Contents

Purpose of this Document ........................................................................................................... v
Using Hyperlinks Within This Document ................................................................................... v

Topic 1: Course Introduction .................................................................................................... 1
  1.1 Welcome .......................................................................................................................... 1
  1.2 Organizational and Non-Organizational Users ................................................................. 1
  1.3 Who Must Take This Course? ......................................................................................... 1
  1.4 Why Do You Have to Take This Course? ....................................................................... 2
  1.5 Types of VA Sensitive Information .................................................................................. 2
  1.6 Rules of Behavior ............................................................................................................ 3
  1.7 What to Expect ................................................................................................................. 4

Topic 2: Handling VA Information .............................................................................................. 5
  2.1 Introduction ..................................................................................................................... 5
  2.2 Protecting Sensitive Information ..................................................................................... 5
  2.3 Need-to-Know .................................................................................................................. 5
  2.4 Handling PII With Care ................................................................................................... 6
  2.5 Safeguarding Paper Documents ..................................................................................... 7
  2.6 Paper Documents ............................................................................................................. 8
  2.7: Mismailing Sensitive Information ............................................................................... 9
  2.8: Records Management ................................................................................................... 10
  2.9: Keeping Records Safe and Secure .............................................................................. 10
  2.10: Summary ..................................................................................................................... 10

Topic 3: Accessing VA Information Systems .............................................................................. 11
  3.1 Introduction .................................................................................................................... 11
  3.2 Protecting Access to VA Systems .................................................................................. 11
  3.3 Identification and Authentication .................................................................................... 11
  3.4 Lost PIV Card ................................................................................................................. 13
  3.5 Minimum Access ............................................................................................................ 14
  3.6 Protecting Systems ......................................................................................................... 15
  3.7 Securing Your VA Workstation ..................................................................................... 15
  3.8 Data Protection Software ............................................................................................... 16
  3.9 Connecting to the Network Using a Non-GFE Computer System ................................. 17
  3.10 Summary ...................................................................................................................... 18
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) 2019 (i.e., October, 2018 through September, 2019).

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, and then, sign the Acknowledge and Accept section for the user group that applies to you. Review the definitions of organizational and non-organizational Users on the next page to determine your user group.

2. Contact your supervisor or Contracting Officer Representative (COR) to submit the signed ROB and to coordinate with your local Talent Management System (TMS) Administrator to ensure you receive credit for completion.

Using Hyperlinks Within This Document

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

1.1 Welcome

Welcome to the VA Privacy and Information Security Awareness and Rules of Behavior: Everyday Journey to Protect VA training course.

1.2 Organizational and Non-Organizational Users

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

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

Each of our journeys are impacted by risks. We need to be aware of these risks and stay vigilant to follow VA’s Rules of Behavior (ROB). This will help us to accomplish our day-to-day duties securely.

When it comes to privacy and information security, all employees are required to follow the ROBs. The ROBs provide guidance for organizational and non-organizational users on how to protect VA sensitive information and safeguard VA systems.

1.3 Who Must Take This Course?

Both organizational and non-organizational users must take this course.

While VA, as an organization, must comply with federal laws dealing with privacy and information security, it all begins with you, the user. Regardless of the role you play at VA, anyone can 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 Veteran’s 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).

All staff with direct access to Protected Health Information (PHI) or access to PHI through VHA computer systems are required to complete the Privacy and HIPAA Training (VA TMS ID: 10203).
1.4 Why Do You Have to Take This Course?

Like any trip you might take, taking the path to protect VA sensitive information is all about reaching your destination safely. This course will help you become more aware of how to protect VA sensitive information.

All users must take this course prior to using or gaining access to VA information or information systems. To keep your access, you must complete this training annually. Each year, when you complete this training, you will review, acknowledge, and accept the ROBs.

Evolving computer technologies and tools increase the speed and effectiveness of providing services to Veterans. At the same time, new risks are a part of every new opportunity. You must always be aware of these risks and be ready to protect sensitive information and systems. Depending on your role and the information and systems you have access to, you may be required to complete additional role-based security training.

1.5 Types of VA Sensitive Information

Sensitive information can be defined as information that is protected against unauthorized disclosure. Types of sensitive information include the following:

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

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

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

- **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.
1.6 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 presented throughout the course that apply to your user type. Understanding these rules will help you stay on track and take the right action when it comes to complying with the ROBs. The ROBs will be presented for your acknowledgement and acceptance at the end of the course.

Basic ROBs that apply to each user type include the following:

Organizational users:

- I WILL comply with all federal VA information security, privacy, and records management policies.
- I WILL have NO expectation of privacy in any records that I create or in my activities while accessing or using VA information systems.
- I WILL complete mandatory security and privacy awareness training within designated time frames, and complete any additional role-based security training required based on my role and responsibilities.
- 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 or unique ROBs as required for access or use of specific VA systems or non-VA systems.

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 or unique ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity’s ROB to conduct VA business. While using their system, I must comply with their ROB.
1.7 What to Expect

During this course, you can expect to gain a better understanding of your roles and responsibilities for protecting VA information. To do so, you will take a virtual journey that includes several stops along the way.

At each stop, you will be given important guidance for your everyday journey to protect VA and our Nation’s Veterans. You will also discover 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.

Practical, realistic scenarios are presented throughout this course. You will have the opportunity to reflect on each situation and decide the best action to take to avoid a violation where privacy and security may have been put at risk.

For each scenario, you will 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 as the last stop of your journey in this course.
Topic 2: Handling VA Information

2.1 Introduction

When you handle sensitive Veteran and VA information, you are operating in a position of trust. Once trust is lost, it can be difficult or even impossible to regain. Be careful to handle that information correctly, regardless of what form it is in.

On this stop in your journey, you will find situations that occur when you are responsible for handling VA information. By following the ROBs and making the right decisions in dealing with VA sensitive information, you are protecting VA, our Veterans, and their families.

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

- Recall how to protect VA sensitive information when handling paper documents, records, and files
- Recognize the requirements that everyone must follow for records management

2.2 Protecting Sensitive Information

Sensitive information can be compromised in many ways, including sharing information with people who do not need to know it or through unauthorized disclosure. You are responsible for making decisions when dealing with VA sensitive information, and you need to choose wisely. One wrong turn, and you could end up in a situation where information is at risk.

The scenarios in this section present the basic concepts that each VA employee can implement in his or her day-to-day work to protect VA sensitive information.

2.3 Need-to-Know

Scenario

Carlos is a nurse at the VA clinic in his hometown. His Uncle George is a combat Veteran receiving care at that same facility. One afternoon, Carlos’ cousin, Sylvia, calls him to say that she thinks her father has started drinking again. She asks Carlos if he will check George’s medical records to see if her father is being treated for alcoholism. He tells her he is not able to get that information for her.

Did Carlos do the right thing?

Determine the best answer from the options below:

A. Yes. Even though George is Carlos’ family member, Carlos does not have a work-related need to know his uncle’s medical information.

B. No. This situation is a family matter. Because of his cousin’s concern, he should have provided the information.
Correct Feedback

The correct answer is A.

Carlos handled this situation correctly. He does not have a need to know what’s in his uncle’s medical record. According to the ROB, he is also not allowed to disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority. He would be accessing the information only for personal reasons, which is a breach of privacy and a violation of HIPAA. Carlos was smart not to let family pressure get to him. He followed the ROB by refusing to get the information for his cousin and avoided a privacy incident.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information.
- I WILL NOT disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals.

Non-Organizational Users:

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

2.4 Handling PII With Care

Scenario

Tamara is a receptionist at her local VA medical center. One morning, she checked out a Veteran who seemed frustrated. She was very busy at the time and wasn’t able to ask if there was anything she could do to help. She thought about it all day and decided to get his file and call him when she got home that evening. She took the Veteran’s file home and called him outside of her working hours to discuss the situation and ended up providing him personal guidance regarding the matter.

Did Tamara handle this situation correctly?

Determine the best answer from the options below:

A. Yes, she was helping a Veteran with his issue.
B. No, Tamara has violated the ROBs that deal with handling PII.
Correct Feedback

The correct answer is B.

Tamara did not handle this situation correctly. The Veteran may misconstrue Tamara’s personal opinion and perspective as official VA guidance. She used her position to access a certain Veteran’s sensitive information and then took that information off site without authorization or permission. This is a violation of VA policy and may result in HR consequences. Never remove PII information from VA without permission and never use it for unauthorized purposes. Information collected during the performance of duties should only be used for official business purposes. Remember, sensitive information can be as simple as names and phone numbers or as critical as a medical diagnosis or treatment. Ensure confidentiality, and treat all sensitive information as if it were your own.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users:

- I WILL obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)).
- I WILL safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel).

2.5 Safeguarding Paper Documents

While it may seem that many documents are electronic, paper documents still exist, and VA has specific best practices for safeguarding them. These documents can include mailings, patient records, files, and other documents that could contain sensitive information.

The scenarios in this section present situations involving the handling of sensitive information, specifically paper documents. It is important to remember that handling such documents appropriately is an essential part of your everyday journey to protect VA.
2.6 Paper Documents

Scenario

Steve works at the VA hospital cafeteria. He has been busy cleaning tables from the lunchtime rush. He’s wiping down the last table when he sees a stack of papers and a CD-ROM lying on the table. He picks them up to throw them away but notices that they contain someone’s personal information. There’s a woman’s name, address, phone number, and Social Security number.

How should Steve handle this situation?

Determine the best answer from the options below:

A. Place the items deep down in the trash so no one will see them.
B. Take the items to his supervisor so she can secure the papers and contact an Information System Security Officer (ISSO) or Privacy Officer (PO).

Correct Feedback

The correct answer is B.

Taking the items containing personal information to his supervisor is the way to go.

The supervisor can then secure the papers and CD-ROM while contacting the ISSO or PO to report the incident. Had Steve not secured the items, he would have left the personal information exposed for someone else to find. This could have created a data breach. The impact could be disastrous; for example, it could cause identity theft, embarrassment for Veterans, loss of PII/PHI, and distrust of VA.

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).
- 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.
2.7: Mismailing Sensitive Information

Scenario

Samir is a VA employee. He needs to mail some documents to a Veteran, Laura. So he looks up Laura’s address in the database, and sends the documents. Later, Samir realizes that he referenced the wrong line for Laura’s address, and the documents were sent to a different Veteran.

Did Samir cause a privacy breach?

Determine the best answer from the options below:

A. No, it was an honest mistake.
B. Yes, he should have been more careful.

Correct Feedback

The correct answer is B.

Samir caused a privacy breach. Samir should have confirmed the details of where the documents were being sent to ensure they reached the right person. Now, a different Veteran may have access to Laura’s PII. He will need to call either his supervisor, PO, and/or ISSO to report the incident.

Prevent identity theft. Keep this in mind when using the United States Postal Service or other delivery services.

- Confirm that mailing labels and window envelopes show only the recipient’s name and address and no other information.
- Always verify the person’s name on the envelope matches the person’s name on the documents inside the envelope.
- Ensure that only authorized information is released.

For mass mailings, always spot check to ensure that the correct information is going out in the correct envelope. For additional information on mailing PII, refer to VA Directive 6609, Mailing of Sensitive Personal 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.
2.8: Records Management

Federal records come in many formats. In general, any materials that document the transaction of VA business are potential records.

Be sure you know what could be a record, and reach out to your supervisor or designated records management official if you have questions or if you are creating, transporting, storing, or disposing of materials that may be records.

Everyone must know how to manage records to comply with the Federal Records Act of 1950. VA has designated records management officials who manage federal records. Federal records must be kept and stored according to the requirements outlined in a records control schedule (RCS).

2.9: Keeping Records Safe and Secure

The ROBs that apply to records include the following:

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

Keep in mind that VA business-related email and text messages may also be considered records. Exercise caution before deleting them. Reference the memorandum VAIQ 7850460, Proper Use of Email and Other Messaging Services, published January 2, 2018, for more guidance.

To increase your knowledge about how to handle records at VA, you can also locate records management training on the Talent Management System (TMS). Records Management for Everyone (VA TMS ID:4192704) and other recommended courses can be found in the Resources section of this course. They are a great way to hone your skills as you continue your journey to protect VA.

2.10: Summary

VA sensitive information comes in many forms and should always be protected.

Follow these best practices when handling VA sensitive information:

- Access information on a need-to-know basis only.
- Avoid unauthorized disclosure of sensitive information.
- Follow the best practices for safeguarding and handling paper documents.
- Verify names and addresses when mailing sensitive information.
- Understand your responsibilities for records management.
Topic 3: Accessing VA Information Systems

3.1 Introduction

VA information systems can be accessed from a variety of locations using a variety of methods. Knowing how to do so securely is important to maintain the integrity of the system.

On this stop of your journey, you will find scenarios that require responsible access to VA network systems.

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

- Recall how to securely access VA systems
- Recall the best action to prevent threats to VA networks and systems

3.2 Protecting Access to VA Systems

VA systems store and process important and sensitive information that is critical for us to provide the best care and service to our Veterans. You must ensure VA systems stay protected to prevent potential compromise of VA sensitive information. Protect your credentials required to access VA systems and make sure you, and others, only have access to the information and systems that are required to do your job.

The scenarios in this section will present you with situations that require you to make the right choice to protect and maintain your accesses to VA information and network systems securely.

3.3 Identification and Authentication

Scenario

When you logged in to your VA-issued computer this morning, you came across an issue you've never faced before. You asked your coworker, Kathy, to take a look. As you explained what happened, your supervisor called and asked if he could speak to you privately for a moment. Kathy offered to continue to work on the problem while you stepped away to speak with your supervisor. She asked you to leave your Personal Identify Verification (PIV) card/credential and Personal Identification Number (PIN) with her in case she gets locked out.

What should you do next?

Determine the best answer from the options below:

A. Stay logged in with your PIV card and give Kathy the PIN so she can continue to work on the issue while you leave to take the call in a private place.

B. Thank Kathy for the offer but refuse. Lock your computer and remove your PIV card before leaving to take the call.
C. Kindly refuse Kathy’s offer and then lock your computer. It’s okay to leave your PIV card inserted in the computer while you step away for the call since someone would need the PIN to access your account.

Correct Feedback

The correct answer is B.

Sharing your account credentials is a violation of the ROBs. Always keep credentials like user names, passwords, and PINs private. Never share your password or other account information, even with trusted coworkers. When leaving your computer workstation, remember to log off and take your PIV card/credential with you. Never leave it in your computer for others to find and compromise. Keep in mind that PIV cards also grant physical access to areas that not all employees have access to. This is another reason to keep your card with you. One of the biggest threats to any organization's data and information networks is the people who have the easiest access: insiders. Sharing your credentials and access to your VA information system presents an opportunity for an insider threat. Some other best practices to protect your account accesses are to create strong passwords that meet VA minimum requirements and store your VA passwords, if needed, only in files that have the latest validated encryption and that only you can decrypt.

Rules of Behavior

Review the associated rules for your user type below.

Non-Organizational Users

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

- I WILL NOT store my VA passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption, and I am the only person who can decrypt the file.

Organizational and Non-Organizational Users

- I WILL use passwords that meet the VA minimum requirements. Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure.
3.4 Lost PIV Card

Scenario

Josh is a benefits advisor for the Veterans Benefits Administration (VBA). It’s Friday, and Josh is looking forward to the weekend. After a very busy day of taking care of Veteran claims and attending meetings, his workday has finally come to an end and he goes to his car to drive home. When he gets to his car, he realizes that his PIV card is no longer on his lanyard. What should Josh do next?

Determine the best answer from the options below:

A. On his way home, he should contact a coworker to coordinate access to the building on Monday.

B. He should send out a group email to his coworkers to ask if anyone found his PIV card.

C. He should report the card loss to the PIV card issuing facility personnel, VA police, and his ISSO within four hours.

Correct Feedback

The correct answer C.

Josh should do the right thing and report the loss of his card. By doing so, Josh will prevent any potential unauthorized use. According to VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, PIV cardholders must notify the PIV card issuing facility personnel, VA police, and their ISSO within four hours of the loss.

Rules of Behavior

Review the associated rule for your user type below.

Organizational and Non-Organizational Users

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

Scenario

Claudia worked in the billing department of a VA hospital for three years. She recently transferred to another job and no longer needs access to the billing system. A friend asked her for help on some charges she didn't think were correct. Claudia checked and discovered that she still has access to the billing system.

What should Claudia do next?

Determine the best answer from the options below:

A. She should log out of the billing system and immediately notify her supervisor that she still has access to the system.

B. She should log out of the billing system and get back to her current tasking.

C. She should look at the billing system to verify that her friend was charged appropriately.

Correct Feedback

The correct answer A.

She should log out and immediately notify her supervisor that she still has access to the billing system. Employees must use their access to VA computer systems and records only for assigned duties. Since Claudia no longer works in billing, she no longer has the right to access the billing system. To avoid becoming an insider threat, you must notify your VA supervisor (or designee) any time you have access to a system you no longer need. Failing to do so exposes PII, invades the privacy of patients, causes potential risk to VA, and violates the need-to-know rule.
Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

• I WILL only use my access to VA computer systems and/or records for officially authorized and assigned duties.

Non-Organizational Users

• I WILL only use my access to VA computer systems and/or records for officially authorized purposes.

Organizational and Non-Organizational Users

• I WILL follow established procedures for requesting access to any VA information system and for notifying VA when the access is no longer needed.

3.6 Protecting Systems

Not only are we all responsible for accessing systems properly, we are also responsible for protecting those systems to minimize the potential for compromise.

The scenarios in this section include situations when you have to make the right choice to protect VA information systems.

3.7 Securing Your VA Workstation

Scenario

Vincent had been working with printed and electronic reports containing patient sensitive information all day. After receiving an urgent call from his daughter’s school, he quickly put the printed material in his desk drawer, gathered his personal belongings, and left without closing the electronic files or signing off his computer. He didn’t even think to grab his PIV card.

Did Vincent’s actions violate the ROBs?

Determine the best answer from the options below:

A. Yes. His actions made sensitive information vulnerable to anyone with access to his office.

B. No. He put the printed materials out of sight in his desk drawer and his VA computer will lock automatically due to inactivity.

Correct Feedback

The correct answer is A.

Vincent’s actions violated the ROBs and put sensitive information at risk. The ROBs require him to log out of all information systems at the end of each workday and to secure his PIV card.
Never leave PIV cards exposed; besides providing potential access to VA systems, it could provide access to restricted facility locations. Ensure that you only use approved methods to gain access to secured areas.

Always remember to 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. Be sure to lock all doors when the office is unattended.

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

3.8 Data Protection Software

Scenario

Michelle is doing some work on her VA-issued laptop that requires research on the internet. While on one of the sites, a pop-up appears saying that her computer is running slow and prompts her to click the link on the page to fix it.

Do you think she needs to check with her ISSO?

Determine the best answer from the options below:

A. Yes, it’s better to ask her ISSO than to ignore a potential threat.
B. No, this message wouldn’t display if there wasn’t a good reason.

Correct Feedback

The correct answer is A.

Michelle should check with her ISSO. It’s a good thing Michelle was cautious because this could be a sign of a ransomware attack. While there is virus protection software on your VA devices, cyber threats evolve so quickly, there’s no way to catch everything. As a note, you should never use any virus protection software, anti-spyware, or firewall/intrusion detection software that is not authorized by VA.

Here are three ways you can determine if a website is real. First, pay close attention to the URL. The address bar contains important information about your location and the security of the information you plan to access. Second, check the connection indicators. The address bar provides information to let you know that your connection to a website is private. Only websites that use “https” combined with a green padlock icon should be trusted with your personal information. Third, look for grammatical errors. Poor English or grammatical errors could indicate that the site is not real.
Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

- I WILL only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA.

Non-Organizational Users

- I WILL, if authorized to directly connect to a VA system, only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA.

Organizational and Non-Organizational Users

- I WILL NOT disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store or use VA information.

3.9 Connecting to the Network Using a Non-GFE Computer System

Scenario

Tony is a new contractor at a VA facility who will be working both on and off site. His role will require him to access sensitive information. As stated in the contract, he will not be issued government-furnished equipment (GFE), such as a laptop, and therefore will be using his corporate computer and his PIV card.

Will Tony be able to connect to the VA network when he is on site?

Determine the best answer from the options below:

A. Yes, as long as he only uses VA-approved solutions for connecting his non-VA-owned system to VA's network.

B. No. Only VA-issued equipment is allowed to connect to VA's network.

Correct Feedback

The correct answer is A.

As long as Tony gets the proper approval from the Contracting Officer's Representative (COR), Area Manager, and Information Technology and Operations (ITOPS) and uses a VA-approved solution to connect, he will be able to connect to the VA network with his corporate computer.
Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

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

Non-Organizational Users

- I WILL only use VA-approved solutions, software, or services for connecting non-VA-owned systems to VA’s network either remotely or directly.
- I WILL NOT use personally-owned equipment on-site at a VA facility to directly connect to the VA network, or connect remotely to the VA network unless approved prior to use (i.e., approval from VA ISO* or Change Management Agent).
  *Note: 1) The Information Security Officer (ISO) role is now referred to as Information System Security Officer (ISSO).

3.10 Summary

Think about accessing VA information systems the same way as you would be operating a motor vehicle. It’s not a right that you get to do so; it’s a privilege. As a user, you are required to abide by the ROBs that advise how to keep VA information systems safe and protected, just as you are required to follow traffic laws.

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

- Protect your credentials; this includes your personal user name, password and PIN, access and verify codes, or other access credential.
- Keep your PIV card secure.
- Only access systems you are permitted to use to do your current job.
- Use only VA-authorized virus protection software, anti-spyware, and firewall/intrusion detection software.
- Only connect approved devices, using approved methods, to VA networks and systems.
Topic 4: Protecting VA Computer Resources

4.1 Introduction

Whether you are issued VA-owned devices or equipment or you just work with them, you must take responsibility for their care and protection. Keep in mind that your journey is not yours alone. You are protecting the security, identity, and privacy of not only yourself but of every single person at VA, VA as a whole, and the Veterans we serve.

On this stop of your journey, you will find situations that deal with proper use and maintenance of VA devices and equipment.

It also includes 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 how to use VA-issued devices securely to prevent risk of exposing VA sensitive information
- Identify how to store, transport, and dispose of any media containing VA sensitive information
- Identify best practices and recertification for users of VA-provided Apple (iOS) mobile devices

4.2 Protecting VA-Issued Devices

You are an important line of defense at VA. Be diligent about protecting VA equipment and the information your devices contain.

The scenarios in this section will require you to make the right decisions to protect VA-issued computers and devices.

4.3 Downloading Software

Scenario

Ian is a VA employee. He and a friend are in the same role but support different offices. His friend mentions that he’s part of an online gaming group that plays during lunch hours. He asks Ian if he would like to join. He tells Ian that if he’s interested, he can download the game to his VA-issued computer, and then his friend provides the URL. Ian decides to join and tries to download the game, but the download is denied.

Were Ian’s actions appropriate?

Determine the best answer from the options below:

A. Yes. The group doesn’t play during working hours.
B. No. Downloading software from the internet poses a security risk.

Correct Feedback

The correct answer is B.
Ian’s actions were not appropriate. The fact is, he doesn’t have the authority to download the game to his computer. Plus, the ROBs prohibit Ian from downloading software from the internet to a VA-owned system. His actions could result in loss of use or limitations on use of equipment and disciplinary or adverse actions.

If Ian needs a download for his job, he will go through ServiceNow to submit a ticket.

For mobile devices, download apps from the Apple App Store ONLY if you are not receiving or inputting VA sensitive information. Only apps from the VA App Catalog have been deemed safe for use with VA sensitive information and for conducting VA business.

Do not use any software or services that you are not authorized to use—including those that require licensing or have copyright restrictions.

While downloading games to a VA-issued device is not appropriate, you can protect your identity on your own devices by using strong passwords for every site you visit often. Use numbers, letters, special characters, or some kind of 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 use only VA-approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions.
- I WILL permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.
- I WILL NOT download software from the Internet, or other public available sources, offered as free trials, shareware; or other unlicensed software to a VA-owned system.

**Non-Organizational Users**

- I WILL permit only those authorized by OIT to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software.
- 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.
4.4 Limited Personal Use

Scenario

Brianna is a clerk at the Veterans Benefits Administration (VBA). During a very slow day at work, she printed out two hundred flyers about upcoming neighborhood community outreach events for distribution to her community club members.

Was Brianna’s personal use of her work computer acceptable?

Determine the best answer from the options below:

A. Yes. Brianna’s personal use of her printing flyers did not interfere with her work responsibilities.

B. No. Brianna’s personal use involved prohibited activities.

Correct Feedback

The correct answer is B.

Brianna’s personal use of her work computer was not acceptable. Using government equipment during work hours and excessive use of consumables are violations of VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.

Rules of Behavior

Review the associated rule for your user type below.

Organizational Users

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

4.5 Unauthorized Visitors and Stolen Laptop

Scenario

During her daily rounds of IT inventory inspection, Wendy notices some unfamiliar people in the area. She asks a few coworkers who they are but no one seems to know. She feels as if she needs to confirm that the strangers are authorized to be in the area but is called away to a meeting. When she returns to her work on the inventory inspection, she finds that a laptop is missing.

Which of the following would have been the best approach to prevent the theft of the laptop?

Determine the best answer from the options below:

A. Wendy could have approached the strangers and asked who they were.
B. Wendy could have asked the strangers to leave the area.
C. Wendy could have approached the strangers and asked to see their VA PIV cards.

Correct Feedback

The correct answer is C.

This is the most vigilant approach. Wendy should have asked for proof that they were authorized to be in the area when she didn’t see their PIV cards. PIV cards should always be visible above the waist. If she had discovered that they weren’t authorized to be in the area, she could have immediately escalated the situation to the facility’s security staff.

VA staff should be vigilant to ensure only authorized personnel are in their work areas to help prevent theft and unauthorized access to sensitive information and systems.

Rules of Behavior

Review the associated rule for your user type below.

Non-Organizational Users

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

4.6 Stolen or Missing Equipment

Scenario

Hank was getting ready to travel on VA business, so he signed out a VA laptop. Because he would be dealing with sensitive information, he made sure it had the newest, validated encryption.

When he stopped for lunch, he took the laptop with him into the restaurant. No one was sitting near him, so he placed the laptop on his chair and left to order his food at the counter. When he returned, the laptop was gone.

Which of the following approaches should Hank have taken to prevent the theft of the laptop?

Determine the best answer from the options below:

A. Hank should have asked the hostess to keep an eye on the laptop.
B. Hank should have carried the laptop with him.

Correct Feedback

The correct answer is B.

In this scenario, Hank should have kept the laptop with him to avoid theft. While keeping mobile and storage devices with you at all times is ideal, it isn’t always convenient. Alternatively, Hank could have secured the laptop with a cable lock in the trunk of his car to prevent the theft. Theft is often a crime of opportunity. Don’t allow someone to take advantage of you.
In the event of theft, remember to report any missing or stolen VA equipment as soon as the loss is discovered. This includes encrypted or unencrypted laptops, tablets, flash drives, and phones.

**Rules of Behavior**

Review the associated rules for your user type below.

**Organizational Users**

- I WILL safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using FIPS 140-2 validated encryption (or its successor) unless it is not technically possible. This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)).

- I WILL secure mobile devices and portable storage devices (e.g., laptops, Universal Serial Bus [USB] flash drives, smartphones, tablets, personal digital assistants [PDA]).

**Non-Organizational Users**

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

### 4.7 Disposing of Old Flash Drives

**Scenario**

Larry’s old VA-issued flash drive malfunctioned, and he had to get a new one. Instead of simply discarding the old one, he contacted the Office of Information Technology (OIT) to make arrangements to turn it in to an authorized OIT representative.

Did Larry take proper action according to the ROBs?

Determine the best answer from the options below:

- A. Yes. This is the correct procedure for disposing of a VA storage device.

- B. No. As long as Larry disposed of the flash drive within his office, he would have met the ROBs.

**Correct Feedback**

The correct answer is A.

Larry took the proper action. Employees should turn in any equipment they will no longer be using to OIT personnel. Larry’s actions prevented the potential loss or exposure of VA or Veteran information.

Remember, when it comes to GFE, for security and inventory control, you must sign for items and return them when they are no longer needed—that includes times when the equipment is no longer functioning as intended. GFE should never been thrown away; it should always be returned to OIT.

**Rules of Behavior**

Review the associated rules for your user type on the next page.
Organizational and Non-Organizational Users

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

Non-Organizational Users

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

4.8 Mobile Phone Recertification

If you have a VA-issued mobile device (e.g., Apple iOS), you must complete security training each year to refresh your knowledge and reaffirm your commitment to follow the related ROBs. By completing this course, you also meet the annual training requirement for mobile devices.

For secure use of VA-issued mobile devices, do the following:

- Enroll GFE mobile devices in AirWatch® before downloading any apps.
- Use apps from the VA App Catalog. They have been deemed safe for use with VA sensitive information and for conducting VA business.
- Download apps from the Apple App Store ONLY if you are not receiving or inputting VA sensitive information, (e.g. hotel, airline, and weather apps). 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.
- Only use VA-approved apps for conducting VA business. Go to Resources for a link to view the approved apps list.
- Enable and use Wi-Fi for automatic updates.
- Never allow access requests.

By accepting the ROBs at the end of this course, you are also acknowledging that you have completed the recertification training for your VA mobile device. For any additional information, please review the course Mobile Training: Security of Apps on iOS Devices (VA TMS ID: 3926744).

4.9 Mobile Phone Reminders

Reminders for VA-issued mobile phone users:

- Protect your identity; never send personal information in a text message.
- Treat the personal information of others the same as you would treat your own.
- Follow all VA ROBs and report any suspected or identified incidents to your supervisor, ISSO, and/or PO.
- Limit your personal use of the device as stated in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.
- Connect to VA securely using the Citrix Access Gateway (CAG) and AnyConnect.
The very things that make mobile devices convenient—their size and mobility—also make them susceptible to unauthorized access, loss, and theft. Mobile device users must be familiar with mobile phone recertification, guidelines, and security.

4.10 Summary

Using and working with computer resources is a way of life nowadays. At VA, a majority of employees work with, or use, some kind of computer resource. It could be a desktop, laptop, tablet, and/or mobile device.

Keep the following in mind when using VA computer resources:

- Use only equipment you are authorized to use.
- Secure the equipment when not in use.
- Avoid prohibited activity on your equipment.
- Take mobile device recertification training, as required.
Topic 5: Securing Electronic Data

5.1 Introduction

Because things can move very quickly when we deal with electronic data, it’s important that we stay alert to protect it. You’ll want to create your own path, no matter what situation you’re in. Always operate with integrity.

On this stop of your journey, you will find situations that require you to make the right choices and take appropriate actions when working with electronic data.

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

- Recall how to safeguard electronic VA sensitive information
- Identify how popular technologies and applications can expose VA sensitive information

5.2 Securing Sensitive Information

We are all responsible for staying vigilant in keeping sensitive information safe through strategies like using data protection software, avoiding social engineering attacks, and transmitting sensitive information according to policy.

The scenarios in this section present situations where you will have to make the right choice to protect electronic information.

5.3 Social Engineering/Phishing

Scenario

Peter is an executive at a VA hospital. He got an email that appeared to be from another VA executive asking for staff payroll information. The email seems legitimate because it appears to come from an @va.gov address, and the sender uses correct VA terms, knows Peter’s title, and even mentions people from the HR department by name, but the email subject was tagged as an external email, which seems odd.

Which is the best approach for Peter to take?

Determine the best answer from the options below:

- A. Provide the information to avoid payroll delays.
- B. Verify that individuals listed are actual HR employees. If so, provide the requested information.
- C. Contact your ISSO to report the suspicious email immediately since it was tagged as an external email.

Correct Feedback

The correct answer is C.
Contacting the ISSO is the best approach. The email looked suspicious, and sharing the SPI would affect the whole staff.

This incident was a whaling attack. Whaling is a type of social engineering technique that focuses on a single high-ranking person or a small group of targets.

Social engineering attackers use human interaction to obtain or compromise information about an organization or its systems. These attackers can be insider threats; individuals who charm you into disclosing VA sensitive information.

**Phishing** is also a type of social engineering. It, however, is a fraudulent email technique that appeals to a large group of people to trick some into responding. Phishing attacks seek personal information by posing as a trustworthy organization.

Do not click on any links or open any attachments. Keep in mind that an insider could become an involuntary threat by opening an attachment containing a virus that installs when opened.

Report any suspicious email by taking a screenshot. Send it immediately to your ISSO or directly to the Enterprise Service Desk (ESD) email address at ESD@va.gov. Most importantly, do not forward the email.

**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 will use encryption products approved and provided by VA to protect sensitive data.

- 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.

**Organizational and Non-Organizational Users**

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

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

Scenario

Raul is working off-site at a contractor’s office to help with a project that includes the use and handling of sensitive information. He uses his VA laptop to remotely connect to the VA network and transmits the sensitive information to the designated VA’s Microsoft SharePoint site.

Raul already has his supervisor’s approval and permission to work remotely and store the sensitive information on the site.

Did Raul follow the proper protocol for transmitting the information remotely?

Determine the best answer from the options below:

A. Yes. Raul’s actions were in line with the ROB governing remote work.

B. No. Raul is using his VA computer, which is already secure, so he doesn’t need supervisor’s approval to work remotely and transfer the sensitive data.

Correct Feedback

The correct answer is A.

Raul is following the proper protocol. The ROBs require that Raul get permission from his supervisor to transmit sensitive information when working on sites that VA doesn't own or manage. Since he already obtained his supervisor's approval and permission, he has completed this requirement.

By using his VA-issued laptop, he is ensured that it has the approved Federal Information Processing Standard (FIPS) 140-2 encryption, since all VA devices and equipment are configured that way by VA IT staff.

If Raul happened to be transmitting PII via fax, he would need to ensure that the fax transmissions were sent to the appropriate recipient. To avoid an insider threat, he should confirm that someone is at the machine to receive the fax, or that the receiving machine is in a secure location, and verify any requests for VA sensitive information before releasing it, even if the request seems harmless.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

- I WILL obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)).

- I WILL transmit individually identifiable information via fax only when no other reasonable means exist, and when someone is at the machine to receive the transmission or the receiving machine is in a secure location.
• I WILL ensure fax transmissions are sent to the appropriate destination. This includes double checking the fax number, confirming delivery, using a fax cover sheet with the required notification message included.

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

5.5 Using Email Securely

VA employees and contractors use email constantly to transmit information. We must maintain accountability for our emails, including ensuring sensitive emails are transmitted according to policy, using personal email properly, and more. Protect identities, and never give out personal information over email.

The scenarios in this section present situations involving the use of VA email and how to keep it secure.

5.6 Email Encryption

Scenario

Janet is a VA employee who is trying to send an encrypted email containing PII to her coworker, James. She received a message stating that Outlook could not send the encrypted message because the recipient is not compliant with Public Key Infrastructure (PKI) encryption guidelines. Because the email is important and has an end-of-day deadline, Janet decides to send the message unencrypted.

Has Janet violated the ROBs?

Determine the best answer from the options below:

A. Yes. The message contains sensitive information.

B. No. The message was important and had a pressing deadline.

Correct Feedback

The correct answer is A.

Janet violated the ROB. Emails that contain sensitive information, including attachments, must be encrypted. Since James’ PKI certificates were not compliant, Janet could have used Active Directory Rights Management Service (RMS) encryption.

To do this, go to the File menu in Outlook and select Set Permissions and Encrypt Only.

While it is important to encrypt emails that contain VA sensitive information, you should not encrypt every message. It is your responsibility to determine which emails contain sensitive information that must be encrypted. Encrypting every message is a violation of the ROB.

There are some exceptions. VBA normally defaults the email setting to auto-encrypt to reduce the number of potential incidents related to encryption by VBA users. However, VBA users are still required to unencrypt emails that do not contain sensitive information.
Contact the VA ESD at YourIT https://yourit.va.gov for any questions about encryption.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

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

5.7 Non-official Email for VA Business

Scenario

Sadie is a member of a project team that delivers products to VA under a contract. She doesn’t like using the VA email system and sometimes uses her corporate email to communicate VA business. To avoid using her VA email altogether, she recently set up an auto-forward option so her VA emails go directly to her corporate email account. She feels this the best way for her to get her job done.

Did Sadie violate VA policy?

Determine the best answer from the options below:

A. Yes, she violated VA policy.
B. No, it’s okay for her to auto-forward her VA emails to her corporate email to conduct VA business in a more timely manner.

Correct Feedback

The correct answer is A.

Sadie violated VA policy by auto-forwarding her emails. Messages that are auto-forwarded may not be tracked, which risks violating records management requirements. VA systems have defenses in place to help protect information; outside email systems do not have the same safeguards.

VA issued guidance in 2018 that mandates VA users to use an official email account, if available. But, if a contractor is unable to use the VA email account due to technical constraints, the corporate email account may be used if appropriate encryption and security requirements are met. Non-official email accounts, such as Gmail or Yahoo, are not allowed.

Since Sadie has a VA email address, she should use it to conduct VA business whenever possible. It seems she decided to use her corporate email instead of her VA email as a matter of convenience instead of a technical limitation, which goes against the guidance.

If there are circumstances when you cannot use your official email account, you must ensure proper record-keeping requirements are met by doing one of the following:
Copy the user's official email address with @va.gov as the domain name, so that the message is sent simultaneously to the official account at the moment of transmission.

Forward a complete copy of the message to the user's official email address with @va.gov as the domain name, within 20 days of the official transmission.

The VA email system creates backup copies so VA can track business actions and manage federal records.

Rules of Behavior
Review the associated rules for your user type below.

Organizational Users

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

5.8 Using Appropriate Wireless Access for VA Business

Scenario
Mahalia is a contractor who is implementing a new VA medical system. In order to stay on schedule during the initial phases of implementation, she uses the VA guest wireless network instead of going through the process to connect to the VA network.

Is this an acceptable practice?
Determine the best answer from the options below:

A. Yes, since it is allowing her to do her job.
B. No. VA business should not be conducted via the guest network.

Correct Feedback
The correct answer is B.

This is not an acceptable practice. Working with VA sensitive information on the guest network puts the information at risk for unauthorized disclosure. The guest network is not secured or encrypted. Mahalia should go through the appropriate process to connect the system to VA’s secure network to move forward with her project.

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 will use encryption products approved and provided by VA to protect sensitive data.
• I WILL NOT attempt to override, circumvent, alter or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff.

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

5.9 Summary

Because so much work is done electronically at VA, it’s imperative that the electronic data be protected. Remember to stop and ask for directions when you are unsure of which way to turn or get lost. If you have a question about how to handle electronic data, please contact your ISSO or PO.

Some ways to keep electronic data safe include the following:

• Watch out for social engineering attacks, like phishing and whaling.

• Take appropriate actions when transmitting sensitive information.

• Use email appropriately.
Topic 6: Working Remotely

6.1 Introduction

Working away from VA facilities presents unique hazards and challenges when protecting VA sensitive information and equipment. Be sure to pinpoint anything suspicious, and follow VA guidelines for remote access to minimize the risk.

On this stop of your journey, you will find situations to help you manage your VA-issued devices and accesses while working away from a physical VA location.

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

- Recall how to securely access VA systems when working from a remote location
- Identify how to properly secure VA systems and information when working from a remote location
- Recognize the requirements for protecting VA devices and systems when travelling internationally

6.2 Working Securely from a Remote Location

Anyone working remotely will be responsible for knowing the policies and procedures for securing the remote location, connecting to the network correctly, and safeguarding sensitive information at the remote location.

The scenarios in this section present situations involving working remotely and related security considerations.

6.3 Securing VA Information at Your Remote Location

Scenario

Lashonda is a telework employee. She lives alone and typically works on her VA laptop at the kitchen table. She is finishing up a few last-minute items when her doorbell rings. She lowers her monitor halfway before answering the door. She is surprised to see her best friend, Andrew. Lashonda invites Andrew in and goes to fix them both a snack. When she returns, Andrew has gotten on Lashonda’s computer to check one of his social media accounts.

What should Lashonda have done to ensure her laptop and VA information were secured?

Determine the best answer from the options below:

A. Lock the screen and take her PIV card out of the laptop.
B. Remind Andrew that it's her VA laptop before she leaves the room to fix the snack.
Correct Feedback

The correct answer is A.

Lashonda should lock the screen and take her PIV card out of the laptop. By doing this, Lashonda has protected her GFE from theft, misuse, and potential loss of information.

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

Don’t forget to secure information and devices while teleworking if others are at home with you; this includes your electronic devices as well as any paper documents. Additionally, whether at home or at another remote work location, be sure to protect your log on credentials and process for remote access to VA networks and systems.

Rules of Behavior

Review the associated rules for your user type below.

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 sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel).

• I WILL protect information about remote access mechanisms from unauthorized use and disclosure.

6.4 Safeguarding Sensitive Information at Your Remote Location

Scenario

Raymond teleworks every Friday. On Thursday, he received written permission from his supervisor to transport some documents with VA sensitive information home so he could catch up on a few deadlines.

After he finishes updating the information from the documents to the VA database, he uses his personal shredder to dispose of the material.

Did Raymond take the right action to protect the sensitive information?

Determine the best answer from the options below:

A. No, this puts VA sensitive information at risk.

B. Yes, he didn’t want to risk the sensitive information being accessed over the weekend.
Correct Feedback

The correct answer is A.

Raymond put VA sensitive information at risk. Although Raymond shredded the sensitive information, he failed to protect it, because he used an unauthorized disposal method. To prevent identity theft, only use authorized shredders at VA facilities when disposing of sensitive information.

Raymond should have followed the approved method to protect the material by locking it up and then returning it to the facility for destruction by VA or its information destruction contractor.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

- I WILL safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel).
- I WILL obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)).

6.5 Protecting Information and Systems While on Travel

Travel is common for employees across VA, so we must be prepared to manage VA-issued devices and accesses while working away from a physical VA location.

The scenarios in this section represent what can affect the security of information and systems while on travel.

6.6 Accessing Information From Publicly Available Systems

Scenario

Steven is a VA contractor visiting relatives out of town. He receives a call from a coworker asking for information regarding a patient. Steven does not have his VA laptop, so he goes to the local library to use a public computer to access the CAG.

Is this an acceptable way to access VA systems?

Determine the best answer from the options below:

A. Yes. VA systems can be accessed remotely from any device.
B. No. VA systems should not be accessed on publicly-available computers.
Correct Feedback

The correct answer is B.

Steven should not access VA systems on publicly-available computers.

In this situation, Steven is accessing non-public VA information. He is using his credentials to access internal VA systems through CAG. By accessing these systems on a public computer, Steven is putting VA information at risk.

You should never use a public computer to remotely connect to the internal VA network. You can use public computers to access public information, like www.va.gov.

Rules of Behavior

Review the associated rules for your user type below.

Organizational and Non-Organizational Users

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

6.7 International Travel

Scenario

Leona is going out of the country for a month. She supports several projects, so she wants to keep up with her emails. She plans to take her VA-issued iPhone with her so that she can check her emails.

While she’s traveling and out of the country, Leona is extremely careful to protect her VA iPhone. She is also extremely careful to log in to her phone only when no one can see her VA credentials.

Has Leona followed all the policies that relate to international travel and GFE mobile devices?

Determine the best answer from the options below:

A. Yes. Leona performed all the required behaviors regarding her GFE mobile phone.

B. No. Leona failed to get permission to use her GFE mobile phone prior to her departure out of the country.

Correct Feedback

The correct answer is B.

Leona has not followed the policies relating to international travel and GFE mobile devices.

If you intend to travel internationally with your GFE mobile devices, you must notify your supervisor, ISSO, the local Area Manager, and Information System Owner prior to your departure. You also need to obtain permission to access VA’s internal network while out of the country.
When you return, you must contact your supervisor. Be aware, you may need to provide your GFE to OIT for inspection.

**Rules of Behavior**

Review the associated rules for your user type below.

**Organizational Users**

- I WILL notify my VA supervisor or designee prior to any international travel with a GFE mobile device (e.g. laptop, PDA) and upon return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.

- I WILL exercise a higher level of awareness in protecting GFE mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

- I WILL NOT access VA’s internal network from any foreign country designated as such unless approved by my VA supervisor, ISO*, local CIO*, and Information System Owner.

**Non-Organizational Users**

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

*Note: 1) The Information Security Officer (ISO) role is now referred to as Information System Security Officer (ISSO). 2) The local CIO role is now referred to as local Area Manager.

**6.8 Summary**

At VA, many employees work remotely. This is a great benefit that has the potential to cause serious incidents if not practiced appropriately. If you work remotely, be sure to plot your daily route carefully. Keep the following in mind when working remotely:

- Ensure that your remote location is secure.
- Use secure VA connection protocols.
- Take precautions to ensure sensitive information is protected.
- Obtain permission to access VA systems when traveling internationally.
Topic 7: Reporting Incidents

7.1 Introduction

On your journey, it’s always a best practice to make sure your vehicle is safe and passes inspection—not just for you, but also for everyone you meet along the way. The same rule applies when it comes to protecting your VA access and VA’s sensitive information. Incident reporting is one way to reduce risks associated with violations and threats. Be sure you know what to do and who to call when you suspect an incident has occurred.

On this stop of your journey, you will find a high-level overview of incidents as well as situations that review the incident 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 What Is an Incident?

As you make your way from one place to the next, you subconsciously look out for things or events that could cause harm to you or someone else. A good practice would be to maintain that same type of caution when working with VA sensitive information or systems to avoid an incident.

An incident is an event that threatens to expose the confidentiality, integrity, or availability of an information system and the information it contains and transmits. Incidents threaten privacy and security and potentially affect VA, Veterans, and you.

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

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

Consequences

It makes a difference whether an incident is accidental or intentional. The consequences for intentional acts are more severe than the consequences for accidents.

Serious consequences of privacy and information security violations could include the following:

- Suspension of your access to VA 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 the following:

• Fines of up to $250,000
• Prison for up to 10 years
• Penalties for mishandling records: The maximum penalty for the willful and unlawful destruction, damage, or alienation of federal records is a $2,000 fine, three 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
• More penalties may apply for violating laws protecting PHI

7.3 Steps and Points of Contact

If you notice anything that may put VA sensitive information or information systems at risk, report it.

Step 1. Note the following details:
• What happened?
• Where did it happen?
• When did it happen?
• Who was involved?

Step 2. Report it by doing the following:
• Employees should immediately report suspected or identified incidents to their supervisor and ISSO or PO. If you do not know the name of your 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 Administrative Officer on Duty.
• Contractors should report every incident to their ISSO or PO and also to their COR and Project Manager. All suspected or identified incidents must be reported immediately.
7.4 Recognize and Report an Incident

Scenario

Wanda and Diana are eating lunch when Diana mentions that she received a suspicious external email with an attachment that she wasn’t expecting. Which of the following is the best approach to the occurrence?

Determine the best answer from the options below:

A. Since Diana didn’t open the attachment, she just needs to delete the email immediately.

B. Diana should not open the attachment and should report this to her ISSO or PO. This might be an incident.

Correct Feedback

The correct answer is B.

Diana should not open the attachment and should report it to her ISSO or PO. The email attachment could contain malware, which may infect Diana’s computer and put the network at risk.

The ROBs require you to report suspected or identified incidents to your ISSO or PO immediately upon suspicion.

Rules of Behavior

Review the associated rules for your user type below.

Organizational Users

• I WILL report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor or designee immediately upon suspicion.

Non-Organizational Users

• I WILL report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) on VA information systems to a VA ISO*, local CIO*, and Information System Owner immediately upon suspicion.

*Note: 1) The Information Security Officer (ISO) role is now referred to as Information System Security Officer (ISSO). 2) The local CIO role is now referred to as local Area Manager.
7.5 Summary

Everyone is responsible for reporting suspected incidents to his or her ISSO or PO. Be sure that you know the following:

- How to recognize an incident
- Who to call to report your observation
- How to report an incident
Topic 8: Summary and Rules of Behavior

8.1 Wrap-Up

Privacy and information security is a high priority for everyone. Knowing the basics and using best practices will help you make good choices to prevent incidents and protect VA and Veterans every day.

While working for VA, you might have access to and use of VA information systems, or you have the potential to 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. Be sure to follow all of the ROBs to ensure your compliance.

You may be required to sign specific or unique ROBs for access to or use of specific VA systems, or of a non-VA entity, in addition to these ROBs. While using that system, you must comply with that ROB.

8.2 Acknowledge, Accept, and Comply With the ROBs

Working for VA, you may access and use VA information systems or you may come in contact with VA sensitive information. This means you must accept responsibility for protecting privacy and ensuring information security. The 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.

Read all of the ROBs closely. By accepting and acknowledging the ROBs, you are agreeing to uphold all of 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, sign and date the appropriate ROBs for your user type.

NOTE: There are two versions of the ROBs, one for organizational users and one for non-organizational users.

Organizational users are identified as VA employees, contractors, researchers, students, volunteers, and representatives of federal, state, local, or tribal agencies not representing a Veteran or claimant. This version of the ROB is available in Appendix A.

Non-organizational users include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for onboarding power of attorney/private attorneys. This version of the ROB is available in Appendix B.

Once you have initialed each page and signed the ROB document, you must submit the document to your supervisor or designee for documentation of course completion.

8.3 Completion

Contact your supervisor or COR to submit the signed ROB and to coordinate with your local TMS Administrator to ensure you receive credit for completion.
Appendix A: Department of Veteran Affairs
Information Security Rules of Behavior for Organizational Users

1. COVERAGE
   a. Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) provides the specific responsibilities and expected behavior for organizational users and non-organizational users of VA systems and VA information as required by OMB Circular A-130, Appendix III, paragraph 3a(2)(a) and VA Handbook 6500, Managing Information Security Risk: VA Information Security Program.
   b. Organizational users are identified as VA employees, contractors, researcher, students, volunteers, and representatives of Federal, state, local or tribal agencies.
   c. Non-organizational users are identified as all information system users other than VA users explicitly categorized as organizational users.
   d. VA Information Security ROB does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA’s information or information systems. The VA Information Security ROB provides the minimal rules with which individual users must comply. Authorized users are required to go beyond stated rules using "due diligence" and the highest ethical standards.

2. COMPLIANCE
   a. Non-compliance with VA ROB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include restricting access, suspension of access privileges, reprimand, demotion and suspension from work. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may result in criminal sanctions.
   b. Unauthorized accessing, uploading, downloading, changing, circumventing, or deleting of information on VA systems; unauthorized modifying VA systems, denying or granting access to VA systems; using VA resources for unauthorized use on VA systems; or otherwise misusing VA systems or resources is strictly prohibited.

3. ACKNOWLEDGEMENT
   a. VA Information Security ROB must be signed before access is provided to VA information systems or VA information. The VA ROB must be signed annually by all users of VA information systems or VA information. This signature indicates agreement to adhere to the VA ROB. Refusal to sign VA Information Security ROB will result in denied access to VA information systems or VA information. Any refusal to sign the VA Information Security ROB may have an adverse impact on employment with VA.
   b. The ROB may be signed in hard copy or electronically. If signed using the hard copy method, the user should initial and date each page and provide the information requested under Acknowledgement and Acceptance. For Other Federal Government Agency users, documentation of a signed ROB will be provided to the VA requesting official.
4. INFORMATION SECURITY RULES OF BEHAVIOR

Access and Use of VA Information Systems

I Will:

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

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data. SOURCE: AC-6
- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8
- Have a VA network connection and a non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any device at the same time unless the dual connection is explicitly authorized. SOURCE: AC-17 (k)
- Host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner, local CIO, or designee and approved by my ISO. SOURCE: AC-18
Protection of Computing Resources

I Will:

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

I Will Not:

• Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee. SOURCE: MP-4

• Attempt to override, circumvent, alter or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff. SOURCE: CM-3

Electronic Data Protection

I Will:

• Only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA. SOURCE: SI-3

• Safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using FIPS 140-2 validated encryption (or its successor) unless it is not technically possible. This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)). SOURCE: SC-13

• Only use devices encrypted with FIPS 140-2 (or its successor) validated encryption. VA owned and approved storage devices/media must use VA's approved configuration and security control requirements. SOURCE: SC-28

• Use VA e-mail in the performance of my duties when issued a VA email account. SOURCE: SC-8

• Obtain approval prior to public dissemination of VA information via e-mail as appropriate. SOURCE: SC-8

I Will Not:

• Transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption. SOURCE: AC-18

• Auto-forward e-mail messages to addresses outside the VA network. SOURCE: SC-8

• Download software from the Internet, or other public available sources, offered as free trials, shareware; or other unlicensed software to a VA- owned system. SOURCE: CM-11

• Disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store or use VA information. SOURCE: CM-10
Teleworking and Remote Access

I Will:

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

I Will Not:

- Access non-public VA information technology resources from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library. SOURCE: AC-17
- Access VA’s internal network from any foreign country designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner. SOURCE: AC-17

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames, and complete any additional role-based security training required based on my role and responsibilities. SOURCE: AT-3
- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. SOURCE: AU-1
• Have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand. SOURCE: MA-2

• Permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software. SOURCE: MA-5

• Sign specific or unique ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity's ROB to conduct VA business. While using their system, I must comply with their ROB. SOURCE: PL-4

Sensitive Information

I Will:

• Ensure that all printed material containing VA sensitive information is physically secured when not in use (e.g., locked cabinet, locked door). SOURCE: MP-4

• Only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. SOURCE: UL-2

• Recognize that access to certain databases 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. SOURCE: UL-2

• Obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)). SOURCE: UL-2

• Protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use encryption products approved and provided by VA to protect sensitive data. SOURCE: SC-13

• Transmit individually identifiable information via fax only when no other reasonable means exist, and when someone is at the machine to receive the transmission or the receiving machine is in a secure location. SOURCE: SC-8

• Encrypt email, including attachments, which contain VA sensitive information. SOURCE: SC-8

• Protect SPI aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function. SOURCE: SC-28

• Ensure fax transmissions are sent to the appropriate destination. This includes double checking the fax number, confirming delivery, using a fax cover sheet with the required notification message included. SOURCE: SC-8
I Will Not:

- Disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals. SOURCE: IP-1

- Allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance by my VA supervisor, ISO, and Information System Owner, local CIO, or designee. SOURCE: AC-20

- Make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to, e-mail, instant messaging, online chat, and web bulletin boards or logs. SOURCE: SC-8

- Encrypt email that does not include VA sensitive information or any email excluded from the encryption requirement. SOURCE: SC-8

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. SOURCE: IA-5 (1)

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

I Will Not:

- Store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption, and I am the only person who can decrypt the file.

- Hardcode credentials into scripts or programs. SOURCE: IA-5 (1) (c)

Incident Reporting

I Will:

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

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

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

________________________________ ____________________________/___/___
Print or type your full name  Signature   Date(month/day/year)

________________________________ ____________________________
Office Phone                  Position Title
Appendix B: Department of Veteran Affairs
Information Security Rules of Behavior for Non-Organizational Users

1. COVERAGE


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

c. Non-organizational users are identified as all information system users other than VA users explicitly categorized as organizational users. These include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for on-boarding power of attorney/private attorneys.

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

e. The VA ROB for Non-Organizational Users does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA’s information or information systems. The ROB simply provides the minimum standards with which individual users must comply, and VA facilities and other agency components may issue standards for protection that exceed the ROB. In addition, authorized users are required to go beyond stated rules using due diligence and the highest ethical standards.

2. COMPLIANCE

a. Non-compliance with the VA ROB for Non-Organizational Users may be cause for suspension or removal of access to VA information or information systems. Such a suspension would not prevent the authorized disclosure of records to an individual; however, it may prevent disclosure through a particular method, e.g., by suspending access through a VA information system. Depending on the severity of the violation and management discretion, consequences may include restricting access or suspension of access privileges. Theft, conversion, or unauthorized access, disposal, or destruction of Federal property or disclosure of information may result in criminal sanctions.
b. Accessing, uploading, downloading, changing, circumventing, or deleting of information on VA systems without authorization; modifying VA systems, denying or granting access to VA systems without authorization; using VA resources for unauthorized purpose on VA systems; or otherwise misusing VA systems or resources is strictly prohibited and may result in criminal sanctions.

c. The VA ROB for Non-Organizational Users does not create any other right or benefit, substantive or procedural, enforceable by law by a party in litigation with the U.S. Government.

3. ACKNOWLEDGEMENT

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

b. The VA ROB for Non-Organizational Users may be signed in hard copy or electronically. If signed using the hard copy method, the user should initial and date each page and provide the information requested under Acknowledgement and Acceptance.

4. INFORMATION SECURITY RULES of BEHAVIOR

Access and Use of VA Information Systems

I Will:

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

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data. SOURCE: VA Handbook 6500 Control AC-6
- Use personally-owned equipment on-site at a VA facility to directly connect to the VA network, or connect remotely to the VA network unless approved prior to use (i.e.,
Protection of Computing Resources

I Will:

• Protect Government Furnished Equipment (GFE) from theft, loss, destruction, misuse, and threats. SOURCE: VA Handbook 6500 Control AC-17

• Follow VA policies and procedures for handling Federal Government IT equipment and sign for items provided to me for my exclusive use and return them when no longer required for VA activities. SOURCE: VA Handbook 6500 Control CM-8(4)

I Will Not:

• Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee. SOURCE: VA Handbook 6500 Control MP-4

• Attempt to override, circumvent, alter, or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff. SOURCE: VA Handbook 6500 Control CM-3

Electronic Data Protection

I Will:

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

I Will Not:

• Download or install prohibited software from the Internet, or other publicly available sources, offered as free trials, shareware, or other unlicensed software to a VA-owned system. SOURCE: VA Handbook 6500 Control CM-11

• Disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store, or use VA information. SOURCE: VA Handbook 6500 Control CM-10

Remote Access

I Will:

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

I Will Not:

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

Access any VA information system from
User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames. SOURCE: VA Handbook 6500 Control AT-3
- Complete any additional role-based security training required based on my role and responsibilities. SOURCE: VA Handbook 6500 Control AT-3
- I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. SOURCE: VA Handbook 6500 Control AU-1
- If applicable, have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon request. SOURCE: VA Handbook 6500 Control MA-2
- Permit only those authorized by OI&T to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software. SOURCE: VA Handbook 6500 Control MA-5
- Sign specific or unique ROBs as required for access or use of specific VA systems or non-VA systems. SOURCE: VA Handbook 6500 Control PL-4

Sensitive Information

I Will Not:

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

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. SOURCE: VA Handbook 6500 Control IA-5(1)
- Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure. SOURCE: VA Handbook 6500 Control IA-5(h)
I Will Not:

- Store my VA passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption, and I am the only person who can decrypt the file. SOURCE: VA Handbook 6500 Control IA-5

- Hardcode credentials into scripts or programs. SOURCE: VA Handbook 6500 Control IA-5(1)(c)

- Divulge a personal username, password, access code, verify code, or other access credential to anyone. SOURCE: VA Handbook 6500 Control AC-17

Incident Reporting

I Will:

- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) on VA information systems to a VA ISO, local CIO, and Information System Owner immediately upon suspicion. SOURCE: VA Handbook 6500 Control IR-6
5. ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of the VA Information Security Rules of Behavior for Non-Organizational Users.

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

__________________________  __________________  __/__/ 
Print or type your full name    Signature             Date (month/day/year)

__________________________  ____________________________
Office Phone                  Position Title
Appendix C: Glossary

DISCLAIMER: Please note that there may be links (or references to links) that are external to the Department of Veterans Affairs (VA) network.

There are links in the Resources page that may be of interest to our users. 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.

A

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

Source: Microsoft and VHA Handbook 1907.01

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

**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.


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: 38 U.S.C. § 5727

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

B – N/A
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.


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

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

Source: 38 U.S.C. § 5727

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

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

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

Source: Adapted from VA Handbook 6300.1

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

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

Source: Adapted from VA Directive 6502, VA Handbook 6502.1

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

Divulge—To disclose or reveal (something private, secret, or previously unknown).

Source: www.dictionary.com

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

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.

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.

Source: Adapted from NIST Standards, http://csrc.nist.gov/groups/STM/cmvp/standards.html

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

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

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

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/

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.
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/

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

Source: 15 USC 1681a

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

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

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

Insider Threat—A current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.

Source: https://www.us-cert.gov/sites/default/files/publications/Combating the Insider Threat_0.pdf

Instagram—A web-based photo sharing site. Users share images, graphics, photos, and short videos with friends.
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: 38 U.S.C. § 5727

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

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.

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

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

Non-Organizational Users—Are identified as all information system users other than VA users explicitly categorized as organizational users. These include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for onboarding power of attorney/private attorneys.

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

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

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

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

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

Password—A word or group of characters that is used to gain entry to an electronic system. A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.
Source: NIST IR 7298, Glossary of Key Information Security Terms

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

Password Requirements—Passwords must contain at least eight non-blank characters. They must contain characters from 3 of the following 4 categories: English 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 3 of the 4 categories as outlined above. When changing a password, four characters must be changed from the old password to the new password. The same password should not be used if it has been used within the past two years.

Source: 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.


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

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

Source: https://www.va.gov/pivproject/

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

Personally Identifiable Information (PII)—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)

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.


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

Source: Adapted from http://www.justice.gov/opcl/privacyact1974.htm

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
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

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

Source: FIPS 196

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

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

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

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

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

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 offers 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
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)

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

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

Text Messages—The sending of short text messages electronically, especially from one cell phone to another.

Source: www.merriam-webster.com

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

Source: NIST SP 800-53 rev 4

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

Two-Factor Authentication—Multifactor Authentication requires the use of two or more different factors to achieve authentication. The factors are defined as (i) something you know (e.g., password,
personal identification number); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Source: VA Handbook 6500.

Second definition: The process of establishing confidence in the identity of users or information systems through two factors. The two factors are something the user knows and something the user has. Source: Adapted from NIST Special Publication 800-63-2, Electronic Authentication Guideline

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. 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 data” means all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

Source: Adapted from 38 U.S.C. Section 5727

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.

Source: Adapted from http://compnetworking.about.com/cs/wireless/f/whatiswireless.htm

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

X – N/A

Y

YouTube—The name of a website on which users can post, view, or share videos.

Source: Adapted from Youtube (n.d.) and Dictionary.com (accessed May 15, 2017)

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

Z – N/A
Appendix D: Privacy and Information Security Resources

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

Table 1. VA Phone Numbers

<table>
<thead>
<tr>
<th>Identity Theft Help Line</th>
<th>(855) 578-5492</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Inspector General (IG) Hotline</td>
<td>(800) 488-8244</td>
</tr>
<tr>
<td>VA Enterprise Service Desk</td>
<td>(855) 673-4357</td>
</tr>
</tbody>
</table>

Table 2. VA Web Links

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ITWD’s role-based training*</td>
<td><a href="http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Pages/default.aspx">http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Pages/default.aspx</a></td>
</tr>
<tr>
<td>Locator to identify ISSOs* and POs*</td>
<td><a href="https://vaww.portal2.va.gov/sites/infosecurity/index.aspx">https://vaww.portal2.va.gov/sites/infosecurity/index.aspx</a></td>
</tr>
</tbody>
</table>
Table 2. VA Web Links

<table>
<thead>
<tr>
<th>Remote access solutions*</th>
<th><a href="https://vpnportal.vansoc.va.gov/Default.aspx">https://vpnportal.vansoc.va.gov/Default.aspx</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Help Site &gt; Rights Management Service (RMS)*</td>
<td><a href="http://vaww.help.portal.va.gov/">http://vaww.help.portal.va.gov/</a></td>
</tr>
<tr>
<td>VA Knowledge Service*</td>
<td><a href="https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/Pages/Home.aspx">https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/Pages/Home.aspx</a></td>
</tr>
<tr>
<td>Mobile Documentation &gt; Procedures*</td>
<td><a href="https://vaww.eie.va.gov/SysDesign/CS/MT/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2FSysDesign%2fCS%2fMT%2fShared%20Documents%2fProcedures&amp;FolderCTID=0x012000CE74B1C730FD694FA9DF56B69E70282500E0245BBF72BEE8C4F93592E1B9ACC2EF3&amp;View=%7B08212D1F-F3A2-4E22-8328-44594CA55E2%7D">https://vaww.eie.va.gov/SysDesign/CS/MT/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2FSysDesign%2fCS%2fMT%2fShared%20Documents%2fProcedures&amp;FolderCTID=0x012000CE74B1C730FD694FA9DF56B69E70282500E0245BBF72BEE8C4F93592E1B9ACC2EF3&amp;View={08212D1F-F3A2-4E22-8328-44594CA55E2}</a></td>
</tr>
<tr>
<td>Project Help Site &gt; Rights Management Service (RMS)*</td>
<td><a href="http://vaww.help.portal.va.gov/">http://vaww.help.portal.va.gov/</a></td>
</tr>
</tbody>
</table>

* Only accessible on the VA Intranet

Table 3. VA TMS Courses

<table>
<thead>
<tr>
<th>Privacy and HIPAA Training (VA TMS ID: 10203)</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Introduction to Rights Management Service—RMS (VA TMS ID: 336914)</td>
</tr>
<tr>
<td>Getting Started with Public Key Infrastructure (VA TMS ID: 1256927)</td>
</tr>
<tr>
<td>VA Telework Training Module for Employees (VA TMS ID: 1367006)</td>
</tr>
<tr>
<td>Social Networking and Security Awareness (VA TMS ID: 2626967)</td>
</tr>
<tr>
<td>Identity Theft and Prevention (VA TMS ID: 3591967)</td>
</tr>
<tr>
<td>Mobile Training: Security of Apps on iOS Devices (VA TMS ID: 3926744)</td>
</tr>
</tbody>
</table>
Table 4. Privacy and Information Security Laws and Regulations

<table>
<thead>
<tr>
<th>Law/Merch</th>
<th>Description</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of Information Act (FOIA)</td>
<td>Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions.</td>
<td><a href="https://www.foia.gov/">https://www.foia.gov/</a></td>
</tr>
<tr>
<td>Health Information Technology for Economic and Clinical Health Act (HITECH)</td>
<td>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.</td>
<td><a href="https://www.healthit.gov/policy-researchers-implementers/health-it-legislation">https://www.healthit.gov/policy-researchers-implementers/health-it-legislation</a></td>
</tr>
<tr>
<td>Paperwork Reduction Act</td>
<td>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.</td>
<td><a href="https://www.epa.gov/laws-regulations/summary-paperwork-reduction-act">https://www.epa.gov/laws-regulations/summary-paperwork-reduction-act</a></td>
</tr>
<tr>
<td>Privacy Act of 1974</td>
<td>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.</td>
<td><a href="https://www.justice.gov/opcl/privacy-act-1974">https://www.justice.gov/opcl/privacy-act-1974</a></td>
</tr>
<tr>
<td>Federal Information Security Modernization Act (FISMA)</td>
<td>Requires federal agencies to have a program to assess risk and protect information and information security assets that support agency operations.</td>
<td><a href="http://www.dhs.gov/files/programs/gc_1281971047761.shtm">http://www.dhs.gov/files/programs/gc_1281971047761.shtm</a></td>
</tr>
</tbody>
</table>
Table 4. Privacy and Information Security Laws and Regulations


<table>
<thead>
<tr>
<th>Title 38 U.S.C. § 5701: Confidential Nature of Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about any claims processed by VA must be kept confidential.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title 38 U.S.C. § 5705: Confidentiality of Medical Quality Assurance Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information generated during a medical quality assurance program may not be disclosed except when authorized.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title 38 U.S.C. § 7332: Confidentiality of Certain Medical Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 5. Selected VA Privacy Handbooks and Directives

Available at [https://www.va.gov/vapubs/](https://www.va.gov/vapubs/)

<table>
<thead>
<tr>
<th>Directive/Handbook</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Directive 6066</td>
<td>Protected Health Information (PHI) and Business Associate Agreements Management</td>
</tr>
<tr>
<td>VA Directive 6300</td>
<td>Records and Information Management</td>
</tr>
<tr>
<td>VA Handbook 6300.1</td>
<td>Records Management Procedures</td>
</tr>
<tr>
<td>VA Handbook 6300.4</td>
<td>Procedures for Processing Requests for Records Subject to the Privacy Act</td>
</tr>
<tr>
<td>VA Handbook 6300.5</td>
<td>Procedures for Establishing and Managing Privacy Act System of Records</td>
</tr>
<tr>
<td>VA Handbook 6300.6</td>
<td>Procedures for Releasing Lists of Veterans’ and Dependents’ Names and Addresses</td>
</tr>
<tr>
<td>VA Handbook 6500.1</td>
<td>Electronic Media Sanitization</td>
</tr>
<tr>
<td>VA Handbook 6500.2</td>
<td>Management of Breaches Involving Sensitive Personal Information</td>
</tr>
<tr>
<td>VA Handbook 6500.10</td>
<td>Mobile Device Security Policy</td>
</tr>
<tr>
<td>VA Handbook 6502</td>
<td>VA Enterprise Privacy Program</td>
</tr>
<tr>
<td>VA Handbook 6502.1</td>
<td>Privacy Event Tracking</td>
</tr>
<tr>
<td>VA Handbook 6512</td>
<td>Secure Wireless Technology</td>
</tr>
<tr>
<td>VA Handbook 6609</td>
<td>Mailing of Sensitive Personal Information</td>
</tr>
<tr>
<td>VA Handbook 1173.08</td>
<td>Medical Equipment and Supplies</td>
</tr>
<tr>
<td>VA Handbook 1907.01</td>
<td>Health Information Management and Health Records</td>
</tr>
</tbody>
</table>

Available at [https://www.va.gov/vhapublications/index.cfm](https://www.va.gov/vhapublications/index.cfm)
**Table 6. Additional Selected VA Handbooks and Directives**

Available at [https://www.va.gov/vapubs/](https://www.va.gov/vapubs/)

<table>
<thead>
<tr>
<th>Directive/Handbook</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Directive 0701, Office of Inspector General Hotline Complaint Referrals</td>
<td></td>
</tr>
<tr>
<td>VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology</td>
<td></td>
</tr>
<tr>
<td>VA Directive 6515, Use of Web-Based Collaboration Technologies</td>
<td></td>
</tr>
<tr>
<td>VA Handbook 5011/5, Hours of Duty and Leave</td>
<td></td>
</tr>
<tr>
<td>VA Handbook 5011/26, Hours of Duty and Leave (Telework)</td>
<td></td>
</tr>
<tr>
<td>VA Handbook 5021/3, Employee/Management Relations</td>
<td></td>
</tr>
<tr>
<td>VA Handbook 5021.6, Appendix A, Employee/Management Relations</td>
<td></td>
</tr>
<tr>
<td>VA Handbook 6500, Appendix F, VA System Security Controls</td>
<td></td>
</tr>
<tr>
<td>VA Handbook 6500.6, Contract Security</td>
<td></td>
</tr>
<tr>
<td>Table 7. VA Forms and Memorandums</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Available at <a href="http://vaww.va.gov/vaforms/">http://vaww.va.gov/vaforms/</a></td>
<td></td>
</tr>
<tr>
<td>VA Form 0244, <em>Records Transmittal and Receipt</em></td>
<td></td>
</tr>
<tr>
<td>VA Form 7468, <em>Request for Disposition of Records</em></td>
<td></td>
</tr>
<tr>
<td>VAIQ 7581492, <em>Use of Personal Email</em></td>
<td></td>
</tr>
<tr>
<td>VAIQ 7633050, <em>Mandatory Use of PIV Card Authentication for VA Information System Access</em></td>
<td></td>
</tr>
<tr>
<td>Available at <a href="https://vaww.visn15.portal.va.gov/stl/sitedirectory/stl-RecordsManagement/Shared%20Documents/Proper%20Use%20of%20Email%20Memo.pdf">https://vaww.visn15.portal.va.gov/stl/sitedirectory/stl-RecordsManagement/Shared%20Documents/Proper%20Use%20of%20Email%20Memo.pdf</a></td>
<td></td>
</tr>
<tr>
<td>VAIQ 7850460, <em>Proper Use of Email and Other Messaging Services</em>, January 2, 2018</td>
<td></td>
</tr>
</tbody>
</table>

*The links in Table 7 are only accessible on the VA Intranet*