time you access VA sensitive information, you must have a need to know. Need to know means that you should have access to only the data, programs, and systems that you need to do your current work. Be careful who you share that information with. There must be a valid, professional, duty-related reason for you to share VA sensitive information with anyone, even with colleagues and coworkers. You cannot disclose any medical diagnoses or treatments without the appropriate authority, legal and otherwise.

You should have the [minimum access](#) necessary to information and systems to perform your current job duties. If you have accesses you no longer need, this can make you an [insider threat](#) because of the potential exposure of PII, invasion of privacy of patients and/or employees, and the possible risk to VA.



VA Privacy and Information Security Awareness and Rules of Behavior

Let your supervisor know when you no longer have a need to access a system or data so you can be removed from the access list and lower your risk of being posed as an insider threat. Most often, your accesses will need to be updated with job changes, retirements, or terminations. Work with your supervisor, Records Management Officer, and [Privacy Officer \(PO\)](#) to take care of any documents or papers you have before changing jobs, retiring, or leaving VA.

2.7 Policy Violation

Scenario

You're wrapping up after a busy day in the office and a coworker comes to you privately. He wants to know if you can look up his sister's medical record; he thinks there may be a serious illness that his sister is not telling him about. He says he's really concerned and wants to know what he can do to support his sister.

Do you help your coworker access his sister's medical records?

Determine the best answer from the options below:

- A. Certainly. You can tell he really cares about his sister, and he wants to help.
- B. Absolutely not! You shouldn't access his sister's medical record. Even though you are able to, it's a privacy violation of the patient, who deserves confidentiality. Also, you have no current need to access it for your work.

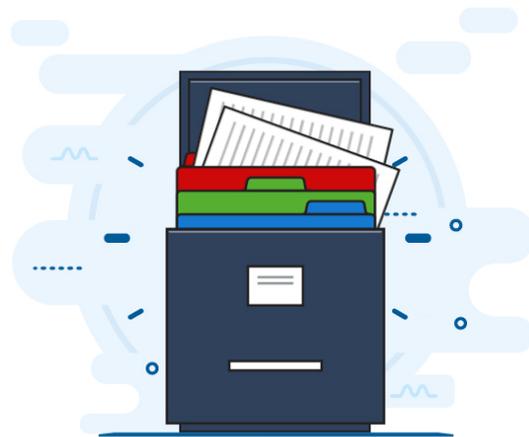
Correct Feedback

The correct answer is B.

You and your coworker do not have a need to know of his sister's medical record. Just because you may be able to access a document, or have a way to access information, does not mean you are allowed to do so. You should access only records for which you have a job-related need-to-know.

Also, according to the ROB, you are not allowed to disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, human immunodeficiency virus (HIV), or sickle cell anemia without appropriate legal authority.

To access any information that you do not have a need to know is a breach of privacy and a violation of HIPAA. ISSOs and POs do weekly audits and can question accesses to determine whether there is a policy violation.





VA Privacy and Information Security Awareness and Rules of Behavior

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL only provide access to VA 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.
- I WILL NOT disclose any information protected by any of VA's privacy statutes or regulations without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, and individuals.

Non-Organizational Users:

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

2.8 Insider Threats

Insider threats are a real concern. Everyone at VA should be on the alert for behaviors and indicators that could be possible precursors to an incident. There are several behaviors that might indicate a growing insider threat such as,

- Inordinate and long-term job dissatisfaction
- Attempts to gain access to information not needed for job performance
- Attempts to exploit system controls or obtain unauthorized access to VA sensitive data
- Unexplained access to financial resources
- Bullying or sexual harassment of fellow employees
- Workplace violence
- Serious violations of policies, procedures, rules, directives, or practices.

The next scenario in this section will present a situation about a potential insider threat.



VA Privacy and Information Security Awareness and Rules of Behavior

2.9 Insider Threat Awareness

Scenario

You are sitting with a coworker at her desktop, training her on new software when you notice a stack of sensitive files on her desk. It seems a bit out of place, especially for the work she does. When she notices you glance over, she quickly puts them away in a drawer.

What should you do?

Determine the best answer from the options below:

- A. Her reaction seems suspicious. Talk to your supervisor to determine if it should be escalated to Human Resources.
- B. Don't worry about it. She probably has them for good reason.



Correct Feedback

The correct answer is A.

You should always be aware and alert to suspicious situations. You know the norms of your team and work area and are suited to noticing any changes or things that are out of place.

There are many behaviors that may be warnings for incidents, including but not limited to:

- Angry or hateful outbursts about coworkers or the organization
- Reports of physical harassing or cyber bullying
- Significant interest in areas outside the scope of work
- Unnecessary downloading or copying of sensitive information.

If you suspect that any of these things are happening in your office, report it to your supervisor, ISSO, PO, or law enforcement. They can handle such things before they become incidents. You can also check the Insider Threat Program website listed in Resources.

The purpose of reporting is not to get people in trouble, but to let the authorities know so they can investigate problems and provide help as appropriate.



VA Privacy and Information Security Awareness and Rules of Behavior

Rules of Behavior

Review the associated rules for your user type below.

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 receive, or in my activities while accessing or using VA information systems.
- I WILL use only VA-approved devices, systems, software, services, and data that I am authorized to use, including complying with any software licensing or copyright restrictions.

Non-Organizational Users:

- 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.

2.10 Summary

Accessing VA data, systems, and networks is a privilege, not a right. It is of utmost importance that you keep it safe and protected, no matter when or where you access it. VA has established policies and guidance, like the ROBs, to help you know how to protect VA, its employees, and its Veterans.

When accessing VA information systems, be sure to do the following:

- Keep your PIV card secure
- Protect your credentials; this includes your user name, password and PIN, access codes, or other access credentials
- Get approval from your supervisor, the COR, the Area Manager, and ITOPS to connect a non-GFE to the VA network
- Access only data and systems you are permitted to use to do your current job
- Be aware of the norms of your office. Report any suspicious behavior to your supervisor, ISSO, PO, or law enforcement to prevent insider threats.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 3: Handling VA Information

3.1 Introduction and Objectives

Handling sensitive information is a matter of trust. Veterans, their families, and your colleagues all depend on you to exercise good judgment when you access or otherwise handle VA sensitive information. Just as you would not want your own personal data treated carelessly, treat the information of others and VA with the same courtesy and in accordance with the ROBs all the time.

This section will provide you with situations and information on properly handling sensitive VA data.

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

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

3.2 Handling Paper Documents

Scenario

You're mopping a spill near a waiting area when you see a folder with papers on a chair. No one is around. You notice that there is PII on the first page, and it seems to include medical records.

How should you handle this?

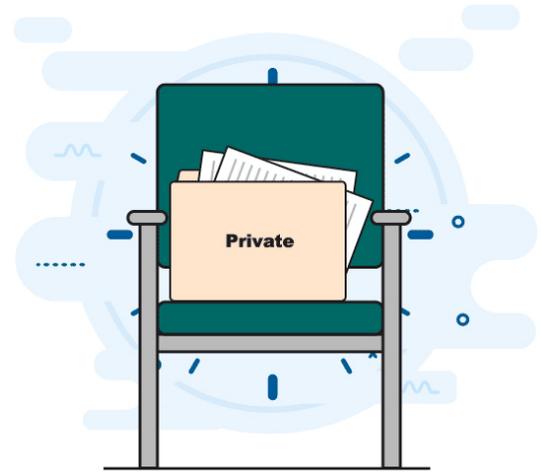
Determine the best answer from the options below:

- A. You leave the folder; someone will come for it.
- B. You toss the folder in the trash; it looks like it's been here a while.
- C. You immediately take the folder to your supervisor and report this as a privacy incident to your ISSO or PO.

Correct Feedback

The correct answer is C.

All sensitive information must be secured. Taking the folder to your supervisor is the right thing to do. You should take the folder to your supervisor, who will secure it and contact your local ISSO or PO.





VA Privacy and Information Security Awareness and Rules of Behavior

Rules of Behavior

Review the associated rules for your user type below.

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).

3.3 Protecting Personally Identifiable Information/Protected Health Information

We deal with many types of sensitive information at VA. Sensitive information can be as simple as names and telephone numbers, or as significant as a medical diagnosis or treatment. It is your duty to protect this information, and only disclose it at the right times to the right people. Treat all VA sensitive information with confidentiality and as if it were your own.

There are special guidelines when handling PII and PHI, including, but not limited to, the following:

- Never remove PII or PHI without express permission from your supervisor and the Area Manager and never use it for unauthorized purposes
- Do not store sensitive information on any Microsoft SharePoint site without approval from your ISSO and PO per guidance from VA Directive and Handbook 6500.
- Never put sensitive information on any non-VA systems or devices unless you are given permission in advance to do so from your supervisor, ISSO, Information [System Owner](#), or Area Manager.

The following scenarios contain situations in which you will determine how to properly avoid mishandling information and mismailing documents.

3.4 Mishandling Information

Scenario

You are transferring to a new work unit and a job you've wanted for a while. As you clear out your desk, you realize you have quite a collection of paper files, some with sensitive information. You will no longer need the information in your new position.

What should you do with the paper files?

Determine the best answer from the options below:

- A. You should contact your PO and Records Management Officer to properly dispose of or store the documentation, since you won't be needing it for the new job.





VA Privacy and Information Security Awareness and Rules of Behavior

- B. Just put it in a box and leave it under your desk. The person who is filling your position can handle it. Besides, they may need it.

Correct Feedback

The correct answer is A.

You should notify the PO and Records Management Officer to let them know that you are transferring to a different job and no longer need the information. If left unsecured, this could be a privacy breach waiting to happen. The optimal situation would be for the PO, Records Management Officer, and you to work together for a solution towards proper storage or destruction. This also applies to retirees and employees leaving VA.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users and Non-Organizational Users:

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

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).

3.5 Preventing Mismatching

Scenario

Just before your lunch break, you're stuffing envelopes to mail to Veterans. When you return from lunch, you realize that you have accidentally placed a Veteran's notice in the wrong envelope.

Should you double-check all the envelopes you have already filled?

Determine the best answer from the options below:

- A. Yes. You want to make sure that you don't mismail any VA sensitive information.
- B. No. It's fine; you are certain that you only made that one error and have corrected it. You need to rush to make sure you send out these notices before you leave for the day.



Correct Feedback

The correct answer is A.

It is very important that you take the time to make sure the names on the envelopes match the names on the documentation inside the envelopes. Also, make sure that only necessary information appears



VA Privacy and Information Security Awareness and Rules of Behavior

on the envelope for mailing purposes. Mismatching is still one of the top ten reported incidents that continue to affect VA. Mismatching carries the potential for [identity theft](#), unauthorized disclosure of PII and PHI, and loss of trust in VA. Take the time to make sure you are correct when preparing mailings with sensitive information.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL recognize that access to certain databases have 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.
- 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.

3.6 Preventing Identity Theft

Identity theft is fraud committed using the identifying information from another person, and it is a very real threat. Being careful when handling PII is one way to combat this threat. Here are some tips for handling PII:

- Never leave paper documents unattended
- Secure paper documents in locked containers when you are not using them
- Verify that information being used is accurate and up to date
- Release only information you are authorized to release to authorized recipients
- Use proper disposal methods when you are done with the sensitive information, whether electronic or paper.

You can always reach to your ISSO or PO for information on proper disposal.

3.7 Complying with Records Management Requirements

Everyone needs to know how to manage records to comply with the [Federal Records Act of 1950](#). As an employee at VA, it is your responsibility to know proper records management. There are [designated VA records management officials](#) who are responsible for federal recordkeeping.

A [records control schedule \(RCS\)](#) describes the requirements needed to maintain and store federal records.



VA Privacy and Information Security Awareness and Rules of Behavior

There are specific ROB that apply to the management of records. They are:

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 receive, or in my activities while accessing or using VA information systems.

Non-Organizational Users:

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

3.8 Keeping Records Secure

Federal records come in a variety of formats. VA business transaction documentation falls under federal records and must be handled as such. You should be familiar with what could be a record. Consult with your supervisor or designated records management official if you are creating, transporting, storing, or disposing of materials that might be records, and also reach to them with any questions about records.

VA records may also include emails and text messages, so be careful about deleting them. Refer to Memorandum VAIQ 7581492 *Proper Use of Email and Other Messaging Services* for more guidance; a link is provided in Resources. Also refer to Resources for Talent Management System courses that are focused on records management.

3.9 Summary

VA sensitive information comes in a variety of formats and you must handle it with care. It is not always easy, but it is necessary to take precautions to protect Veterans, their families, and each other as employees. Pace yourself, and take the extra time necessary to be sure of your work. A little more time spent up front can prevent the extra time that would be needed to correct mistakes that could cause embarrassment to VA and our Veterans.

Follow these best practices when handling VA sensitive information:

- Access information on a need-to-know basis only
- Secure sensitive information when not in use to avoid unauthorized disclosure
- Verify names and addresses when mailing sensitive information to prevent mismailing and potential identity theft
- Understand your responsibilities for records management.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 4: Safeguarding Electronic Information

4.1 Introduction and Objectives

Electronic data has its own set of information security and privacy risks. Take the time to safeguard it. Due to the ease with which it can be exposed, it may be more vulnerable than paper documentation.

In this section, you will find information and scenarios that will require you to consider how to work with electronic information and how to protect it.

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

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

4.2 Transmitting Data Securely

VA sensitive information requires secure transmittal. [Encryption](#) is one way to securely send sensitive data, and it is the preferred method. When you encrypt the email, any attachments will be encrypted as well. Use the encryption software or products that are provided and approved by VA.

Only fax information when there is no other reasonable means to transmit the data. If you need to fax data, make sure it is secure. Follow these guidelines:

- Obtain supervisor approval
- Confirm there is someone who is authorized to retrieve it on the other end
- Double-check the fax number and use the appropriate fax coversheet
- Confirm delivery of the information with the person who is supposed to receive it.

As always, use care and caution when transmitting any sensitive information.

4.3 Using External/Removable Media

Removable and external media devices are very handy for storing and transferring electronic data. However, to prevent the transfer of viruses as well as the theft and misuse of electronic information, the media ports are locked down on most VA-issued equipment, including conference room laptops.

If you need access to media ports on your laptop, you must submit a request to the Enterprise Service Desk. The Enterprise Service Desk will then route the request to the proper authorities for approval.

If you have been issued removable media, like thumb drives or audio recorders, that may have sensitive information on them, do not forget to lock them up when not in use. You are not only responsible for securing the media and devices but also the sensitive information that is on them. Failure to protect devices and the information on them can result in written reprimands up to termination, depending on the nature of the offense.



VA Privacy and Information Security Awareness and Rules of Behavior

Any VA-issued equipment that you will no longer be using, like old flash drives, should be returned to [Office of Information and Technology \(OIT\)](#) personnel. This helps OIT personnel with their inventory security and prevents potential loss or exposure of VA sensitive information. Never just throw away old equipment, even if it is not working.

In the event you find removable media unguarded, take it to the ISSO or VA police and report it as an incident.

4.4 Encrypting Email

Scenario

You need to send some reports to a coworker that contain the names, addresses, and Social Security numbers of a group of patients that are participating in a research study. You write the email and attach the report. What else should you do before sending the email?

Determine the best answer from the options below:

- A. Proceed to send the email. Everything looks good.
- B. Encrypt the email before sending.

Correct Feedback

The correct answer is B.

The ROB requires that you use encryption when sending VA sensitive information through emails, whether it's to Veterans or VA personnel. Sending unencrypted emails can result in identity theft and other security breaches if the PII or PHI goes to an unauthorized individual. Sensitive information should never be included in the subject line of the email because the subject line is not encrypted when using any type of email encryption solution.

Always use [Public Key Infrastructure \(PKI\) encryption](#) guidelines. If you have any issues with encryption, you should contact the Enterprise Service Desk to create a ticket to get the problem fixed. You could also explore other options like faxing the report to your coworker or hand-delivering it if your coworker is local, but only as a last resort. You could also use [Azure \(RMS\)](#) encryption to send the documents.

Don't encrypt emails that don't include sensitive information; this is a violation of the ROB. It's important to note that 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.





VA Privacy and Information Security Awareness and Rules of Behavior

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

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

4.5 Recognizing Phishing Attempts

Scenario

You just received an email that appears to be coming from the Enterprise Service Desk. It states that they need your VA PIV PIN to make some long overdue updates to your VA account. While the email looks official, it is marked “External,” which doesn’t seem right.

How should you respond to the email?

Determine the best answer from the options below:

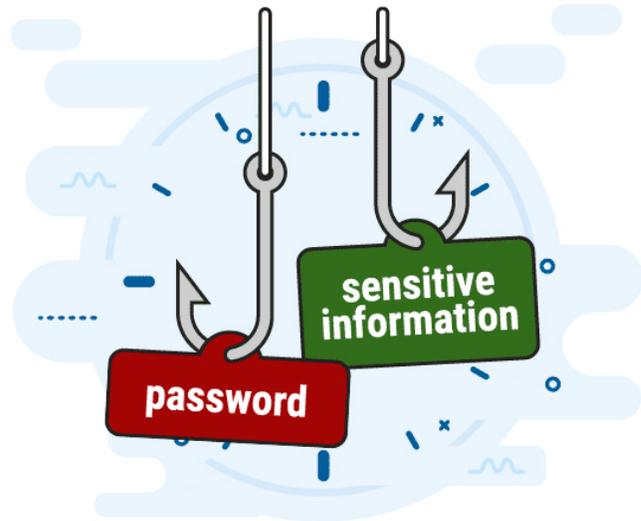
- Do not respond to the email; it doesn’t seem legitimate. The sender’s email doesn’t have @va.gov in the address.
- Nothing seems odd except the email is marked as external. The representative must be using his or her personal computer instead of his or her GFE.

Correct Feedback

The correct answer is A.

The email is not legitimate and the Enterprise Service Desk would not ask for your PIV PIN to access your account. Also, they wouldn’t use a personal computer for VA-related business. It is your responsibility to be aware of such [phishing](#) attempts and protect your information and access to VA systems.

Do not open the email and do not click links or attachments in suspicious emails. Attachments can carry [viruses](#) or malware that will install itself once opened. Create an Enterprise Service Desk ticket, providing as much information as possible. Access the Resources for a link to more guidance on reporting a suspicious email. You can also contact your local ISSO for guidance.





VA Privacy and Information Security Awareness and Rules of Behavior

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and use encryption products approved and provided by VA to protect sensitive data.
- I WILL only provide access to VA 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.

4.6 Recognizing Social Engineering

Scenario

As you wrap up a few urgent tasks, you get a phone call from a person who claims to be a liaison for a local hospital. He begins asking detailed questions about a Veteran's PHI, stating he needs the information for the treatment the Veteran is getting over there. He does have some of the information correct, and seems to be rather confident that you will cooperate, especially when he tells you, "Your supervisor has already been notified about this." But he is avoiding answering several of your questions.



How should you proceed with the person on the phone?

Determine the best answer from the options below:

- A. Tell him you'll call him back. Do not share the details that he requested about the Veteran's sensitive information. He can't identify a clear reason for needing this information. You shouldn't give out any information before verifying the need to know.
- B. He sounds official, and he says he works at the hospital nearby. You think he got your name from your supervisor, especially given his urgent tone.



VA Privacy and Information Security Awareness and Rules of Behavior

Correct Feedback

The correct answer is A.

Sometimes, attackers will attempt to manipulate people using sympathy or implied trust or authority to get information for which they do not have a need to know; this is known as [social engineering](#). Always verify the source asking for that information and confirm with your supervisor. Never send information via email to any external sources you cannot verify. If it is a legitimate request for information, those who are requesting it will be willing to let you verify.

Also, do not give access to databases so that the individual can search the information for themselves, and do not provide any information yourself, no matter how you are pressured. Refer requests for information to the Office of the Inspector General. A link is available in Resources.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- 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.
- I WILL NOT make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to verbal communications, e-mail, text messaging, instant messaging, online chat, social media, and web sites.

4.7 Recognizing Social Media Safety

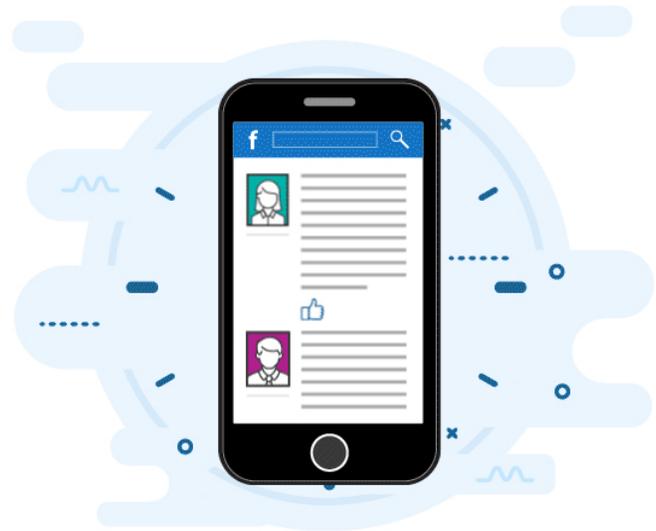
Scenario

You are part of a team that worked with a patient whose story made the local news. A reporter reaches out to you via Facebook and wants to know details on the patient in the story for a Facebook article.

Should you accept or decline this request?

Determine the best answer from the options below:

- A. Accept the reporter's request to provide details for the Facebook article. You'll be famous in town!
- B. Decline giving any information pertaining to the patient. The reporter is asking questions and details that really should not be shared on any social media platform, including Facebook.





VA Privacy and Information Security Awareness and Rules of Behavior

Correct Feedback

The correct answer is B.

While use of social media to promote and collaborate within and outside of VA is highly encouraged, you should safeguard VA information and systems rigorously. For more information, reference VA Directive 6515, *Use of Web-Based Collaboration Technologies*.

The ROBs require you to protect information about VA regardless of the medium it is in. Never post sensitive information on social media accounts, private or VA-related. If you are contacted by a reporter, whether via social media, phone, or email, you must obtain approval to speak about VA information. Do not give out information unless you are authorized to do so.

While certain social media platforms are used to promote and collaborate for VA business, keep in mind that accessing personal social media on government equipment during work hours is a violation of VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*.

You can protect your identity on your own devices by using strong [passwords](#) for sites you visit often. Use numbers, letters, special characters, or a phrase known only to you. Also, keep your social media identity limited. Never include detailed personal information on any social media website.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL, if content I publish on blogs, wikis or any other form of user-generated media might reasonably be perceived as the position of VA, publish a disclaimer that the views are my own and do not represent VA.
- I WILL only disseminate VA information to the public via e-mail when authorized to do so and in the performance of my duties.

Organizational and Non-Organizational Users:

- I WILL limit the personal use of social media/networking sites in accordance with VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology.
- I WILL use web-based collaboration and social media tools in accordance with VA Directive 6515, Use of Web-Based Collaboration Technologies.
- I WILL NOT, in my capacity as a VA representative, comment or provide information on any matter about which I do not have actual, up-to-date knowledge.



VA Privacy and Information Security Awareness and Rules of Behavior

4.8 Summary

Electronic data comes with its own unique challenges in information security and privacy risks, but there are ways to reduce the risk of a data leak or a potential privacy breach. Some best practices for safeguarding electronic information include:

- Transmit sensitive data securely over proper channels
- Encrypt VA sensitive information, including PII and PHI
- Be watchful for social engineering and phishing attempts and report them accordingly
- Exercise caution on social media platforms and never post VA information that could expose a Veteran's information.

Carefully consider each situation as it comes to make the best decision to protect the sensitive information entrusted to you. A well thought-out decision is worth the time to avoid the potential consequences that could result from a hasty decision.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 5: Protecting VA Electronic Resources

5.1 Introduction and Objectives

Just like safeguarding VA sensitive information, it is your responsibility to track, protect, and care for any VA electronic devices that are issued to you. You must also protect whatever information may be stored or processed on these devices. Making sure these devices are up to date and secure is never a waste of time.

In this section, you will find situations that deal with proper use and maintenance of VA devices and equipment and information regarding best practices and recertification for users of VA-provided Apple (iOS) [mobile devices](#).

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

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

5.2 VA-Issued Devices

VA relies on you to be diligent in protecting any resources issued to you. You are the first line of defense against things like theft or loss of VA-issued equipment. If you lose a VA device, you also lose the information that is stored on it. That can cause a breach of privacy or exposure of sensitive information, even with the VA security controls and device encryption provided. Protect these resources like you would your own phone, laptop, or tablet.

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

- If you need repair or maintenance for your VA-issued equipment, use only those authorized by OIT to repair your equipment.
- If you experience theft or loss of VA-issued devices, report it as soon as it is discovered to VA police, the Enterprise Service Desk, and the local ISSO. If you find VA equipment unattended, take it to the ISSO or VA police.

If you leave VA, you must work with your supervisor to return all VA devices and equipment and outprocess. Remember that you are under security constraints not to divulge any information you had access to during your time with VA.

In this section, you will find information and situations that relate to proper use and protection of VA-issued devices and equipment.



VA Privacy and Information Security Awareness and Rules of Behavior

5.3 Software Downloads

While downloading software may seem harmless, it is not allowed on VA-issued devices. Only VA-approved software, in compliance with software licensing and copyright restrictions, can be installed on VA-issued devices. If you find yourself needing specific software to do your work, you should discuss it with your supervisor and submit a request to the Enterprise Service Desk. The Enterprise Service Desk will then route the request to the proper authority. You are not allowed to download software from the internet to your VA-owned systems unless you have been authorized to do so.

This guidance also includes apps for any VA-issued mobile devices. You can download apps from the Apple App Store ONLY if you are not receiving or inputting VA sensitive information. These are apps that can be used for VA business but do not contain any VA sensitive information, nor do they connect to the VA network (e.g., hotel, airline, and weather apps).

5.4 Theft or Misuse of VA Equipment

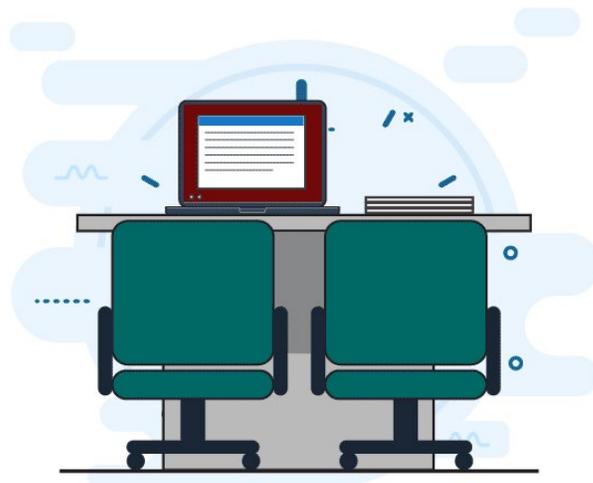
Scenario

You're presenting at an industry conference in a hotel business center. At the lunch break, you decide to leave your laptop in the conference room and close the door; unfortunately, it doesn't have a lock.

Is this good enough to secure your VA-issued laptop while you are at lunch?

Determine the best answer from the options below:

- A. No. You should take it with you or secure it in a locked room.
- B. Yes. You're only going to be gone a few minutes, and there is hotel staff nearby.



Correct Feedback

The correct answer is A.

You are responsible to secure the VA devices that are issued to you. Always keep your laptop and mobile devices secure, and never leave them exposed, even for a moment. In the event of theft, remember to report any missing or stolen VA equipment as soon as it is discovered to the VA police, the Enterprise Service Desk, and the local ISSO. If you find VA equipment unguarded, take it to the ISSO or VA police.

Rules of Behavior

Review the associated rules for your user type below.



VA Privacy and Information Security Awareness and Rules of Behavior

Organizational Users:

- I WILL keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information, regardless of work location. I will protect GFE from theft, loss, destruction, misuse, and emerging threats.
- I WILL safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using Federal Information Processing Standard (FIPS) 140-3 validated encryption (or its successor) unless it is not technically possible.
- I WILL secure mobile devices (e.g., laptops, tablets, smartphones) and portable storage devices (e.g., compact discs (CD), digital video discs (DVD), universal serial bus (USB) flash drives).

Non-Organizational Users:

- I WILL protect Government Furnished Equipment (GFE) from theft, loss, destruction, misuse, and threats.

5.5 VA-Issued Mobile Phones Re-certification and ROB

If you have been issued a VA mobile device, like an iPhone or tablet, you must retake the mobile phone certification every year as well. Taking this course will meet your annual requirement for mobile device certification.

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

- Enroll GFE mobile devices in [Workspace One Hub](#), formally known as [AirWatch®](#), before downloading any VA-approved apps.
- Use apps from the VA App Catalog. They have been deemed safe for use with VA sensitive information and for conducting VA business.
- Use only VA-approved apps for conducting VA business. Go to the Resources section for a link to view the approved apps list.
- Enable and use [Wi-Fi](#) for automatic updates.
- Never allow access requests.

5.6 Mobile Phone Reminders

If you have a VA-issued mobile device, such as a phone, iPad, or tablet, take a moment to review the following reminders:

- Follow all VA ROBs as agreed to and report any suspected or actual incidents to the Enterprise Service Desk and ISSO.
- Treat the personal information of others the same as you would treat your own.



VA Privacy and Information Security Awareness and Rules of Behavior

- Limit your personal use of the device(s) as stated in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.

Tablets and mobile phones have become more prevalent in recent years. The two greatest conveniences of mobile devices, size and mobility, are also their greatest weaknesses and can lead to theft, loss, or unauthorized use. Be sure you are familiar with the best practices and security guidelines, and complete the annual recertification as required.

5.7 Summary

You must protect VA-issued devices and resources, especially those that contain VA sensitive information. Follow these guidelines:

- Be diligent in protecting any devices and resources issued to you.
- Download only authorized software and apps to VA-issued electronic devices.
- Always protect laptops, tablets, and mobile phones from loss, theft, and unauthorized access.
- Annually recertify your knowledge about how to use and protect your VA-issued mobile device.

Report loss, theft, or any other incidents to the VA police, the Enterprise Service Desk, and to the local ISSO.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 6: Working Remotely

6.1 Introduction and Objectives

There are many VA employees who do not physically work in a VA facility. Remote work has its own set of unique challenges when safeguarding and protecting VA information, systems, and equipment. Review VA guidelines concerning [remote access](#) and report any suspicious events to help minimize risks. Diligence is necessary at all times when working remotely.

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

- Identify proper procedures for securely accessing VA information and systems remotely
- Recognize the requirements for protecting and accessing VA information while on travel.

6.2 Securely Accessing VA Systems Remotely

Prior to anyone starting a telework schedule, there should be a conversation with the supervisor and/or Area Manager to outline rules for transmitting sensitive information, setting up the physical work location, handling records, and destroying sensitive information. Putting a secure procedure in place for working remotely will ensure that the employee is aware of the requirements before starting to telework.

Secure access begins with having the permissions to get into the VA network using the [Citrix Access Gateway \(CAG\)](#), [AnyConnect](#), or the [Remote Enterprise Security Compliance Update Environment \(RESCUE\)](#). These access methods require [two-factor authentication](#) through use of a PIV card reader or [SafeNet MobilePASS token](#). From there, you can securely connect to the VA network.

Additionally, whether at home or at another remote work location, make sure to:

- Protect your log-in credentials
- Obtain approval from your supervisor and Area Manager to securely access VA networks and systems
- Obtain approval from your supervisor to properly handle records and sensitive information remotely.

The situations and information presented in this section will help you understand the policies and procedures to securely access VA systems and information from remote locations.

6.3 Using Unsecured Wireless Connections

While unsecured [wireless networks](#) may be convenient for checking personal email or [social media](#) while you are on personal time, this should be done only on your personal devices.

It is not appropriate to use an unsecured wireless connection to conduct VA business. Any guest wireless network at a VA facility should not be used for VA business. You need to go through the proper process to connect to the VA network to fulfill your duty to protect VA sensitive information. The



VA Privacy and Information Security Awareness and Rules of Behavior

VA network has all the encryption and data protection services required to securely handle VA information and prevent unauthorized disclosures.

You are prohibited from setting up any servers or wireless access points on the VA network unless you are expressly approved to do so.

6.4 Using VA Systems and Accessing Information While on Travel

Scenario

You are preparing to leave on business travel. It also happens to be a place you have personally wanted to visit for some time. You have planned to extend your time there by a few days on personal time. You got the proper permissions via email from your supervisor about traveling with your VA-issued equipment for the business travel.

Which of the following is the best course of action concerning your VA-issued equipment during the days you'll be on personal travel?

Determine the best answer from the options below:

- A. I can use my VA-issued equipment only on the business portion of my trip, not my personal time. I need to put my VA laptop and iPhone in my carry-on bag, and I'll bring my personal laptop and phone too.
- B. I only need my VA-issued equipment; I can use it to check email or book tourist events during the personal travel. I'll put the Facebook and Instagram apps on my VA-issued iPhone so I can post pictures of my trip; I'll just remove them after I get back.

Correct Feedback

The correct answer is A.

It is expected that you would take your laptop and other VA-issued equipment on business travel. However, you must initiate the request to take your VA equipment on personal travel via your supervisor. There are no specific forms to fill out, but there are special permissions to acquire if you are traveling domestically. Check with your supervisor for the details. Either way, you should not use your VA equipment while on personal travel.

You should secure any VA devices while traveling, and never put them into checked luggage on travel. Place them in your carry-on and keep them with you at all times.

Be sure to contact your VA supervisor, ISSO, and Area Manager if you plan to travel outside the U.S. and if you expect to have a need to access VA networks while traveling. If you are approved, exercise heightened awareness in protecting and securing your devices and equipment when traveling outside





VA Privacy and Information Security Awareness and Rules of Behavior

the country. If you are traveling to a non-NATO country, you are not allowed to use your VA equipment at all. Be sure to review VHA Directive 1400.6 for detailed guidance on foreign travel.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL NOT access VA's internal network from any foreign country designated as posing a significant threat unless approved by my VA supervisor, ISSO, local AM, and Information System Owner. This prohibition does not affect access to VA external web applications.
- I WILL notify my VA supervisor or designee prior to and upon return from any international travel with a GFE mobile device (e.g. laptop, smartphone) and comply with any security measures, including using a specifically configured device issued for international travel and/or surrendering the device for inspection or reimaging.
- 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.

Non-Organizational Users:

- I WILL NOT access VA's internal network from any foreign country designated as a security risk unless approved by my supervisor, COR, ISSO, local AM, and Information System Owner. This prohibition does not affect access to VA external web applications.
- I WILL NOT access any VA information system from any foreign country unless approved by a VA ISSO, local AM, and Information System Owner.
- I WILL notify my supervisor, COR, ISSO, and local Area Manager (AM), or designee prior to any international travel with a VA mobile device (laptop, PDA) so that appropriate actions can be taken prior to my departure and upon my 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 mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

6.5 Using Non-Official Email for VA Purposes

You should always use your official VA email account for VA business transactions because these types of communications can be considered records. This is especially important since VA email accounts have all the safeguards necessary to protect any sensitive information being transmitted, and it allows for backup copies of emails to be made. Do not auto-forward your VA email to any outside accounts such as Gmail or Yahoo.



VA Privacy and Information Security Awareness and Rules of Behavior

Contractors may be allowed to use their corporate email accounts if they do not have access to a VA email account and the encryption and security requirements are met.

Do not email sensitive information to your personal account or other non-official account when working remotely. If for some reason you cannot use your official VA email account, ensure proper recordkeeping by doing one of the following:

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

6.6 Summary

Protecting VA systems, equipment, and information while working remotely has unique challenges, but following these guidelines and taking the time to properly and securely access the VA network can help minimize risks of security incidents and privacy breaches.

Be sure to:

- Get permission to remotely access the VA network
- Follow approved procedures to securely connect to the VA network
- Take appropriate precautions when on business and international travel
- Use official VA email for VA business whenever possible.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 7: Reporting Incidents

7.1 Introduction and Objectives

If you see something suspicious or what appears to be an incident, you must report it. Incident reporting helps lower the risks of violations and threats. Timely reporting can help minimize the potential consequences of an incident. Make sure you know who to contact if you suspect that there is or will be an incident.

In this section, you will get an overview of what an incident is and you will have the chance to review situations that could lead to or be an incident. You will also get the chance to review the reporting process.

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

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

7.2 Recognizing a Potential Incident

An event that threatens to expose or compromise the [integrity](#), [confidentiality](#), and [availability](#) of information and the system it resides in is called an [incident](#). These types of events can damage information security and privacy and may affect Veterans, VA, and you as an employee. An example of an incident would be emailing sensitive information to the wrong contact.

7.3 Internet Awareness and Safety

VA uses data protection software to provide anti-spyware, virus protection, and firewall/intrusion detection on VA-issued computers and technology. These programs run in the background and are updated as needed by OIT to make sure VA resources are protected.

Normally, the data protection software that VA installs on your machine will handle the threats and let you know if it finds anything unsafe. However, threats are evolving continuously, and not every cyberattack can be blocked.

One of the biggest threats comes from unsafe website browsing. While conducting work-related research, you may come across websites that look legitimate but may actually set you up for a cyberattack. Here are a few best practices to determine if a website is safe or not.

- Take a close look at the URL. There are indicators about the location and security of the information you are accessing. Check for typo-squatting, where attackers create website URLs that commonly have misspellings of legitimate websites (e.g., amazan.com instead of amazon.com). If in doubt, contact your ISSO and report any suspected incidents.
- Don't assume that because it has HTTPS in the URL it is a safe site. This is merely an indication that the site uses encryption for the internet/network traffic to and from the



VA Privacy and Information Security Awareness and Rules of Behavior

website. Cyberattackers can use sites with SSL encryption to mimic legitimate sites. If in doubt, contact your ISSO and report any suspected incidents.

- Beware of ransomware. When a ransomware attack occurs, you become unable to access your data, and a pop-up indicating encryption of your data appears. Typically, payment will be demanded to release the data back to you. A phone number may be given to process that payment to fix the issue. Call your ISSO, the Enterprise Service Desk, and VA police immediately if this occurs.

If in doubt, contact your ISSO to report any suspected incidents.

7.4 Reporting Incidents

The ROBs require you to report suspected or actual information security incidents immediately. You need to get in touch with your ISSO or PO and tell them exactly what you saw. It's always better to be safe than sorry and report any suspected incidents, even if it ends up not being an incident after all. Timely reporting can prevent an incident from reaching more people and creating additional damage.

Unintentional incidents are handled differently than intentional incidents. If an incident is deemed to be intentional, the consequences are more severe than if the incident is accidental or unintentional.

There are serious consequences for causing incidents. These can include:

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

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

- Fines of up to \$250,000
- Prison for up to 10 years

Other penalties:

- Penalties for mishandling records: 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.
- Penalties for violating the Privacy Act: You can face up to \$5,000 in fines and a year in prison.
- Penalties for HIPAA violations: You can face fines from \$100 to \$1.5 million and potential jail time.



VA Privacy and Information Security Awareness and Rules of Behavior

More penalties may apply for violating laws protecting PHI.nces for causing incidents. These can include:

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

More penalties may apply for violating laws protecting PHI.

7.5 Identifying Points of Contact

If you notice anything out of the ordinary that you suspect is an incident, you need to report it immediately.

The first step is to note the details.

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

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

- Employees should report suspected or identified incidents to their supervisor, local Area Manager, ISSO, or PO immediately. If you do not know the name of your Area Manager, ISSO, or PO, you can check the locator link provided in the Resources section. If you work in VHA, you can also report incidents to your Administrator of the Day (AOD) and the Enterprise Service Desk.
- Contractors should report every incident to their ISSO or PO as well as to their COR and Project Manager. All suspected or identified incidents must be reported immediately.



VA Privacy and Information Security Awareness and Rules of Behavior

7.6 Recognizing and Reporting an Incident

Scenario

You are scrolling through your Instagram newsfeed one Saturday when you see that a coworker you follow posted sensitive information about a Veteran in his care. It seems like the post was meant in good faith, but sensitive information was still exposed.

How should you handle this unauthorized disclosure on Instagram?

Determine the best answer from the options below:

- A. This post has sensitive information about that Veteran's health, perhaps unintentionally. You should report this post to your supervisor and the ISSO as well as the PO.
- B. Your coworker seemed to have good intentions; after all he's posting this to raise awareness for that illness. When you see him at work on Monday, you'll tell him to take the post down.



Correct Feedback

The correct answer is A.

You recognized an incident, and you should report it. Never post sensitive information about Veterans or employees or anyone on any social media. While the post may have been made with no intended malice, it opened the possibility for identity theft, embarrassment for the Veteran, and loss of trust in VA. It also was a policy violation in which privacy was compromised, so reaching out to your supervisor, ISSO, and/or PO is definitely a right step.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL report suspected or identified information security incidents including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor, Information System Security Officer (ISSO) or designee immediately upon suspicion.
- I WILL NOT make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to verbal communications, e-mail, text messaging, instant messaging, online chat, social media, and web sites.



VA Privacy and Information Security Awareness and Rules of Behavior

- I WILL NOT post information protected by the Privacy Act of 1974, 38 USC 5701, 5705, or 7332, the Health Insurance Portability and Accountability Act (HIPAA) Rules, or VA policy on any non-VA websites, without legal authority and prior approval by an authorized official.

Non-Organizational Users:

- I WILL report suspected or identified information security incidents, including unauthorized disclosures of VA information or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) on VA information systems to a VA ISSO, local Area Manager (AM), and Information System Owner immediately upon suspicion.

Organizational and Non-Organizational Users:

- I WILL ensure that my use of social media to conduct VA business complies with law, guidance, and VA policy.
- I WILL use my best judgment when interacting on social media about matters related to VA's mission.
- I WILL only post and use content in accordance with applicable ethics, intellectual property, records, and privacy laws, regulations, and policies.

7.7 Summary

Everyone is responsible for reporting any suspicious activity or possible incidents. You know what normal behavior in your work area is, and VA relies on you to be aware of what is going on around you at all times. Make sure that you know the following:

- How to recognize an incident
- How to report the incident
- Whom you must call to report suspected incidents.

You may be able to prevent a large-scale problem if you report any suspected incidents immediately rather than waiting.



VA Privacy and Information Security Awareness and Rules of Behavior

Topic 8: Course Summary and Rules of Behavior

8.1 Summary

It is everyone's responsibility to protect privacy and be diligent about information security. Everyone has the potential to encounter sensitive information while working at VA.

The ROBs are the minimum compliance standard for all VA personnel in all locations. To stay in compliance, you must follow the ROBs. In the event you have access to significant systems or information, you may be required to sign additional ROBs dealing specifically with those systems or information. You will be required to comply with those ROBs as well.

8.2 Acknowledge, Accept, and Comply with the ROBs

When you work for VA, you may encounter VA sensitive information. This means you must accept responsibility for protecting privacy and ensuring information security. The ROBs 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.

A few new rules have been added, so please read through these carefully. Once you are ready, select your user type to acknowledge and accept the ROBs. Read all the ROBs closely. By acknowledging and accepting the ROBs, you are agreeing to uphold all the behaviors stated in the rules. Many, but not all, of the ROBs have been explained in this course.

To complete this training, you must review, initial each page, and sign and date the appropriate ROBs for your user type.

Remember, there are two versions of the ROBs, one for organizational users and one for non-organizational users. The following provides the descriptions for each:

- **Organizational users** are VA employees, contractors, researchers, students, volunteers, and representatives of federal, state, local, or tribal agencies who are authorized to access VA information and information systems but do not represent a Veteran or claimant. This version of the ROB is available in Appendix A.
- **Non-Organizational users** are users other than 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. This version of the ROB is available in Appendix B.

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



VA Privacy and Information Security Awareness and Rules of Behavior

8.3 Completion

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



VA Privacy and Information Security Awareness and Rules of Behavior

Appendix A: Department of Veterans Affairs Information Security Rules of Behavior For Organizational Users

1. COVERAGE

- a. This Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) identifies the specific responsibilities and expected behavior for organizational users of VA systems and VA information and information systems as required by OMB Circular A-130, Appendix I, paragraph 4h (6-7) and VA Directive 6500, *VA Cybersecurity Program*.
- b. *Organizational users* are VA employees, contractors, researchers, students, volunteers, and representatives of Federal, state, local or tribal agencies who are authorized to access VA information and information systems but do not represent a Veteran or claimant.
- c. *Non-organizational users* are users other than 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. The rules of behavior for Non-Organizational Users are identified in the Department of Veterans Affairs Information Security Rules of Behavior for Non-Organizational Users.
- d. The ROB provides the minimum requirements with which users -of VA information and information systems must comply and does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to certain information or information systems. When appropriate, users may exceed these minimum requirements to protect VA information and information systems by exercising due diligence and ethical standards.

2. COMPLIANCE

- a. Non-compliance with the 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 access, upload, download, change, circumvention, or deletion of information on VA systems; unauthorized modification VA systems, denying or granting access to VA systems; unauthorized use on VA systems; or otherwise misusing VA systems or resources is strictly prohibited.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

- c. The 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. The ROB must be signed before access is provided to a new user of VA information and information systems. Thereafter, the VA ROB must be signed annually by all users of VA information and information systems. This signature indicates agreement to comply with the ROB, and refusal to sign VA Information Security ROB will result in denied access to VA information and information systems. 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, state, local, and tribal 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.
- Have NO expectation of privacy in any records that I create or receive, or in my activities while accessing or using VA information systems.
- Use only VA-approved devices, systems, software, services, and data that I am authorized to use, including complying with any software licensing or copyright restrictions.
- 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.
- Only use my access to VA information and information systems for officially authorized and assigned duties.
- Log out of all information systems at the end of each workday.
- Log off or lock any VA computer or console leaving my workstation.
- Only use other Federal government information systems as expressly authorized by the terms of those systems; personal use is prohibited.
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive information.
- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.
- Have a VA network connection and a non-VA network connection, such as a modem or phone line or wireless network card, physically connected to any device at the same time unless the dual connection is explicitly authorized.
- 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 Area Manager (AM) or designee, and approved by my Information System Security Officer (ISSO).

Protection of VA-Issued Devices

I Will:

- Secure mobile devices (e.g., laptops, tablets, smartphones) and portable storage devices (e.g., compact discs (CD), digital video discs (DVD), universal serial bus (USB) flash drives).

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee.
- Attempt to override, circumvent, alter or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff.

Data Protection

I Will:

- Only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA.
- Safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using FIPS 140-3 validated encryption (or its successor) unless it is not technically possible.
- Only use VA-owned or approved storage devices encrypted with FIPS 140-3 (or its successor) validated encryption, consistent with VA's approved configuration and security control requirements to perform VA work.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

- Use VA e-mail in the performance of my duties when issued a VA email account.
- Only use non-VA email when use of a non-VA email account is unavoidable.
- Only disseminate VA information to the public via e-mail when authorized to do so and in the performance of my duties.

I Will Not:

- Transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-3 (or its successor) validated encryption.
- Auto-forward e-mail messages to addresses outside the VA network.
- Download software from the Internet, or other public available sources, offered as free trials, shareware, or other unlicensed software to a VA-owned system.
- Disable or degrade software programs used by VA that install security software updates on computer equipment used to connect to VA information systems, or used to create, store or use VA information.

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.
- Obtain approval prior to using remote access capabilities to connect non-GFE devices to VA's network.
- Notify my VA supervisor or designee prior to and upon return from any international travel with a GFE mobile device (e.g. laptop, smartphone) and comply with any security measures, including using a specifically configured device issued for international travel and/or surrendering the device for inspection or reimaging.
- Safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel).
- Provide authorized OIT personnel access to inspect the remote location pursuant to an approved telework agreement that includes access to VA sensitive information.
- Protect information about remote access mechanisms from unauthorized use and disclosure.
- 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.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

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.
- Access VA's internal network from any foreign country designated as posing a significant threat unless approved by my VA supervisor, ISSO, local AM, and Information System Owner. This prohibition does not affect access to VA external web applications.

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames and complete any additional role-based security training required for my role and responsibilities.
- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems and take appropriate action.
- Have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.
- Permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.
- Sign specific 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.

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).
- Only provide access to VA 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.
- 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.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

- 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)).
- 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.
- Transmit VA sensitive information via fax only when no other reasonable means exist, and when either someone is at the receiving machine to receive the transmission or the receiving machine is in a secure location.
- Encrypt email, including attachments, that contain VA sensitive information. I will not encrypt email that does not include VA sensitive information, or any email excluded from the encryption requirement.
- Protect VA sensitive information aggregated in lists, databases, or logbooks, and include only the minimum necessary SPI to perform a legitimate business function.
- 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 Not:

- Disclose any information protected by any of VA's privacy statutes or regulations without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, and individuals.
- Allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance by my VA supervisor, ISSO, and Information System Owner, local AM, or designee.
- Make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to verbal communications, e-mail, text messaging, instant messaging, online chat, social media, and web sites.

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements.
- Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

I Will Not:

- Store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-3 (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.

Incident Reporting

I Will:

- Report suspected or identified information security incidents including unauthorized disclosures of VA information, or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor, Information System Security Officer (ISSO) or designee immediately upon suspicion.

Social Media & Networking to Conduct Official VA Business

I Will:

- Use the VA intranet to conduct VA business on social media/networking sites wherever possible.
- Use web-based collaboration and social media tools in accordance with VA Directive 6515, Use of Web-Based Collaboration Technologies.
- Limit the personal use of social media/networking sites, in accordance with VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology.
- Obtain approval from the Office of Public and Intergovernmental Affairs (OPIA) before establishing a VA social media account.
- Ensure that my use of social media, to conduct VA business, complies with law, guidance, and VA policy.
- Be professional at all times when posting to VA-related social media.
- Use my best judgment when interacting on social media about matters related to VA's mission.
- In my capacity as a VA representative, post only information about which I have actual knowledge.
- Identify myself and my roles as a VA representative when commenting or providing information on matters related to the VA's mission, and ensure that my profile and any related content is consistent with how I wish to present myself to colleagues, Veterans, and the general public.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

- Only post and use content in accordance with applicable ethics, intellectual property, records, and privacy laws, regulations, and policies.
- Use only instant messaging services approved by VA.
- If content I publish on blogs, wikis or any other form of user-generated media might reasonably be perceived as the position of VA, publish a disclaimer that the views are my own and do not represent VA.

I Will Not:

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

5. ACKNOWLEDGEMENT AND ACCEPTANCE

- a. I acknowledge that I have received a copy of VA Information Security Rules of Behavior for Organizational Users.
- b. I understand, accept and agree to comply with all terms and conditions of VA Information Security Rules of Behavior for Organizational Users.
- c. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

Print or type your full name

Signature

Date

Office Phone _____

Position Title _____



VA Privacy and Information Security Awareness and Rules of Behavior

Appendix B: Department of Veterans Affairs Information Security Rules of Behavior For Non-Organizational Users

1. COVERAGE

- a. This Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) identifies the specific responsibilities and expected behavior for non-organizational users of VA information and information systems as required by 38 U.S.C. § 5723(f)(5), OMB Circular A-130, Appendix I, §§ 4(h) (6-7) and VA Handbook 6500, *Managing Information Security Risk: VA Information Security Program*.
- b. *Organizational users* are VA employees, contractors, researchers, students, volunteers, and representatives of Federal, state, local or tribal agencies who are authorized to access VA information and information systems but do not represent a Veteran or claimant. The rules of behavior for organizational users are identified in the Department of Veterans Affairs Information Security Rules of Behavior for Non-Organizational Users.
- c. *Non-organizational users* other than 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 is the information under the control of VA or stored on a VA information system. This includes both VA sensitive and non-sensitive information. Information properly disclosed by VA to a non-organizational user (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.
- e. The 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 ROB provides the minimum requirements, which individual users of VA information and information systems must agree to comply, and VA facilities and other agency components may issue requirements for protection that exceed the ROB.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

2. COMPLIANCE

- a. Non-compliance with ROB may result in 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 suspension of access through a VA information system. Depending on the severity of the violation and management discretion, consequences may include access restriction or suspension of access privileges. Theft, conversion, or unauthorized disclosure or disposal of Federal property or disclosure of information may result in criminal sanctions.
- b. Unauthorized access, upload, download, change, circumvention, or deletion of information on VA systems without authorization; modification VA systems; denying or granting access to VA systems without authorization; unauthorized purpose on VA systems; or otherwise misusing VA systems or resources is strictly prohibited and may result in criminal sanctions.
- c. The 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. This ROB must be signed before access is provided to a new user of VA information and information systems. Thereafter, the ROB must be signed annually by all non-organizational users of the VA information or information systems. This signature indicates agreement to comply with ROB, and refusal to sign the ROB will result in denial of access to VA information or information systems.
- b. This ROB may be signed in hard copy or electronically. If signed using the hard copy method, the user must initial and date each page and provide the information requested under Acknowledgement and Acceptance.

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.
- 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.
- Follow established procedures for requesting access to any VA information system and for notifying VA when the access is no longer needed.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

- Only use my access to VA information and information systems for officially authorized purposes.
- Only use VA-approved solutions, software, or services for connecting non-VA- owned systems to VA's network either remotely or directly.

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive information.
- 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 Information System Security Officer (ISSO) or Change Management Agent.

Protection of VA-Issued Devices

I Will:

- Protect Government Furnished Equipment (GFE) from theft, loss, destruction, misuse, and threats.
- 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.

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee.
- Attempt to override, circumvent, alter, or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff.

Data Protection

I Will:

- If authorized to directly connect to a VA system, only use virus protection software, antispyware, and firewall/intrusion detection software authorized by VA.

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.
- Disable or degrade software programs used by VA that install security software updates on computer equipment and all electronic devices used to connect to VA information systems, or used to create, store, or use VA information.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

Remote Access

I Will:

- Protect information about remote access mechanisms from unauthorized use and disclosure.
- I will notify my supervisor, COR, ISSO, and local Area Manager (AM), or designee prior to any international travel with a VA mobile device (laptop, PDA) so that appropriate actions can be taken prior to my departure and upon my 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 mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

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.
- Access any VA information system from any foreign country unless approved by a VA ISSO, local Area Manager (AM) and Information System Owner.
- Access VA's internal network from any foreign country designated as a security risk unless approved by my supervisor, COR, ISSO, local AM, and Information System Owner. This prohibition does not affect access to VA external web applications.

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames.
- Complete any additional role-based security training required based on my role and responsibilities.
- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action.
- 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.
- Permit only those authorized by OIT to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software.
- Sign specific or unique ROBs as required for access or use of specific VA systems or non-VA systems.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

Sensitive Information

I Will Not:

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

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements.
- Protect my passwords; verify codes, tokens, and credentials to prevent unauthorized use and disclosure.

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 140-3 (or its successor) validated encryption, and I am the only person who can decrypt the file.
- Hardcode credentials into scripts or programs.
- Divulge a personal username, password, access code, verify code, or other access credential to anyone.

Incident Reporting

I Will:

- Report suspected or identified information security incidents, including unauthorized disclosures of VA information or access to a VA information system, as well as anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) on VA information systems to a VA ISSO, local Area Manager (AM), and Information System Owner immediately upon suspicion.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

Social Media & Networking to Conduct Official VA Business

I Will:

- Use the VA intranet to conduct VA business on social media/networking sites wherever possible.
- Use web-based collaboration and social media tools in accordance with VA Directive 6515, Use of Web-Based Collaboration Technologies.
- Limit the personal use of social media/networking sites in accordance with VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology.
- Obtain approval from the Office of Public and Intergovernmental Affairs (OPIA) before establishing a VA social media account.
- Ensure that my use of social media to conduct VA business complies with law, guidance, and VA policy.
- Be professional at all times when posting to VA-related social media.
- Use my best judgment when interacting on social media about matters related to VA's mission.
- In my capacity as a VA representative, post only factual information about which I have actual/firsthand knowledge.
- Identify myself and my roles as a VA representative when commenting or providing information on matters related to VA's mission, and ensure that my profile and any related content is consistent with how I wish to present myself to colleagues, Veterans, and the general public.
- Only post and use content in accordance with applicable ethics, intellectual property, records, and privacy laws, regulations, and policies.
- Use only instant messaging services approved by VA.
- If content I publish on blogs, wikis or any other form of user-generated media might reasonably be perceived as the position of VA, publish a disclaimer that the views are my own and I do not represent the VA.

Initials



VA Privacy and Information Security Awareness and Rules of Behavior

I Will Not:

- Comment on VA mission-related legal matters unless I am the VA official spokesperson for the matter and have management approval to do so.
- In my capacity as a VA representative, comment or provide information on any matter about which I do not have actual, up-to-date knowledge.
- Post information protected by the Privacy Act of 1974, 38 USC 5701, 5705, or 7332, the Health Insurance Portability and Accountability Act (HIPAA) Rules, or VA policy on any non-VA websites, without legal authority and prior approval by authorized official;
- Use my VA title or indicate that I represent VA when acting outside of my official capacities.
- Use profanity; make libelous statements; or use privately-created works without the express, written permission of the author.
- Quote more than short excerpts of another person's work unless the source is properly credited.

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

Print or type your full name

Signature

Date

Office Phone _____

Position Title _____



VA Privacy and Information Security Awareness and Rules of Behavior

Appendix C: Glossary

A

AirWatch® - AirWatch® is an enterprise solution that allows for centralized account and security setting management.

Source: vaww.eie.va.gov

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

AnyConnect - AnyConnect Secure Mobility Client (formerly Cisco AnyConnect VPN Client) provides endpoint security, policy enforcement, and encrypted network connectivity for a variety of platforms to allow corporate network access.

Source: <https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=5897#>

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

Area Manager - The individual working with the senior agency Information System Security Officer (ISSO), Authorizing Official (AO), or Information System Owner for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system. This role was previously referred to as the Facility Chief Information Officer (CIO).

Source: NIST SP 800-161 (CNSSI 4009)

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

Authorized User - Individual, or (system) process acting on behalf of an individual, authorized to access an information system. Source: SP 800-53

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

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

Source: NIST SP 800-53

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

Azure RMS - The protection technology used by Azure Information Protection. This cloud-based protection service uses encryption, identity, and authorization policies to help secure your files and email, and it works across multiple devices—phones, tablets, and PCs. Information can be protected



VA Privacy and Information Security Awareness and Rules of Behavior

both within your organization and outside your organization because that protection remains with the data, even when it leaves your organization's boundaries.

Source: <https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms>

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

B - N/A

C

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

Source: Office of Information and Technology, VA ESE OE Remote Bundle Package Storefront 3.6 End User Guide for Chrome OS version 1.3, March 17, 2017

<https://raportal.vpn.va.gov/Main1/ImageStream.aspx?DocID=7995>

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

Source: NIST SP 800-53

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

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

Source: VA Handbook 6500.6 Glossary

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



VA Privacy and Information Security Awareness and Rules of Behavior

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

Source: VA Handbook 0735

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

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

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

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

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

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

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

D

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

Source: 38 U.S.C. § 5727

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

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



VA Privacy and Information Security Awareness and Rules of Behavior

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

Employee - An individual who is appointed in the civil service and engaged in the performance of a federal function under supervision by a federal officer or employee. Title 38 Hybrid employee is an individual appointed on a temporary or permanent basis (full-time, part-time, or without compensation) under 38 U.S.C., chapters 73 and 74 in occupations (positions) identified in 38 U.S.C. 7401 (1) or (3).

Source: 5 U.S.C. § 2105(a)

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

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

Enterprise Service Desk (ESD) - The Enterprise Service Desk is the help desk for all VA employees. Formerly referred to as the National Service Desk, employees go to the ESD for timely resolution of their technology needs, ranging in complexity from simple password resets to more serious service disruptions.



VA Privacy and Information Security Awareness and Rules of Behavior

Source: <https://vaww.oit.va.gov/itops-transformation-update-14-spotlight-enterprise-service-desk/>

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

Source: Adapted from VA Handbook 6300.1

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>



VA Privacy and Information Security Awareness and Rules of Behavior

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-interimfinal-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 healthcare 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 healthcare system by encouraging the widespread use of electronic data interchange in the U.S. healthcare system.

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

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



VA Privacy and Information Security Awareness and Rules of Behavior

I

Identity Theft - A fraud committed using the identifying information of another person.

Source: 15 USC 1681a.

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: FIPS 200; NIST SP 800-53 rev.4

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

Information Security - The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Source: 38 U.S.C. § 5727

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

Information System Security Officer - Individual working with the senior agency ISSO, AO, or Information System Owner to help ensure the appropriate operational security posture is maintained for an information system or program.

Source: CNSSI-4009 [VA Adapted]

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

Information Technology Operations and Services (ITOPS) - ITOPS delivers enterprise-wide IT infrastructure engineering and operations services effectively, efficiently and securely to enhance the customer experience and enable VA to optimize service delivery to Veterans.

Source: <https://vaww.oit.va.gov/oit/itops/>

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

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

Source: CNSSI 4009



VA Privacy and Information Security Awareness and Rules of Behavior

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 - The term “integrity” means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Source: NIST SP 800-53

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

J - N/A

K

Knowledge Service (KS) - VA’s knowledge portal for providing cybersecurity policies, procedures, and guidance.

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

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 government, is performed on the employee’s non-work time, does not interfere with VA’s mission or operations, and does not violate standards of ethical conduct for executive branch employees.

Source: Adapted from VA Directive 6001

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



VA Privacy and Information Security Awareness and Rules of Behavior

M

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

Source: NIST SP 800-61

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>

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

Source: NIST 800-53; VAH 6500.10



VA Privacy and Information Security Awareness and Rules of Behavior

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

N

Need to Know - Need to know limits information access to the information that an individual requires to carry out his or her job responsibilities.

Source: Lynda.com (now LinkedIn Learning) course on IT security: Need to Know; SSCP Cert Prep: 2 Security Operations and Administration

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

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

Source: NIST SP 800-53

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

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

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

O

Office of Information Technology - The Office of Information and Technology (OIT) thrives on diversity. We recruit, develop, and sustain a 16,000+ team of employees and contractors who use their talents and backgrounds to deliver technologies and services that improve the Veteran experience.

Source: <https://vaww.oit.va.gov/oit/>

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

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

Source: This definition is based on the Information Security Rules of Behavior for Organizational Users policy.



VA Privacy and Information Security Awareness and Rules of Behavior

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 three of the following four categories: English uppercase characters, English lowercase 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 three of the four 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: NIST SP 800-53

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

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

Source: West's Encyclopedia of American Law, edition 2. (2008)

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



VA Privacy and Information Security Awareness and Rules of Behavior

standard for internet security. As an added benefit, PKI can provide the functionality for digital signatures to ensure document authenticity.

Source: <https://www.oit.va.gov/programs/piv/locations.cfm>

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

Personally Identifiable Information (PII) - Personally identifiable information (PII) means 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. Examples of PII elements include, but are not limited to, 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.

Source: Reference is OMB Circular A-130

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 healthcare 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



VA Privacy and Information Security Awareness and Rules of Behavior

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

Privacy Officer - The PO is responsible for taking proactive measures to help ensure that PII collected by VA is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusions upon individual privacy, thereby minimizing privacy events. Additionally, it is the defensive duty of a PO to assist in mitigating damage when PII is compromised.

Source: VA Directive 6509 [VA Adapted]

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

Privileged User - A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Source: SP 800-53

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; participation 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



VA Privacy and Information Security Awareness and Rules of Behavior

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 - An 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: FIPS 196, VA Handbook 6500 Glossary

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



VA Privacy and Information Security Awareness and Rules of Behavior

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

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

Source: 36 CFR 1220

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: NIST SP 800-18

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

Remote Enterprise Security Compliance Update Environment (RESCUE) - A virtual private network (VPN) to connect to the VA Enterprise Network other than using the Citrix Access Gateway (CAG). RESCUE is for GFE only.

Source: [https://vaww.visn23.portal.va.gov/iow/SiteDirectory/Privacy-Info-Security/User Guides/VA Remote Access - Rescue, CAG, SMC, Contractors/RESCUE GFE Windows 7 User Guide.pdf](https://vaww.visn23.portal.va.gov/iow/SiteDirectory/Privacy-Info-Security/User%20Guides/VA%20Remote%20Access%20-%20Rescue,%20CAG,%20SMC,%20Contractors/RESCUE%20GFE%20Windows%207%20User%20Guide.pdf)

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



VA Privacy and Information Security Awareness and Rules of Behavior

Rules of Behavior (ROB) - The term “VA National Rules of Behavior” means a set of Department rules that describes the responsibilities and expected behavior of personnel with regard to information system usage.

Source: VAIQ 7823189, Updated VA Information Security Rules of Behavior, September 15, 2017

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

S

SafeNet Mobile PASS Token - SafeNet MobilePASS is a one-time password (OTP) software authentication solution that combines the security of proven two-factor strong authentication with the convenience, simplicity, and ease of use of OTPs generated on personal mobile devices or PCs.

Source: <https://safenet.gemalto.com/multi-factor-authentication/authenticators/software-authentication/mobilepass-otp-authenticator/>

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

Sensitive Personal Information (SPI) - The term “sensitive personal information,” with respect to an individual, means any information about the individual maintained by an agency, including the following: education, financial transactions, medical history, and criminal or employment history; or information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records.

Source: 38 U.S.C. § 5727

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

ServiceNow (IT Service Management Tool) - A comprehensive single platform that modernizes the way our customers access IT support in VA. ServiceNow will enhance OIT employees' ability to prioritize incidents, analyze issues, and capture service management metrics. It will offer an advanced self-service portal through which users can submit requests, report issues, and talk to technicians via an online chat function.

Source: Adapted from <https://www.oit.va.gov/reports/year-in-review-2017/index.cfm?v=modernization&project=cloud>

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



VA Privacy and Information Security Awareness and Rules of Behavior

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, YouTube, etc. 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

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

Source: CNSSI 4009-2015

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,



VA Privacy and Information Security Awareness and Rules of Behavior

disclosure, modification of information, and/or denial of service (DoS). Examples of threats include phishing, social engineering, and spoofing.

Source: NIST SP 800-53 rev 4

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.

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, human immunodeficiency virus (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 HIV, or sickle cell anemia records.



VA Privacy and Information Security Awareness and Rules of Behavior

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 - The term “VA sensitive information” means any information that has not been cleared for public release and has been collected, developed, received, transmitted, used or stored by VA, or by a non-VA entity in support of an official VA activity. VA Sensitive Information may also be referred to as Controlled Unclassified Information (CUI).

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: NIST SP 800-113

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

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

Source: NIST SP 800-82 Revision 2 (May 2015)

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.



VA Privacy and Information Security Awareness and Rules of Behavior

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

Workspace One Hub - Workspace One Hub is a commercially available enterprise-used app that contains an enhanced version of Airwatch Agent.

Source: vawww.eie.gov/SysDesign/CS/MT/default.aspx

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 and Dictionary.com

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

Z - N/A



VA Privacy and Information Security Awareness and Rules of Behavior

Appendix D: Privacy and Information Security Resources

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

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.

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 Enterprise Service Desk to request computer, network, or access support or to report security incidents to the Cybersecurity Operations Center (CSOC): (855) 673-4357

VA Web Links

- Insider Threat Program website:
https://www.osp.va.gov/insider_threat_program_awareness_reporting_tool.asp
- ITWD's role-based training*:
<http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Pages/default.aspx>
- Locator to identify ISSOs* and POs*: <https://vaww.portal2.va.gov/sites/infosecurity/ISO-PO-Locator/default.aspx>
- Mobile Documentation > Approved Devices and Apps*:
<https://vaww.eie.va.gov/SysDesign/CS/MT/Shared%20Documents/Forms/Documents.aspx?RootFolder=%2fSysDesign%2fCS%2fMT%2fShared%20Documents%2fApproved%20Devices%20and%20Apps&Folder>
- Mobile Documentation > Procedures*:
<https://vaww.eie.va.gov/SysDesign/CS/MT/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fSysDesign%2fCS%2fMT%2fShared%20Documents%2fProcedures&FolderCTID=0x012000CE74B1C730FD694FA9DF56B69E70282500E0245BBF72BE8C4F93592E1B9ACC2EF3&View={08212D1F-F3A2-4E22-8328-44594CAA55E2}>
- PIV Badge Office: www.osp.va.gov or <https://www.oit.va.gov/programs/piv/how-to.cfm>
- PIV Card Project: <https://www.oit.va.gov/programs/piv/>



VA Privacy and Information Security Awareness and Rules of Behavior

- Project Help Site > Rights Management Service (RMS)*: <http://vaww.help.portal.va.gov/>
- Office of Inspector General (Information Requests): <https://www.va.gov/oig/foia/>
- Office Service Operations, Enterprise Security Operations (ESO), Specialized Device Security Division*: <https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/HISD.aspx>
- Remote access solutions*: <https://raportal.vpn.va.gov/Main1/>
- VA CSOC Threat Assessment and Analysis Portal, User Reporting Page*: <https://esm.vansoc.va.gov/Pages/User-Reporting-Page.aspx>
- VA Controlled Unclassified Information (CUI)*: <https://vaww.oit.va.gov/services/cui/>
- VA Knowledge Service*: <https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/Pages/Home.aspx>

*Accessible only on the VA Intranet.

TMS Courses

Talent Management System available at: <https://www.tms.va.gov/SecureAuth35/>

- *An Introduction to Rights Management Service—RMS* (VA TMS ID: 336914)
- *Getting Started with Public Key Infrastructure (PKI) Manual Enroll* (VA TMS ID: 1256927)
- *Identity Theft and Prevention* (VA TMS ID: 3591967)
- *Mobile Training: Security of Apps on iOS Devices* (VA TMS ID: 3926744)
- *Privacy and HIPAA Training* (VA TMS ID: 10203)
- *Social Networking and Security Awareness* (VA TMS ID: 2626967)
- *VA Telework Training Module for Employees* (VA TMS ID: 1367006)

Privacy and Information Security Laws and Regulations

- *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>
- *Freedom of Information Act (FOIA)*: Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions. <https://www.foia.gov/>



VA Privacy and Information Security Awareness and Rules of Behavior

- **Health Information Technology for Economic and Clinical Health Act (HITECH):** 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 of 1974:** Requires federal agencies to establish appropriate safeguards to ensure the security and confidentiality of the records they maintain about individuals, establishes restrictions on the disclosure and use of those records by federal agencies, and permits individuals to access and request amendments to records about themselves. <https://www.justice.gov/opcl/privacy-act-1974>
- **United States Code (U.S.C.):** Veterans Confidentiality Statutes Title 38 U.S.C. § 5701: Confidential Nature of Claims: Information about any claims processed by VA must be kept confidential. <https://www.govinfo.gov/app/details/USCODE-2010-title38/USCODE-2010-title38-partIV-chap57-subchapl-sec5701/context>
- **Title 38 U.S.C. § 5705:** Confidentiality of Medical Quality Assurance Records: Information generated during a medical quality assurance program may not be disclosed except when authorized. <https://www.govinfo.gov/app/details/USCODE-2010-title38/USCODE-2010-title38-partIV-chap57-subchapl-sec5705>
- **Title 38 U.S.C. § 7332:** Confidentiality of Certain Medical Records: 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. <https://www.govinfo.gov/app/details/USCODE-2011-title38/USCODE-2011-title38-partV-chap73-subchapIII-sec7332/summary>



VA Privacy and Information Security Awareness and Rules of Behavior

VA Directives and Handbooks

VA Publications available at: <https://www.va.gov/vapubs/>

Directives

- VA Directive 6500, *VA Cybersecurity Program*
- VHA Directive 1400.06, *Foreign Travel*
- VA Directive 0710, *Personnel Security and Suitability Program*
- VA Directive 6066, *Protected Health Information (PHI) and Business Associate Agreements Management*
- VA Directive 6300, *Records and Information Management*
- VHA Directive 1605, *VHA Privacy Program*

Handbooks

- VA Handbook 6609, *Mailing of Sensitive Personal Information*
- VA Handbook 0710, *Personnel Security and Suitability Program*
- VA Directive 6300, *Records and Information Management*
- VA Handbook 6300.5, *Procedures for Establishing and Maintaining Privacy Act Systems of Records*
- VA Handbook 6300.6, *Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses*
- VA Handbook 6300.4, *Procedures for Processing Requests for Records Subject to the Privacy Act*
- VA Handbook 6300.1, *Records Management Procedures*
- VA Handbook 6500, *Risk Management Framework for VA Information Systems—Tier 3: VA Information Security Program*
- VA Handbook 6500.1, *Electronic Media Sanitization*
- VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*
- VA Handbook 6500.10, *Mobile Device Security Policy*
- VA Handbook 6512, *Secure Wireless Technology*
- VA Handbook 6502, *VA Enterprise Privacy Program*
- VA Handbook 6502.01, *Privacy Event Tracking*

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

- VHA Handbook 1907.01, *Health Information Management and Health Records*



VA Privacy and Information Security Awareness and Rules of Behavior

- VHA Handbook 1173.08, *Medical Equipment and Supplies*
- VHA Directive 1605, *VHA Privacy Program*
- VHA Handbook 1605.02, *Minimum Necessary Standard for Protected Health Information*
- VHA Handbook 1605.01, *Privacy and Release of Information*

Additional Selected VA Handbooks and Directives

- VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*
- VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*
- VA Directive 0701, *Office of Inspector General Hotline Complaint Referrals*
- VA Handbook 5021.6, Appendix A, *Employee/Management Relations*
- VA Handbook 6500, Appendix F, *VA System Security Controls*
- VA Handbook 6500.6, *Contract Security*
- VA Handbook 5011/5, *Hours of Duty and Leave*
- VA Handbook 5011/26, *Hours of Duty and Leave (Telework)*
- VA Handbook 5021/3, *Employee/Management Relations*
- VA Directive 6515, *Use of Web-Based Collaboration Technologies*

VA Forms and Memorandums

VA Forms Home Page available at: <https://www.va.gov/vaforms/default.asp/>

- VA Form 0740, *New Telework Request Agreement*, Aug 2013
- VA Form 0244, *Records Transmittal and Receipt*
- VA Form 7468, *Request for Disposition of Records*

VA Memorandums available at: <https://vaww.vashare.oit.va.gov/sites/ois/knowledgeservice/pages/das-ois-memos.aspx/>

- Memorandum VIEWS 01249876, *Information Security Rules of Behavior for Organizational Users*, September 23, 2019
- Memorandum VIEWS 01249880, *Information Security Rules of Behavior for Non-Organizational Users*, September 23, 2019
- Memorandum VAIQ 7633050, *Mandatory Use of PIV Card Authentication for VA Information System Access*
- Memorandum VAIQ 7581492, *Proper Use of Email and Other Messaging Services*