VA Privacy and Information Security Awareness and Rules of Behavior

# Making the Connection

FY17 Text-Only Course Transcript

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

# Table of Contents

# Purpose of This Document

This text-only course transcript was designed to accommodate users in any of these circumstances:

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

This version of the *VA Privacy and Information Security Awareness and Rules of Behavior Text-Only Course Transcript* is valid for fiscal year (FY) 2017 (i.e., October 2016 through September 2017).

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

1. Print and sign the Information Security Rules of Behavior (ROB), as well as initial each page in the space provided
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 more detailed information and the knowledge checks 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.**

# Module 1: Welcome

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

## Who Must Take This Course

This course is all about making a connection between your knowledge and the things you can do every day to make a difference for Veterans. VA must comply with federal laws about privacy and information security. Everyone who comes in contact with information and information systems at VA has a duty to protect privacy and ensure information security.

This course will help you understand your roles and responsibilities for protecting VA information. You must complete this training to use or gain access to VA information or information systems. To maintain your access, you must complete this training each year.

Those who use VA information or VA information systems must take this training, including:

### *Organizational users*

Organizational users are identified as VA employees, contractors, researcher, students, volunteers, and representatives of Federal, state, local or tribal agencies.

### *Non-organizational users*

Non-organizational users are identified as all information system users other than VA users explicitly categorized as organizational users.

There are some exceptions to users who must take this training:

### *Students or other trainees*

If you are a health professions trainee (i.e., student, intern, resident, or fellow), you are not required to complete this course, but you must complete the course VHA Mandatory Training for Trainees-Refresher (VA TMS ID: 3192008).

### *VHA and VBA employees and contractors*

If you have access to Protected Health Information (PHI), you are also required to complete the Privacy and HIPAA Focused Training (VA TMS ID: 10203).

### Rules of Behavior (ROB)

**1. COVERAGE**

1b. Organizational users are identified as VA employees, contractors, researcher, students, volunteers, and representatives of Federal, state, local or tribal agencies.

1c. Non-organizational users are identified as all information system users other than VA users explicitly categorized as organizational users.

**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

**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

## Federal Requirements

Many laws require privacy and information security training, including:

- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)

Many other federal laws are related to privacy, records and information management, and information security, including:

- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Federal Records Act of 1950
- Freedom of Information Act (FOIA)

You can find more information in Appendix C, Privacy and Information Security Resources.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**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

## Course Objectives

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 be aware of these risks at all times and be ready to protect sensitive information and systems.

When you have finished this course, you will be able to:

- Identify the types of VA information and information systems you are required to protect
- Recall the steps you must take to protect personal privacy, VA sensitive information, and information security
- Recognize the penalties you may face for failing to protect privacy and security
- Identify incidents and recall the process for reporting incidents that can compromise or possibly impact privacy and security
- Acknowledge, accept, and comply with the ROB

You will be able to make the connection between your actions and the confidence Veterans can feel toward VA. You make that confidence connection for Veterans by knowing the Rules of Behavior and remembering to follow them.

### Rules of Behavior

**1. COVERAGE**

1a. Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) provides the specific responsibilities and expected behavior for organizational users and non-organizational users of VA systems and VA information as required by 0MB Circular A-130, Appendix Ill, paragraph 3a(2)(a) and VA Handbook 6500, Managing Information Security Risk: VA Information Security Program.

1d. 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.

**3. ACKNOWLEDGEMENT**

3a. 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.

**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

# Module 2: Privacy and Security Basics

## Objectives

Veterans and their families depend on you to protect their privacy and personal information. Becoming aware of the risks and threats to privacy and information security is the first step to keeping Veterans' trust in VA.

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

- Recall the types of VA sensitive information
- Identify basic ways to protect VA sensitive information

## Privacy and Information Security Requirements

You have a responsibility to protect privacy and maintain information security. Information security is a set of principles and actions that ensure VA information systems and VA sensitive information are only accessed by authorized people or systems and are available when you need them.

You must protect all types of VA sensitive information when you are:

- Talking with others
- Handling paper documents or electronic files
- Using email and other types of electronic messaging
- Using VA systems
- Using electronic equipment and devices
- Using information technologies, such as the Internet and social media

You are required to uphold these responsibilities and follow the law. You are also required to report whenever you suspect or notice these requirements are not being followed. If you do not follow the rules and report incidents, you could face penalties, have to pay fines, lose your job, or even face prison time.

### Penalties

Privacy Act penalties include up to $5,000 in fines and a year in prison per violation. HIPAA violations may result in fines from $100 to $1.5 million and jail time. FISMA noncompliance can result in loss of funding and contracts.

These three concepts are important: confidentiality, integrity, and availability.

### Confidentiality

Confidentiality means information must not be disclosed to people who do not have permission or legal authority to know it. For example, VA sensitive information should not be made public.

### Integrity

Integrity means all VA sensitive information is kept from being damaged, destroyed, or improperly changed.

### Availability

Availability means people with permission can access information, information systems, and networks when they need them.

### Rules of Behavior

**2. COMPLIANCE**

2a. 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.

2b. 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.

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will Not:***

- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8

**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

## Types of VA Sensitive Information

It is your responsibility to protect privacy. That means you do not disclose, alter, or destroy VA sensitive information unless you have permission from your supervisor, Privacy Officer (PO), Information Security Officer (ISO), or records management official. Veterans are counting on you.

### Personally Identifiable Information (PII) and Sensitive Personal Information (SPI)

Personally Identifiable Information (PII), also called Sensitive Personal Information (SPI), refers to information about a specific person, such as:

- Name, home address, and home phone number
- Social Security number
- Date of birth
- Credit card numbers
- Education records
- Financial records
- Criminal and employment histories

### Protected Health Information (PHI)

Protected Health Information (PHI) includes health records or payment information linked to a specific person, such as:

- Patient medical records
- Patient appointment reminders
- Patient diagnoses
- Patient test results
- Patient payment history

### Regulatory or program-specific information

Regulatory or program-specific information is information that may not be released or may only be released in certain situations. This category of information would not normally be released to the public. Examples include:

- Certain medical quality assurance records
- Names and addresses of active duty members, Veterans, and their dependents

- VA information technology (IT) internal systems information revealing information about how systems are set up. Examples include framework used for servers, desktops, and networks; application name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission, business use, or need
- Federal records of information compiled for law enforcement purposes (civil, criminal, or military law)

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

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

***I Will Not:***

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

## Federal Records

The Federal Records Act of 1950 and later regulations require federal agencies to create and maintain federal records. Federal records document the business activities of the organization or agency. They are federal property and must be managed and maintained in accordance with the prevailing law.

VA sensitive information may be found in federal records, which have specific handling requirements. Federal records may be kept in a variety of formats. Federal records that contain VA sensitive information must be handled with care.

Each work unit within VA must create and maintain a listing of records known as a file plan or records inventory. Federal records must be kept according to a Records Control Schedule (RCS) or General Records Schedule (GRS).

Designated records management officials manage federal records across VA administrations and facilities. Work with your locally designated records management official if you are creating, transporting, storing, or disposing of records to be sure VA sensitive information is protected.

Find more information about federal records in in Appendix C, Privacy and Information Security Resources.

### Records

Records, as defined by 44 U.S.C., 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. It 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.

### RCS or GRS

Federal records must be kept according to an RCS that is approved by the National Archives and Records Administration (NARA). The RCS provides the retention and disposition rulings for all scheduled federal records listed in the RCS. The GRS is a records schedule that applies to all federal agencies within the U.S. Government. These include retentions and disposition ruling for common records within the government.

| Knowledge Check: Types of VA Sensitive Information |
| --- |
| Consider the following question by selecting the best answer. |
| Which of the following VA sensitive information examples represents PII?<br>A. Medical program quality assurance records<br>B. Framework used for servers<br>C. An employee's Social Security number<br>D. A VA computer network diagram |
| The correct answer C. An employee's Social Security number is an example of PII. Remember to protect all types of VA sensitive information. |

### Rules of Behavior

**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

## Continuous Readiness in Information Security Program

It is your responsibility to keep VA sensitive information safe wherever you are working. VA's Continuous Readiness in Information Security Program (CRISP) highlights what to do to protect VA sensitive information:

- Follow all information security and privacy policies and procedures and the ROB
- View, access, and collect only the information you need to do your job
- Encrypt emails containing VA sensitive information
- Do not talk about VA sensitive information in public
- Do not share VA sensitive information with anyone who should not have it or does not have a need to know or legal authority

### Rules of Behavior

**1. COVERAGE**

1d. 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.

### More Information

CRISP is a program that incorporates security and privacy into everyone's daily functions and promotes ongoing security and privacy practices for VA's environment.

## Passwords

To protect your VA-issued devices and your access to VA sensitive information, follow VA's password requirements.

Strong passwords meet VA's minimum password requirements. Weak passwords contain easy-to-guess information such as Password1 or Password 2, your user name, your first or last name, dictionary words, or phrases similar to your previous passwords.

### VA's Password Requirements

Your password must have at least eight characters and must include at least three of the following:

- Capital letters (A, B, C, etc.)
- Lowercase letters (a, b, c, etc.)
- Numbers (0–9)
- Special characters (such as @, #, $, %)

Other guidelines for passwords include:

- Do not reuse a password that has been used within your last three password changes
- Change your password every 90 days or as required
- Change your password if you suspect your log-in has been compromised
- If you think your password has been compromised, report it

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

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

## Personal Identity Verification

A Personal Identity Verification (PIV) card, also known as a PIV badge, is an identification (ID) card that enables access to VA buildings, networks, and resources.

Protect PIV cards from loss or theft by following these tips:

- Always keep your PIV card with you by attaching it to something on you, such as a lanyard around your neck
- Make a habit of checking for it whenever you leave a room
- Never leave your PIV card in your computer
- Be extra careful when you are in a public place
- If you lose your PIV card or find a lost PIV card, report it to VA security and law enforcement, the ISO, and your management to ensure it is revoked in the system immediately

VA has adopted a two-factor authentication approach to control access to information systems. You must use your PIV card for access to information and information systems unless there is a legitimate exemption. PIV cards comply with FIPS 201 and related guidance.

## Making the Connection: Natalie's Story

### Keeping PIV cards safe

I went to the VA Medical Center for a checkup last week. In the cafeteria, one of those badges the employees use was just lying there on the lunch table.

I wondered…could someone use that card to get at my personal information? Should I be worried?

Just as I sat down, the employee who had left the card came back to pick it up. He told me VA has security measures to prevent an intruder from getting to my information, even if he or she had that card…things like passwords, permissions to use networks, and other ways to make sure my information is safe. I'm glad to know VA takes my privacy seriously!

Veterans form impressions from the situations they witness where information may be at risk. Any situation can be an opportunity to improve understanding.

## What Is Two-Factor Authentication?

PIV cards are part of the two-factor authentication approach that VA has adopted to control access to information systems. The first element of two-factor authentication is something you have, such as your PIV card that can be scanned for access to VA buildings, networks, and resources.

The second element is something you know, such as your Personal Identification Number (PIN) to access information systems. For example, each time you log on to your computer, you insert a PIV card into the card reader and provide your PIN in order to establish a network connection.

If a device does not have a PIV card reader, VA offers the SafeNet MobilePASS application for VA Citrix Access Gateway (CAG) remote access, which installs a software token on the device. The device with the registered token becomes the something you have.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will:***

- Follow established procedures for requesting access to any VA computer system and for notifying my VA supervisor or designee when the access is no longer needed. SOURCE: AC-2

## Securing Paper and Electronic Files

Secure files with VA sensitive information when you are not using them. Follow these guidelines to keep them safe:

- Lock computer screens and VA-issued devices when you are not using them
- Keep paper files in locked cabinets or drawers
- Follow records management guidance when handling documents and files that are records
- Encrypt electronic files, such as emails with VA sensitive information, as required
- Do not transmit messages or attachments containing PHI, PII, or VA sensitive information through mobile text message or unapproved instant messaging (IM) systems
- If you see or find files containing VA sensitive information that are not secured properly, secure them and report it

### Rules of Behavior

**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
- Log out of all information system at the end of each workday. SOURCE: AC-11
- Log off or lock any VA computer or console before walking away. SOURCE: AC-11

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

***I Will Not:***

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

## Who Can Help?

You can reach out to any of the following for help complying with regulations.

### Supervisors

Supervisors are responsible for protecting VA sensitive information and information systems in the following ways:

- Ensure staff understand IT security and privacy information protection issues
- Ensure staff comply with security and privacy regulations and policies
- Ensure staff only have access within the scope of their duties
- Verify staff complete all privacy and security information security training requirements
- Ensure staff sign the ROB each year
- Help staff report identified privacy and information security incidents

### Contracting Officers (COs) or Contracting Officer Representatives (CORs)

Contracting Officers (COs) or Contracting Officer Representatives (CORs) are responsible for these actions to protect VA sensitive information and information systems:

- Ensure contractors sign the ROB each year if required by the contract
- Maintain the original or a copy of the signed ROB (Some CORs may require paper copies in addition to the electronic acknowledgment at the end of this course)
- Ensure contractors complete required privacy and information security awareness training before they begin the contract and for each year of the contract
- Ensure contractors know when and how to report security and privacy incidents

### Privacy Officers (POs)

Privacy Officers (POs) have these responsibilities to protect VA sensitive information and information systems:

- Promote privacy awareness
- Communicate privacy training requirements and deadlines

- Ensure compliance with federal privacy laws and regulations and VA directives, handbooks, and other guidance
- Respond to, investigate, and report privacy incidents
- Provide support when incidents occur
- Coordinate and collaborate to ensure training is completed
- Coordinate with ISOs and System Managers to ensure that data and associated risks are identified and documented in Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) submissions

Note: See Appendix D, Privacy and Information Security Resources for a link to the PO Locator to identify the PO for your location.

### Rules of Behavior

**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
- 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

**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

## Connecting Points

Here are the connecting points you can recall to protect VA privacy and VA sensitive information:

- Protect VA sensitive information, which includes PHI, PII, and regulatory or program-specific information
- Reach out to your supervisor, CO, PO, or ISO to help you comply with policies and regulations

- Follow the ROB to protect privacy and ensure security of VA sensitive information and information systems

# Module 3. Risks in the Digital Age

## Objectives

Technologies in the digital age make daily tasks easier to accomplish by making it easy for everyone to connect and communicate faster. VA keeps up with these trends and technologies to serve Veterans and their families efficiently and effectively. But with the benefits come the risks. VA takes steps to ensure information is secure from cyberattacks and theft. You can do your part by following the ROB.

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

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

## Texting

Text messaging has become a convenient way to communicate, and you may use text messaging on your VA-issued mobile devices just as you would use email for VA business. However, there are some risks to text messaging:

- There is no guarantee that an intended recipient is in possession of his or her mobile device
- Text messages appear in plain text and can easily be viewed by anyone nearby
- Text messages are stored on the device until they are deleted
- Mobile carriers have data retention policies that include text messages

Remember that you are not allowed to use your text messaging on your personal devices for VA business.

### More Information

If you do use text messaging on your VA-issued device for VA business, consider the following tips:

- Never send or share PHI, PII, or any other VA sensitive information in a text message
- Be aware of your surroundings or go to a private area when texting
- Be aware that VA business-related text messages may be records and exercise caution before deleting them
- Use a more secure form of communication for sensitive matters

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Electronic Data Protection**

***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

**Sensitive Information**

***I Will Not*:**

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

## Instant Messaging (IM)

VA has an approved IM system to exchange information securely on its networks. This instant message (IM) system lets you communicate securely with others on the VA network. If you use IM regularly for VA business, be aware:

- Transmission of messages is encrypted, but actual messages are not encrypted on the computer screen
- IM conversations are often saved by default and unencrypted in Microsoft® Outlook's® Conversation History

### More Information

Consider these tips to protect VA sensitive information when using IM:

- Close the IM window when a conversation ends so no passerby can view it on your screen
- If you have access to settings, turn off the conversation-saving feature in Outlook (sometimes individuals have this capability; sometimes it is controlled by your IT department)
- Never conduct VA business using instant message features of personally owned devices
- Never include PHI, PII, or other VA sensitive information in non-approved IM systems

## Rules of Behavior

### 4. INFORMATION SECURITY RULES of BEHAVIOR

**Sensitive Information**

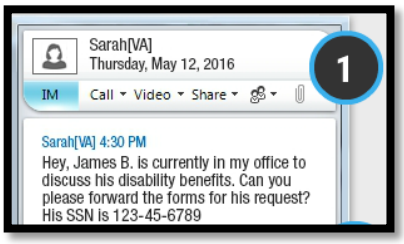
***I Will Not:***

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

## Interactive Exercise #1: Sending IMs Securely

It's time for an interactive exercise. Select the correct answer for each of the questions based on the information provided.

### Exercise #1: Scenario




Sarah has been working closely with a Veteran to help him understand his benefits. She needs to follow up with her colleague, Jerry, and knows he always answers immediately over VA's approved IM.

An instant message (from VA IM) from Sarah to Jerry. Sarah: "Hey, James B. is currently in my office to discuss his disability benefits. Can you please forward the forms for his request? His SSN is 123-45-6789."

### Exercise #1: Question

Is it acceptable to send the instant message with the Veteran's name and SSN over VA's instant messaging system?

- Yes
- No

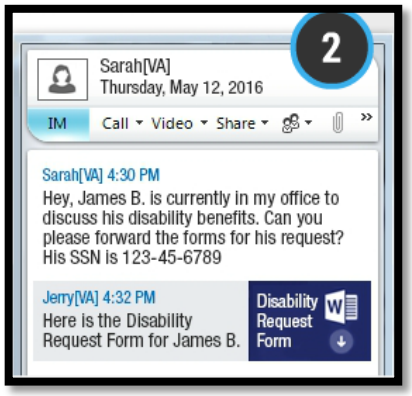
The correct answer is Yes. She can send this instant message with PII from her VA desktop to Jerry's VA desktop. Transmission of messages is encrypted; however, actual messages are not encrypted on the computer screen, so she needs to be aware that the messages appear in plain text and can easily be viewed by anyone nearby.

## Interactive Exercise #2: Sending IMs Securely

Select the correct answer for each of the questions based on the information provided.

### Exercise #2: Scenario

An instant message (from VA IM) from Jerry to Sara with an attachment. IM text reads “Here is the Disability Request Form for James B.”




### Exercise #2: Question

Sarah receives a response from Jerry with an attached document. Is Jerry violating policy by attaching the document within VA’s instant messaging system?

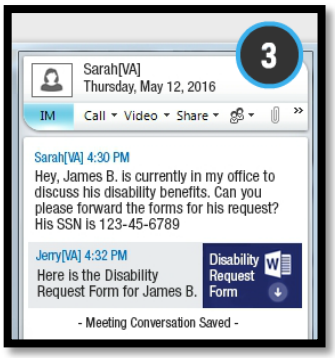
- Yes
- No

The correct answer is No. He is not violating the policy. VA’s approved IM system transmits encrypted messages; however, actual messages are not encrypted on the computer screen.

## Interactive Exercise #3: Sending IMs Securely

### Exercise #3: Scenario

Instant messages (from VA IM) between Jerry and Sara with an attachment and Conversation Saved at the bottom.




Sarah and James are finished meeting, and she received the form that they needed. Sarah has another appointment immediately after James leaves and will need to continue working on his request later in the day.

### Exercise #3: Question

Is it appropriate for Sarah to leave the screen open while her next appointment takes place?

- Yes
- No

The correct answer is No. It violates policy to keep the IM window open. She must close the IM window when a conversation ends so no passerby can view it on the screen. This could possibly pose a risk for exposing VA sensitive information.

## Social Media

Social media tools are popular ways to connect with others. VA allows the use of certain social media and other web-based collaboration tools to work together and share business information.

These include:

- Facebook
- Twitter
- Flickr
- Google+
- Instagram
- VAntage Point
- YouTube
- VA Pulse

Keep in mind, however, that each program office and facility site may have its own rules for access and use. If you are unsure about access to specific social media sites, contact your supervisor. Accessing sites and tools on the Internet may expose VA to security and privacy threats.

## Risks of Using Social Media

Here are some risks of using social media:

- Information is not private in an online forum
- Posting photos and text may reveal VA sensitive information
- Web pages and online postings may contain malicious codes, links, and attachments
- Establishing an online presence makes you a target for hackers and a source for phishing

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Sensitive Information**

***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. SOURCE: UL-2

***I Will Not:***

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

## More Information

If you use approved social media regularly for VA business, keep these guidelines in mind to keep VA and Veterans safe:

- Never comment on VA legal matters, unless you are an official spokesperson and have approval to do so
- Never post or share PHI, PII, SPI, VA sensitive information, or VA business information in any social media forum
- Never conduct VA business through social media private messaging servers
- Never store VA sensitive information on file-sharing sites
- Never click on links or open attachments posted on social media

- Never share account or access credentials
- Be aware that details you reveal in photos and text postings may violate others' privacy
- When using public social media sites for personal use, remain as anonymous as possible by not revealing too much personal information, employment information, or organizational affiliations in online postings and profiles

| **Knowledge Check: Using Social Media to Conduct Business** |
| --- |
| Consider the following question by selecting the best answer. |
| Which of the following examples of social media sites can be used within VA to collaborate and share VA business information securely?<br><br>A. Facebook, Snapchat, and Google+<br>B. Facebook, VA Pulse, and Instagram<br>C. Tumblr, Flickr, and Pinterest<br>D. YouTube, Vine, Pinterest |
| The correct answer is B. Facebook, VA Pulse, and Instagram. VA allows the use of certain social media and other web-based collaboration tools to work together and share business information. Do not share VA sensitive information on social media sites. |

## Hacking

Hacking refers to breaking into a system without authorization or intentionally violating the terms or restrictions of accessing a system for which an individual has been given access. Hacking may originate from within or outside VA networks and facilities.

Examples of internal hacking include installing unauthorized software to steal VA sensitive information and bypassing network security controls without authorization.

Hacking attacks may have a wide range of direct and indirect impacts for VA, including:

- Compromised security and networks (which could lead to more cyberattacks)
- Data breaches
- Compromised accounts and information
- Identity theft
- Lost time and money
- Loss of trust in VA

## More Information

Following the ROB is the right step for protecting VA from hacking attempts. External sources of hacking include social engineering attempts to steal log-in credentials and stealing personal information through phishing emails. Here are other things you can do:

- Use approved devices, software, information, and systems only for the intended purposes
- Report suspicious activities
- Never access systems that you are not authorized to access
- Never bypass or exploit security and controls of VA systems and devices
- Never download or install software on your VA devices without approval
- Never let unauthorized individuals access VA sensitive information, VA-issued devices, or VA systems

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will:***

- Log off or lock any VA computer or console before walking away. SOURCE: AC-11

***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
- 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

**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

***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. SOURCE: CM-10

**Teleworking and Remote Access**

***I Will:***

- Protect GFE from theft, loss, destruction, misuse, and emerging threats. SOURCE: AC-17

## Social Engineering

One way a hacker might try to gain access to VA networks is through social engineering. Social engineering is an attempt to trick someone into disclosing VA sensitive information, performing unauthorized actions on VA equipment and devices, or providing unauthorized access to VA systems, networks, or facilities. These attempts may come in the form of a face-to-face conversation, regular mail, email, or even IM or text message.

Follow these tips to deal with social engineering attacks:

- Protect PHI, PII, and VA sensitive information
- If you are unsure of someone's credentials, exercise due diligence to verify them
- If someone asks you to perform an unauthorized action on a VA-issued device, verify with the authorizing authority
- Report suspicious activities
- Never share log-in or access information to any accounts, networks, or systems
- Never allow individuals into areas where they are not authorized to enter

### More Information

Examples of social engineering attacks may be:

- Someone claims to be from the help desk and wants to run updates on your VA-issued laptop.
- A caller who is unable to verify any information says he is a Veteran who has lost his My HealtheVet log-in credentials.
- An email apparently from the Inspector General asks you to verify your log-in password for VA Pulse by replying with the information.
- Over lunch, a coworker from a different department says she is a close friend of a Veteran who has just been admitted to the medical center and wants to know what information you have about him.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Teleworking and Remote Access**

***I Will:***

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

**User Accountability**

***I Will:***

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

**Identification and Authentication**

***I Will:***

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

## Phishing

Phishing is a specific type of social engineering that uses email, text message, or IM to trick a person into revealing Sensitive Personal Information. In a phishing scam, a message appears to be from a trusted individual or organization that directs the victim to open an attachment or a link to a website. The attachment or link maliciously installs software to steal information or opens a website that requests account numbers,

usernames and passwords, or other personal data and information. In a recent internal VA survey, 30% of respondents did not recognize phishing threats.

Here's how to protect yourself from phishing attacks:

- Notice any details in the email or link that might indicate it is a phishing scam, such as misspellings, typos, or links that are similar but are not the organization's website
- Never open a link or attachment from someone you do not know
- Be cautious with emails from unknown senders and outside of VA that have "[EXTERNAL]" appended to the subject line
- If you are unsure about a link or attachment from someone you do know, confirm with the sender
- Report suspicious activities to your supervisor, ISO, or PO

For more information or questions, contact National Security Operations Center (NSOC) through the VA National Service Desk.

## Knowledge Check: Phishing

Consider the following question by selecting the best answer.

Which of the following examples represents a possible phishing attack?

A. An email from an unknown sender contains only a link or attachment without a message
B. A VA employee bypassing security controls on a VA device
C. Someone calling to request your log-in and password to access the VA network
D. Someone entering the building without an official identification badge

The correct answer is A. Phishing is a specific type of social engineering that uses email, text message, or IM to trick a person into revealing Sensitive Personal Information. An email from an unknown sender containing only a link or attachment without a message is an example of a possible phishing attempt.

## Making the Connection: Mr. and Mrs. Salazar's Story

### More Than a Number

My husband and I are both Veterans. We get nervous when we hear a story on the news about businesses or federal agencies that have had data stolen by a hacker.

We wonder what VA is doing to make sure that doesn't happen to us.

I decided to call VA and ask how I can protect my VA information and what would happen if my VA sensitive information is stolen. I learned that VA's More Than a Number identity protection program is a resource for ways to protect our family and keep our identities safe.

Sometimes news stories cause Veterans to worry about VA's security practices. Identity theft is a common concern.

## Identity Theft

Identity theft is a crime in which someone obtains and uses someone else's personal information for fraud or deception. VA information and networks are a gold mine for hackers and identity thieves. Fortunately, VA is committed to protecting Veterans and their families from identity theft. VA relies on you to do your part by following security and privacy guidelines.

- Follow the ROB to protect PHI, PII, and VA sensitive information
- Handle, transmit, store, and dispose of SPI and VA sensitive information according to VA policies and procedures
- Never share log-in or access information for any accounts, networks, or systems
- Never allow an unauthorized person to access your VA-issued devices
- Report any suspicious activities

### What to Do if You or Someone You Know Is a Victim

Chances are you know someone who has had his or her identity stolen. Here are steps from the VA Office of Information Security that you can take if you or someone you know might be a victim of identity theft:

- Contact the VA Identity Theft Help Line (see the Resources section for information)

- File a complaint with the Federal Trade Commission (FTC)
- Place a fraud alert on your credit report
- Order a copy of your credit report
- Contact your banks and financial institutions
- Report it to the police and keep a copy of the report on hand

### Rules of Behavior

**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

**Electronic Data Protection**

***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)). 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

**Sensitive Information**

***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. 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

## Connecting Points

Here are some connecting points to recall when using popular technologies:

- Always protect PHI, PII, and VA sensitive information
- Use text messaging and IM securely
- Never transmit PHI, PII, or any other VA sensitive information over text messaging or unapproved IM systems
- Be aware of what you post and reveal on social media
- Follow VA policies and procedures to prevent hacking and other cyberattacks
- Watch out for phishing attacks disguised as ordinary emails and messages
- Take precautions to protect yourself and Veterans from identity theft

# Module 4: Using Systems Securely

## Objectives

VA depends on you to keep systems and networks secure. Follow VA policies and use only approved connections when you access VA information systems.

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

- Recall how to securely access VA systems
- Identify threats to VA networks

## VA Networks

You have access to many resources on VA networks. But with that access comes the responsibility to keep VA's networks and systems safe and secure.

Here are things you must do to be secure when you access VA's networks:

- Only access networks and systems that you are allowed to access
- Do not have an open VA network connection and an open non-VA network connection connected to your computer or device at the same time unless authorized
- Never disable any VA network security controls
- Report any suspicious activities

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

***I Will Not:***

- Have a VA network connection and a non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any

device at the same time unless the dual connection is explicitly authorized. SOURCE: AC-17 (k)

**Protection of Computing Resources**

***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. 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

**Teleworking and Remote Access**

***I Will:***

- 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

## Wireless Networks

When you connect to VA's networks, use a hardwired connection if possible. Connecting by Wi-Fi (wireless access) puts VA at risk. If you must use a wireless connection, use VA-approved remote access and VA-approved wireless devices.

Remember the rules when accessing from a wireless connection:

- When you use a secure, password-protected public Internet connection, use VA’s remote access technologies to access any VA resources
- Never access nonpublic VA resources from public computers or devices, such as a public computer at a library or a tablet displayed in a retail store
- Never bring your personally owned equipment into a VA facility and connect to the network
- If you have been approved to use a personal device for VA business, you may only use VA-approved remote access technologies, such as CAG, to access VA resources

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

**Electronic Data Protection**

***I Will:***

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

***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

**Teleworking and Remote Access**

***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

## Remote Access

Use VA-approved remote access methods to access VA resources whenever you are connecting from outside of a VA facility. In most cases, a telework agreement is necessary to regularly access VA systems remotely. Contact your ISO for information on how to get a remote access account.

You must follow VA’s national and local security policies, procedures, and configuration standards before being allowed access to any VA network.

Being granted remote access capabilities means you must:

- Have approval from your supervisor to work from home and, if required, a signed telework agreement

- Connect through the Citrix Access Gateway (CAG) with two-factor authentication through required use of a PIV card reader or SafeNet MobilePASS token
- Never conduct VA business through your personal emails, personal IMs, or personal phone text messages
- Let your supervisor and ISO know when you no longer need remote access

## More Information

### *Citrix Access Gateway (CAG)*

CAG is the only VA-approved method to connect remotely for non-VA devices, such as personal devices or those devices used by contractors. You can also use CAG for remote access from a VA-furnished device.

### *Remote Enterprise Security Compliance Update Environment (RESCUE)*

RESCUE provides Virtual Private Network (VPN) access on VA-furnished devices. If VA has issued you a laptop computer, you can use RESCUE to access VA's network when you are not connected directly within a VA facility.

### *Two-Factor Authentication*

Two-factor authentication verifies your identity with two elements: something you have, such as your PIV card, and something you know, a PIN. If a device does not have a card reader, VA offers the SafeNet MobilePASS application for VA CAG remote access, which installs a software token on the device.

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will:***

- Follow established procedures for requesting access to any VA computer system and for notifying my VA supervisor or designee when the access is no longer needed. SOURCE: AC-2

**Teleworking and Remote Access**

***I Will:***

- 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

***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

**Sensitive Information**

***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. SOURCE: UL-2

## Network Access While Traveling Outside the United States

The risk of exposing VA networks to unauthorized parties can be greater when traveling outside the United States. You may access VA external web applications while traveling, but certain other access is prohibited. Be sure to contact your VA supervisor, ISO, PO, or local Chief Information Officer (CIO) if you plan to travel outside the U.S. and if you expect to have a need to access VA networks while traveling.

You are not allowed to access VA internal networks when you are traveling to countries that pose a significant security risk, unless you have specific authorization from your VA supervisor, ISO, local CIO, and Information System Owner. These countries include non-NATO countries and other high risk countries as identified by VA or the State Department.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Telework and Remote Access**

***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. SOURCE: AC-19
- 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

## Telework Guidance

Teleworking, or telecommuting, refers to a work flexibility arrangement under which you do not commute to a central place of work every day. If you are approved to telecommute, you may work from another approved worksite, such as a home office or another facility. Keep in mind that you may need a signed telework agreement to telework. Some software tools used when working remotely include:

- VA-approved remote access
- Conference calling
- Video conferencing

Use all teleworking tools securely to protect VA sensitive information.

### VA's Telework Policy

VA's telework policy is located in VA Handbook 5011/26, Hours of Duty and Leave (Telework) and is also known as the Alternative Workplace Arrangement policy. Review the handbook for information on the VA telework program and telework criteria as well as examples of the forms to request permission.

VA Form 0740 is used to establish a telework agreement. This document includes the request to telework, the employee's workplace arrangements and work schedule, and information about equipment used to telework. If you are eligible for telework, you must first complete the VA Telework Training Module for Employees; this is an annual requirement. Then, attach your certificate of completion with the telework agreement forms. Start by asking your supervisor for directions to complete the request.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Telework 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
- 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

***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

| **Knowledge Check: Remote Access** |
|---|
| Consider the following question by selecting the best answer. |
| Which of the following is allowed under VA's remote access and telework policies?<br><br>A. Connecting to VA resources through a personal VPN you set up<br>B. Sending draft documents of a pending VA policy from your personal Gmail account<br>C. Connecting to VA resources through the VPN using your PIV card and password |
| The correct answer C. Use VA-approved remote access methods to access VA resources and to conduct VA business whenever you are connecting from outside of a VA facility. Connect through the VPN by using a PIV card and password. You must have approval to have remote access. |

## Risks and Threats

VA information systems, software, and networks need ongoing protection from threats that can expose VA sensitive information. The VA NSOC monitors all network traffic for unusual or unapproved activities.

Here are some actions you can take to protect VA information systems:

- Never give your password to anyone

- Never download a program or software from the Internet onto your VA-issued computer
- Check with your supervisor, ISO, and your local Office of Information and Technology (OI&T) representative to request additional software
- Be suspicious of virus alerts on web pages, and never click on untrusted links
- Report all suspected threats and warnings to your ISO

While VA network controls and tools filter out a lot of the information security threats, some do manage to get through.

## More Information

Malware, phishing, and spoofing are common risks and threats that you may see in the form of emails and attachments. Know the risks and actions to take when you receive any suspicious emails or attachments.

### *Malware*

Malware is software that can harm a computer or system. It includes viruses, worms, Trojan horses, and spyware.

Risks:

- Interrupts computer function
- Collects VA sensitive information
- Gains unapproved access to computer systems
- Alters or deletes VA sensitive information

Protection Methods:

- Access and use only VA-approved security software, which are listed on the One-VA Technical Reference Model (see the Resources section for information)
- Do not open suspicious email attachments or websites
- Do not select links inside pop-ups
- Do not download unapproved software, free trials, etc.

### *Phishing and Spoofing*

Phishing is an effort to steal personal data or information through an email or URL link. Many times phishing attacks use spoofing. Spoofing is an attempt to modify code in an email so the recipient thinks it is from a known or trusted person.

Risks:

- Collects VA sensitive information by pretending to be an honest source

- Appears as a link to a real website and redirects the user to a fake site

Protection Methods:

- Right-click the suspicious link to display the URL
- Ensure you have VA-approved encryption on your devices
- Type the website address instead of selecting provided links

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

**Electronic Data Protection**

***I Will:***

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

***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. SOURCE: CM-11

**Identification and Authentication**

***I Will:***

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

## Making the Connection: Wendy's Story

### Unauthorized Access

My daughter just got a job in patient billing for the VA health care facility where I am a patient. I asked her to look up my personal medical records to see if she could find out my latest test results.

I am worried about those results, and I've called the clinic twice.

I was surprised when she said she can't do that. She said VA employees have to have a job-related need to know before they can see anyone's personal information and they also have to be authorized by IT. You know, even if she couldn't do what I wanted, I was glad to learn that VA has rules to protect my personal health information.

Be careful to use only the information you are authorized to use for doing your job.

## Insider Threats

One of the biggest threats to any organization's data and information networks is the people who have the easiest access: insiders. Organizations are exposed to insider threats when employees have access to sensitive information or systems and the organization does not have effective controls or is not enforcing controls to prevent misuse.

Many people are naturally curious, but acting on your curiosity can lead to violating privacy and confidentiality. This will weaken Veterans' trust in VA.

Insiders know how a facility operates and may have access to information that they can be tempted to use illegally or even sell to others. The potential for fraud increases when the opportunity is available. Avoid being caught up in an illegal scam by closely following all of the ROB.

Help protect VA from insider threats by noticing odd behaviors. Remember, if something a colleague is doing doesn't seem quite right, report it as an incident.

### More Information

***Insider Threats***

Risks:

- An insider could use authorized access, by accident or by intent, to harm information systems and VA sensitive information
- An insider could become an involuntary threat by opening an attachment containing a virus that installs when opened
- An insider could be a social engineer, a friendly actor who charms you into disclosing VA sensitive information

Prevention:

- Never share your password or other account information, even with trusted coworkers
- Verify any requests for VA sensitive information before releasing it, even if the request seems harmless to you
- Use the access you've been given to the network only to perform your official duties. If you require more access, go through appropriate channels to get it

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Identification and Authentication**

***I Will:***

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

**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

## Preventing Attacks

You can help prevent attacks on VA information systems by following these guidelines:

- Follow instructions to update your VA-approved security software
- Avoid strange websites
- Avoid opening strange emails or attachments
- Never disable or bypass system controls to access VA sensitive information, unless specifically authorized by your local CIO

Report anything odd on your computer system to your ISO, such as:

- Odd characters in a document or email
- Missing data
- Sudden increases in spam or unsolicited email
- Strange attachments in emails

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Protection of Computing Resources**

***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. SOURCE: CM-3

**Electronic Data Protection**

***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. SOURCE: CM-10

**Incident Reporting**

***I Will:***

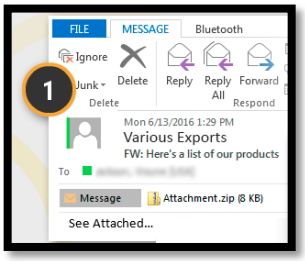
- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor or designee immediately upon suspicion. SOURCE: IR-6

## Interactive Exercise #1: Preventing Attacks

It's time for an interactive exercise. Select the correct answer for each of the questions based on the information provided.

### Exercise #1: Scenario

An email message that has a *.zip attachment from a vendor.




You receive an email with an attachment (zip file with generic name of "attachment.zip") from a vendor you have never heard of. The subject line says Various Exports FW: Here's a list of our products.

### Exercise #1: Question

Do you open the attachment?

- Yes
- No

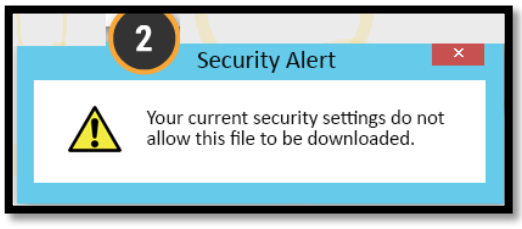
The correct answer is No. Never open an attachment from an unknown email address. Never forward the email with the attachment because it has the potential to cause further damage to the network.

## Interactive Exercise #2: Preventing Attacks

Select the correct answer for each of the questions based on the information provided.

### Exercise #2: Scenario

A browser window with a Security Alert dialog box stating "Your current security settings do not allow this file to be downloaded."




You are at home working on your VA-issued laptop. A friend stops by and wants to show you a website. You type in

### Exercise #2: Question

Do you bypass the security controls and disable the antivirus so that you can view the content?

- Yes
- No

The correct answer is No. Never bypass or risk security and controls of VA systems and devices.

| Interactive Exercise #2: Preventing Attacks | |
|---|---|
| the web address and realize only some of the content is displayed. Your friend suggests that you disable your laptop's firewall and antivirus so you can access the page. | |

| Interactive Exercise #3: Preventing Attacks | |
|---|---|
| Select the correct answer for each of the questions based on the information provided. | |
| **Exercise #3: Scenario**<br>A woman on the phone sitting in front of her laptop.<br>  <br><br>You receive a call from an anonymous number, and the caller states that your computer has been infected with a virus and that he or she needs your username and password to troubleshoot. | **Exercise #3: Question**<br>Is this an example of a possible social engineering attack?<br>• Yes<br>• No<br>The correct answer is Yes. This could be a social engineering attack. There are people who may use a friendly or official manner to try to trick you into giving them information or performing unauthorized actions on VA equipment or systems. Never give your password to anyone. |

## Connecting Points

Here are the connecting points to recall to keep VA systems secure:

- Access only the VA networks and systems you are authorized to access
- Follow VA guidelines and policies when you access networks and systems wirelessly or remotely
- If you are a teleworker, follow VA's telework policy
- Recognize and report threats to VA systems, including common and insider threats

# Module 5: Using Equipment and Devices Securely

## Objectives

Equipment and devices at VA come in all sizes and shapes. Some are big and stationary, such as a desktop computer. Others are small and portable, such as a mobile phone. Despite the differences, they all have privacy and security risks that you must manage.

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

- Recall how to use VA-issued devices securely to prevent unauthorized access to VA sensitive information
- Recognize when you may use personally owned equipment for VA business

## Making the Connection: Christopher's Story

### Missing Equipment

I had to stop at the store on my way home from work last week. While I was in the store, someone broke into my car and took my VA-issued equipment. They stole my iPad, cell phone, and PIV card. Even my personal laptop was stolen.

Since it's my responsibility, I quickly notified the local police department and VA Police Service and both have taken statements along with police reports. The wireless carrier was notified and terminated cellular service to the iPad and cell phone. VA IT had the iPad remotely erased.

Protect the devices that are assigned to you. You are responsible for the care, use, and protection of these devices and the information stored on them.

## Inventory Control for Electronic Devices

VA employees, contractors, and volunteers use VA electronic devices to support their work.

Examples of electronic devices include desktop computers, laptops, BlackBerrys, Apple internet operating system (iOS) devices, Android devices, universal serial bus (USB) drives, biomedical equipment, and copy machines. Inventory control is important because it ensures VA equipment is not lost or stolen and is in the correct place.

## More Information

Here is what you need to remember to keep track of electronic devices and keep them secure:

- Protect the devices that are assigned to you. You are responsible for the care, use, and protection of these devices and the information stored on them
- Be especially careful with your laptop in airport security lines. The airport security conveyor belt is a common place for laptop theft. Place your computer on the belt only when you are the next in line, and always keep your eyes on it
- Work with your supervisor to notify your IT inventory coordinators prior to changing locations or changing jobs. IT equipment has to be accounted for, like all other federal property. Missing laptops, data cables, and other IT equipment means possible risk for Veterans and lost resources for VA
- Agree to periodic electronic device inspections
- Enable VA-approved security tools

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will Not:***

- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8

**Protection of Computing Resources**

***I Will Not:***

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

**Electronic Data Protection**

***I Will:***

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

**Teleworking and Remote Access**

***I Will:***

- Keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information, regardless of work location. SOURCE: AC-17
- Protect GFE from theft, loss, destruction, misuse, and emerging threats. SOURCE: AC-17

**User Accountability**

***I Will:***

- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. SOURCE: AU-1
- Have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand. SOURCE: MA-2
- Permit only those authorized by OI&T to perform maintenance on IT components, including installation or removal of hardware or software. SOURCE: MA-5

## Medical Devices

Some laptops that run software for biomedical equipment or devices cannot be encrypted. Since VA needs these devices to treat patients and store patient information, these devices are exempt from encryption, but must be placed on a separate local area network (LAN) or virtual local area network (VLAN) to ensure security. Before disposing of biomedical equipment capable of storing information electronically, contact your CIO and ISO.

NSOC's Enterprise Network Defense (END) team recommends ensuring that all medical devices are protected in accordance with VA policies. You can find the Field Security Service Health Information Security Division SharePoint site for Medical Device Protection Program (MDPP) guidance in the Resources section. Work with device vendors to ensure all software is secure and properly patched and that appropriate security measures, such as strong passwords, are employed where applicable. Report incidents to NSOC.

### More Information

A wide cross section of biomedical devices share some common security risks, including:

- Lack of validation to access or use the equipment
- Weak or default passwords like “admin” or “1234”
- Embedded web servers and interfaces that make biomedical devices an easy threat
- Embedded web services that allow devices to communicate with one another

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

**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

**Identification and Authentication**

***I Will:***

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

## Using VA-Issued Devices Securely

You are responsible for the care, use, and protection of any VA-issued devices and the information stored on them.

To protect the information on your VA devices:

- Keep your security software up-to-date, following VA’s guidance
- Use VA-approved encryption and passwords
- Enable VA-approved security tools
- Never open attachments from an unknown sender

- Never select a URL sent by an unknown sender directing you to a website. This is typically simple to spot, as most emails from unknown senders and outside of VA have “[EXTERNAL]” appended to the subject line
- Report all odd messages or suspected threats and warnings to your ISO

For more information about encryption for your VA devices, contact your ISO or the VA National Service Desk.

## More Information

### *Know the rules*

Get approval from your supervisor, local ISO, and CIO before you transport, transmit, access, or use VA sensitive information remotely.

### *Protect patient data and your information*

Only certain VA-issued devices have been approved for use with VA sensitive information. Never assume that a VA-issued device is protected and allowed for use with VA sensitive information without clear guidance from OI&T or your ISO.

### *Keep it with you*

Never leave any of your mobile devices or portable equipment unattended. Smaller mobile devices that do not have the ability to use a cable lock should be kept with you personally or in a secure place, such as a locked cabinet, desk, or safe, if available. If you are working in an uncontrolled area, use VA-issued cable locks for laptops and tablets with this capability to help keep your equipment secure, and keep your smaller mobile devices that are unable to be cable locked with you.

### *Safeguard VA data*

Do not install any non-VA approved applications onto your mobile device if they have not been approved by VA. Many applications exist on these platforms that have the ability to gain access to secure VA data through cloud connections, as well as harmful applications that try to use your mobile device as a gateway into the VA network. If there are applications that you believe should be made available to you on these mobile platforms, requests for approval can be made through the VA National Service Desk. It is very important to enter patient or government sensitive information only in approved applications. Non-VA approved apps could take sensitive data and transmit it to anyone, including recipients in foreign countries.

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**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:***

- 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

***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. SOURCE: CM-10

**Identification and Authentication**

***I Will:***

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

## Policy and Use of VA-Issued Devices

VA allows limited personal use of government office equipment, including information technology.

VA employees may access and use VA-issued devices and equipment (e.g., mobile telephones, tablets, computers, and copiers) for personal activities, as long as this limited personal use is occurring with supervisor approval, and it:

- Does not interfere with work
- Does not affect productivity
- Does not violate standards of ethical conduct

Contractors may not access or use VA-issued devices for personal use unless it is stated in the terms of the contract.

No one may access or use VA-issued devices for prohibited activities.

### More Information

Prohibited activities include, but are not limited to:

- Creating, viewing, or sending pornographic material
- Creating, viewing, or sending material related to gambling, illegal weapons, terrorist activities, or other illegal activities
- Creating, copying, or sending chain letters
- Sending unapproved mass mailings
- Supporting “for profit” activities outside of VA
- Participating in unapproved lobbying or fundraising

### Rules of Behavior

**2. COMPLIANCE**

2b. 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.

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will:***

- Only use my access to VA computer systems and/or records for officially authorized and assigned duties. SOURCE: AC-6
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

***I Will Not:***

- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment including Information Technology. SOURCE: AC-8

## Privacy and Security on VA Mobile Devices

If you have a VA mobile device, be sure you know the requirements for protecting privacy and ensuring security when using apps.

### Downloading Public Apps

When downloaded, many public apps ask users for access to information stored on a user's device.

VA requires users to click "Don't Allow" for all pop-ups requesting access to contacts, photos, calendar, and other settings. Clicking "OK" to such requests for access when downloading, installing, or using public apps may open the device to potential tracing capabilities and put your device data at risk.

Confirm where the app data is being stored to ensure that no VA sensitive information is stored on the Cloud. Do not automatically accept access requests for information such as:

- Location
- Contacts
- Calendar
- Photos
- Microphone

### Public Apps and PHI/PII

No public apps should contain sensitive information regardless of the security implied by the manufacturer or developer. You must protect VA sensitive information when you use any type of electronic device or communication to store, transport, or dispose of information.

### Mobile Device Privacy Settings

In the privacy section of the settings option on your mobile device, you have the ability to see which apps are accessing your data. Be proactive about updating your privacy settings to ensure that none of your apps are putting your data, or your patient's data, at risk.

If you are not receiving or inputting any information related to VA on your government-furnished device, then you can download apps from other public app stores, but you must participate in the mandatory training prior to doing so.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***I Will Not:***

- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8

**Electronic Data Protection**

***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)). 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

***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. SOURCE: CM-11

## Apps

Software applications or “apps” can make some tasks faster and easier on mobile devices. If the VA App Catalog does not have the apps you need for your VA task, you may need to download apps from a public app store. All VA ROB must be followed. VA-approved public app stores include:

- Apple App Store
- Google Play Store

If you are authorized to use VA mobile devices, use due diligence and the highest ethical standards when downloading from public app stores and updating any public apps. Make sure you understand app software updates and ensure there is no privacy or security risk associated with the update. You may also be required to take mandatory training.

### Guidance

If you download and use apps on your mobile device:

- Protect VA sensitive information when you use any type of electronic device or communication to store, transport, or dispose of information
- Get approval to download apps to your VA device
- Use only apps available in the VA App Catalog with VA sensitive data and information
- Be wary of pop-ups that might request access to your information
- Do not use public apps that store or process PII or PHI

### Mandatory Training

If you are not receiving or entering any information related to VA on your government-furnished device, then you can download apps from other public app stores, but you must participate in the mandatory training prior to doing so.

To use and download public apps through public app stores, you must participate in a mandatory training session available through the MyVeHU Campus titled *Protecting Privacy and Security While Using Apps from the Public App Store*.

Other training available on the TMS includes the *Mobile Training: Security of Apps on iOS Devices* (TMS: 3926744). See Appendix D, Privacy and Information Security Resources for more information.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

**Electronic Data Protection**

***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)). 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

***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. SOURCE: CM-11

**Sensitive Information**

***I Will:***

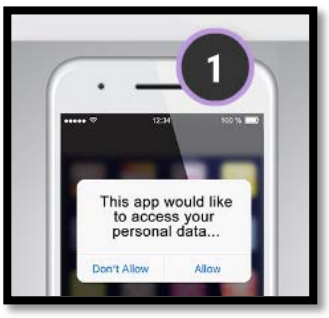
- Obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)). SOURCE: UL-2

## Interactive Exercise #1: VA-Issued Devices

It's time for an interactive exercise. Select the correct answer for each of the questions based on the information provided.

### Exercise #1: Scenario

A mobile device with a message requesting access to personal data stating, "This app would like to access your personal data…" and displaying Don't Allow or Allow buttons




You want to check out a new video app and load it on your VA mobile device.

You go to the public app store on the

### Exercise #1: Question

Do you select Allow to permit access to your information?

- Yes
- No

The correct answer is No. Do not install or accept any applications on your VA mobile device that have not been approved by VA. Some applications may have the ability to enable intruders to gain access to secure VA data through cloud connections. Some applications can be harmful applications that try to

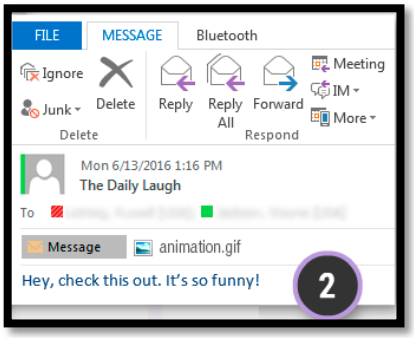
| | |
|---|---|
| Internet, select Install, and get a pop-up requesting access to information stored on your device. | use your mobile device as a gateway into the VA network. |

## Interactive Exercise #2: VA-Issued Devices

Select the correct answer for each of the questions based on the information provided.

### Exercise #2: Scenario

An email from The Daily Laugh with an animated gif attached. "Hey, check this out. It's so funny!"




Your coworker wants to send out a mass email with a cute animation for the holidays using the VA network. Is this example permitted within the guidelines for limited personal use?

### Exercise #2: Question

Your coworker wants to send out a mass email with a cute animation for the holidays using the VA network. Is this example permitted within the guidelines for limited personal use?

- Yes
- No

The correct answer is No. This would be considered misuse of VA systems. VA Directive 6001 provides guidelines for limited personal use of VA issued devices. Sending mass emails would be considered misuse of VA systems.

## Interactive Exercise #3: VA-Issued Devices

Select the correct answer for each of the questions based on the information provided.

### Exercise #3: Scenario

Your VA-furnished laptop has reached its storage capacity and you have many files that you do not want to delete.

### Exercise #3: Question

Can you use your personal external hard drive to store your VA sensitive documents?

- Yes
- No

| | |
|---|---|
| Image of a laptop with an external hard drive next to it.   | The correct answer is No. Removable media may contain or allow access to private information. This could lead to potential loss or exposure of sensitive Veteran information. Use VA-approved portable electronic devices, which are encrypted, adding a layer of protection to your data. Never use removable media to transfer data to a personal device. VA data should only be located on VA-approved devices. |

## Personal Electronic Devices

You must have permission to use any personal electronic devices and personally owned equipment for VA work. Keep these guidelines in mind when using personal electronic devices:

- VA does not allow you to bring your personally owned equipment into a VA facility and connect to the network
- Personally owned devices may only use CAG as a VA-approved remote access technology to access VA resources
- If you are approved to bring personally owned equipment into a VA facility, you must have approval from the System Owner or local CIO to use remote access from your personally owned equipment while in the facility
- Never store VA sensitive information on any personal electronic device

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6

**Telework and Remote Access**

***I Will:***

- 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

## Unencrypted Devices

Some personal devices and equipment may not connect to a VA system but do connect wirelessly to a VA device, such as wireless headsets, wireless keyboards, and Bluetooth devices. These devices may be unencrypted.

### Wireless telephone headset

Other people can listen to phone conversations and download your data when you use an unencrypted wireless headset. Even encrypted wireless headsets are a security risk, especially when used outside of a VA facility. Bluetooth headsets are not FIPS encrypted. Do not use a wireless headset while working on VA business-related activities unless it meets FIPS 140-2 validated encryption and has been approved by your Facility CIO.

### Wireless keyboards

Do not use a wireless keyboard while working on VA business-related activities unless it has been approved by your Facility CIO.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Access and Use of VA Information Systems**

***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. SOURCE: AC-6

***I Will Not:***

- Have a VA network connection and a non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any device at the same time unless the dual connection is explicitly authorized. SOURCE: AC-17

- 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

**Electronic Data Protection**

***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)). 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

***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

**Sensitive Information**

***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)). SOURCE: UL-2

## Portable Storage and Removable Media

Portable storage devices, such as thumb drives and portable hard drives, and removable media, such as writeable DVDs, are convenient ways to transfer data. However, they create a risk to privacy and security because they may contain VA sensitive information. If you use these storage devices or media, follow these restrictions:

- VA data should only be stored and processed on VA-approved devices
- If you use a portable storage device, make sure it is VA-approved
- Never use removable media to transfer data to a personal device
- Keep portable storage devices and removable media secure when not in use

## Rules of Behavior

### 4. INFORMATION SECURITY RULES of BEHAVIOR

**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

**Electronic Data Protection**

***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)). 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

**Sensitive Information**

***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)). SOURCE: UL-2

| Knowledge Check: Personal Electronic Devices |
| --- |
| Consider the following question by selecting the best answer. |
| Which of the following statements is true regarding the use of personal electronic devices at VA?<br><br>A. Personally owned devices may only use VA-approved remote access technologies to access VA resources<br><br>B. You can bring any type of equipment into a VA facility and connect to the network without approval as long as you protect VA sensitive information<br>C. You can use a removable storage device to transfer VA sensitive information to your personal laptop at home<br>D. VA sensitive information may be stored on your personal electronic device |
| The correct answer A. Personally owned devices may only use VA-approved remote access technologies to access VA resources. However, remember that you must have approval to use any type of personally owned device to connect remotely. |

## Connecting Points

Here are the connecting points to recall when using electronic devices:

- Keep equipment, storage devices, and removable media with you at all times
- Use only VA-encrypted electronic devices that have been approved by your ISO and CIO
- Use only VA-approved apps from the VA App Catalog for VA data
- Do not access VA systems with personal devices or personally owned equipment without authorization

# Module 6. Conversations and Email

## Objectives

Everyday tasks, such as conversations and emailing, require security awareness at VA. Keep privacy and information in mind when you talk to someone or communicate electronically about VA sensitive information.

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

- Recall how to protect VA sensitive information in conversations
- Identify how to safely communicate VA sensitive information in electronic messages

## Making the Connection: Tony's Story

### Be Aware of Your Surroundings

I recently attended a fellow Veteran's funeral service. There was a woman, Wanda, who stood up to speak about Jack. As she was talking, I realized that she may have compromised his privacy by sharing some stories about him while he was being treated at VA's mental health facility.

This made me feel uncomfortable.

Even though Wanda was fond of Jack, she had the responsibility as a VA employee to maintain his privacy and not discuss that he had been treated at a mental health facility. Discussing Veterans' sensitive information should never happen in a public setting.

Be aware of your surroundings when discussing sensitive conversations, and avoid revealing any VA sensitive information until you are in a more secure location.

## Face-to-Face and Phone Conversations

You are responsible for protecting Veterans' privacy and information in all situations. Follow these guidelines to protect VA sensitive information when you are having conversations in person or when using the phone.

In person:

- Discuss sensitive information in private, such as in a private office
- Close office doors or leave areas where others can overhear

- Lower your voice when others are around
- Avoid talking about VA sensitive information in lobbies or elevators or other public places

On the phone:

- Never give PII or PHI over the phone to someone you do not know or who may not have the legal authority to receive it
- Never leave PII or PHI in a voicemail

### More Information

***Face-to-face or phone conversations***

Be aware of your surroundings and be careful what you say in face-to-face or phone conversations to prevent disclosing VA sensitive information to anyone who doesn't need to know.

Discussing Veterans' SPI over the phone or face-to-face in waiting areas, hallways, or elevators should never happen. Conversations, including one side of a phone conversation, can be overheard by anyone passing by. Be aware of your surroundings and go to a private area for sensitive conversations, and avoid revealing any VA sensitive information until you are in a more secure location.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Sensitive Information**

***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. 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

## Securing Email

Unencrypted email messages can expose private information. Emailed information is more secure if it is encrypted. You must encrypt all emails and attachments that contain VA sensitive information. You can also use a digital signature to add another level of

security to your email messages. Adding a digital signature to an email allows the recipient to verify the authenticity and integrity of the messages you send.

Always follow the guidelines and best practices when sending encrypted emails containing VA sensitive information.

VA uses two types of encryption to protect email: Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption and Active Directory Rights Management Service (ADRMS). VA-issued computers encrypt email through Microsoft Outlook. Mobile devices, such as BlackBerry phones and iPhones, must have an encryption certificate or an ADRMS client installed, which allows the device to send and receive encrypted emails.

## More Information

### *Guidelines and practices when sending encrypted emails*

- Do not include VA sensitive information in the subject line
- Include your name and phone number in encrypted emails
- Confirm all individuals on the distribution list are approved to receive the information
- Consider the audience carefully before using Reply All for an email
- Be sure your computer's settings have turned off the feature to Auto Forward messages to addresses outside of VA's network

### *S/MIME*

You may also hear S/MIME encryption referred to as a Public Key Infrastructure (PKI) certificate. This form of encryption prevents information in email messages and email attachments from being read by people who are not authorized. It also provides authentication of the sender if the message is signed. S/MIME works for both external and internal messaging if the recipient also has a VA trusted PKI certificate.

S/MIME does not encrypt information sent in the subject line of an email. Never put VA sensitive information in the subject line of an email.

If you have questions about how to use S/MIME, you can search for more training in the TMS or contact the VA National Service Desk.

### *ADRMS*

ADRMS, previously called Rights Management Service (RMS), protects the content of email messages, email attachments, and other Microsoft Office® documents. ADRMS provides additional controls that S/MIME does not. ADRMS can prevent forwarding,

copying, and Microsoft-provided screen captures of RMS-protected content. ADRMS works internally and externally if the external user is enrolled in the VA ADRMS system. You can request external user access to VA's ADRMS system.

If you have questions about how to use ADRMS, you can search for more training in the TMS or contact the VA National Service Desk.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Electronic Data Protection**

***I Will*:**

- Use VA e-mail in the performance of my duties and when issued a VA email account. SOURCE: SC-8
- 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
- Obtain approval prior to public dissemination of VA information via e-mail as appropriate. SOURCE: SC-8

***I Will Not:***

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

**Sensitive Information**

***I Will:***

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

***I Will Not:***

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

## Prohibited Use of Personal Email

According to VA Memorandum VAIQ #7581492, Use of Personal Email, "the use of a personal email account or the use of a personal email system to conduct official agency business is not allowed." Do not use your personal email address to communicate about

VA business. When you use VA email, a copy is kept of all emails and makes it possible for VA to keep track of business actions.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Electronic Data Protection**

***I Will*:**

- Comply with all federal VA information security, privacy, and records management policies. SOURCE: PM-1
- Use VA e-mail in the performance of my duties and 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

**Teleworking and Remote Access**

***I Will:***

- Keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information, regardless of work location. SOURCE: AC-17
- Protect GFE from theft, loss, destruction, misuse, and emerging threats. SOURCE: AC-17

**Sensitive Information**

***I Will Not:***

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

## Electronic Calendar and Invitations

Electronic calendars are helpful tools, but they can expose VA sensitive information. Do not enter VA sensitive information into a Microsoft Outlook Calendar item or meeting invitation Subject line because it does not have the proper security controls. Any VA sensitive information that you send for a meeting must be sent by a secure electronic format, such as encrypted email.

Never use public electronic calendars or schedulers, such as Google or Yahoo calendars, for VA business.

Public electronic calendars are not VA-approved, do not have adequate security, and can be more easily invaded by hackers.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Sensitive Information**

***I Will Not:***

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

| Knowledge Check: Electronic Calendars and Invitations |
| --- |
| Consider the following question by selecting the best answer. |
| You are planning a meeting to discuss a patient's lab test results. Which of the following examples protects PII or PHI in the subject line of an Outlook meeting invitation?<br><br>A. Meeting with John Smith DOB: 01-30-75<br>B. John Smith, 444 Cherry Lane, cancer treatment<br>C. Mary Smith biopsy results<br>D. Meeting about patient biopsy |
| The correct answer is D. Meeting about patient biopsy. Do not put PHI or PII in the subject line of a meeting invitation because it does not have the proper security controls. Always protect VA sensitive information in electronic communication. |

## Connecting Points

Here are the connecting points to recall so that you can safely share VA sensitive information in everyday conversations and emails:

- Protect information in conversations and electronic messages
- Disclose VA sensitive information only to those who need to know
- Encrypt messages and attachments containing VA sensitive information
- Never include VA sensitive information in electronic calendars or email subject lines

# Module 7: Handling Paper and Electronic Documents

## Objectives

VA sensitive information can be found in many types of documents or media. You need to know how to keep documents, records, and files containing VA sensitive information safe, whether they are in paper or electronic form.

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

- Recognize how to protect VA sensitive information when handling paper documents, records, and files
- Identify how to store safely, transport, and dispose of any media containing VA sensitive information

## Making the Connection: Tanya's Story

### Mishandling Documents

While talking with the clerk at my doctor's office, I placed my tablet on top of the counter. When I left, I accidentally picked up the documentation that the clerk was working on along with my tablet.

That evening I realized my mistake and returned the documents the next morning. The clerk said she noticed the documents were missing, but didn't know what had happened to them. She was relieved that I had returned them, but still had to report the mishandled documents.

It is important to keep VA sensitive documents secure, especially in a public area. Always maintaining a clean-desk policy helps to ensure that documents are not mishandled.

## Requirements for Handling Paper Documents

Improperly handling paper documents and files creates the majority of privacy and information security incidents reported at VA each year. Be sure you know the best practices for handling documents, files, and federal records in paper format.

Paper documents are familiar to most of us. A few other specialty items must also be handled as if they are paper documents.

Every facility has designated individuals who administer or oversee the VA Federal Records Program in their respective area.

This role goes by many names across VA administrations. We refer to designated records management officials in this course to describe those who have local oversight responsibilities to ensure that file plans are maintained. The designated records official coordinates the storage and disposition of records and provides assistance with the local records program.

## More Information

### *Paper documents and files*

Follow these best practices to protect VA sensitive information stored in paper documents and files:

- Do not leave files out in areas such as public spaces, private offices, conference rooms, copy or fax machines, mailboxes, or wall trays
- Lock files and documents in a drawer or cabinet when you are not in your work area
- Get written permission from your supervisor, CIO, and ISO before you transport VA sensitive information from VA locations
- Always transport VA sensitive information in secure containers or briefcases
- Maintain a clean-desk policy where you ensure you do not leave VA sensitive information unattended on your desk during the day or when you leave for the day

### *Examples of paper documents*

Some examples of paper documents include:

- Printouts of letters, reports, forms, or other content that was first created on a computer
- Copies made on a copy machine
- Fax transmissions sent or received
- Handwritten notes
- Drawings
- Magazines
- Photos
- Maps

## Rules of Behavior

**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

**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
- 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
- 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

## Records

Most paper documents or files may also be federal records and, if properly scheduled with NARA, will be identified in the applicable Records Control Schedule (RCS) or General Records Schedule (GRS). These records must be available for use as appropriate as noted in the applicable RCS and disposed of properly.

### More Information

***Using and storing paper records***

- Use a notice sheet as required before sending paper records to anyone. Refer to VA Directive 6609 for instructions on mailing documents or federal records containing SPI
- Documents containing PHI must be sent using a HIPAA sealed envelope
- Clearly mark any folders in storage boxes if they contain VA sensitive information. If you need to move federal records to off-site storage, first contact your designated records management official. Be sure to clearly mark transfer forms (SF-135 or VA Form 0244) when moving records that contain VA sensitive information

- Be sure federal records that are stored off-site are listed on the work center's file inventory. As long as federal records are in the legal custody of VA, designated records officials must maintain access control and security for records with VA sensitive information in them. Coordinate with your designated records management official if you are storing or handling federal records

### *Destroying or disposing of paper records*

Ask your supervisor or designated records management official for guidance before you dispose of or destroy any material that may be a federal record. You can also consult VA Directive 6300 and VA Handbook 6300.1 for guidance.

### *Using paper logbooks*

- Paper logbooks must not be used unless you have permission. To maintain a paper logbook, you must have an important business need or legal requirement and you must have it approved by the Facility or Program Director
- VA does not allow the use of paper logbooks for personal use. This includes the use of paper logbooks in clinics and medical centers. VHA strongly discourages any use of paper logbooks
- Logbooks with VA sensitive information should be kept in electronic files on authorized VA systems. If your job requires you to maintain a logbook, use an electronic logbook if possible

If you find an old paper logbook, contact your local designated records management official or Privacy Officer to determine how to handle it.

## Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Electronic Data Protection**

***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)). SOURCE: SC-13

**Sensitive Information**

***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. SOURCE: SC-13

## Faxing

The best practice for VA facilities is to only use a fax to transmit VA sensitive information when a secure electronic transmission is not available.

If you do use fax technology:

- Be sure to send faxes from a location that is not public
- Be sure your recipient also has a secure location or someone is by the receiving machine to collect the information
- Include a fax cover sheet with the following information:
    - Recipient's name
    - Your name and contact information
    - Instructions for the recipient to verify fax receipt
    - The following statement should be used on fax cover sheets:
      *This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above.*

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Sensitive Information**

***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. 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
- 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

## Mailings

VA sends thousands of pieces of mail to individuals and thousands of batches of form letters every week. It is a big challenge to get it right every time. Many VA facilities also have a locally approved mail system to transfer paper files among staff at the facility.

Each piece of internal mail or U.S. mail must be handled with a commitment to protect sensitive information.

### More Information

#### *Internal office mail services*

- Place documents in closed interoffice envelopes
- Place a Notice Sheet in the closed interoffice envelope when contents include sensitive information
- Place documents with VA sensitive information in sealed envelopes inside the interoffice envelope for added safety. If you are sending PHI via interoffice mail, you are required to use a HIPAA sealed envelope
- Include the name of the recipient and verify his or her mail center address before sending
- Distribute interoffice mail to the correct addresses right away
- Transport VA sensitive information in secure containers or briefcases

#### *Regular mail or delivery services*

When using the U.S. Postal Service (USPS) or other delivery services, keep this checklist in mind:

- Pack envelopes, parcels, packages, and boxes in a way that will prevent loss, tampering, or unauthorized access
- Verify the person’s name on the envelope matches the person’s name on the documents inside the envelope
- Confirm envelopes are securely sealed
- Make sure mass-produced letters and mail merges that contain VA sensitive information are sealed prior to delivery to the approved shipping service

- Check the recipient name and mailing address
- Confirm that mailing labels and window envelopes show only the recipient's name and address and no other information
- Send original documents and all media that contain VA sensitive information through a shipping service with tracking capabilities, such as USPS, United Parcel Service (UPS), or FedEx (Copies of documents containing VA sensitive information may be sent through the untracked USPS)

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Sensitive Information**

***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)). SOURCE: UL-2

## Making the Connection: Sarah's Story

### Handling Prescription Mailings

Whenever I call to get my prescription refilled, it always seems like the first time. I've noticed that they carefully cross-check my information with what is in the database.

Because my address had changed, the pharmacist asked a few additional questions to validate my identity before mailing my prescriptions.

After the call, I completed the customer satisfaction survey. I am glad they are always thorough by confirming my information each time my prescription is issued. Getting the wrong prescription could make me sick or even put my life at risk—and could give someone else my personal information.

VA's mail order prescription drug service sends out millions of packages each year with very few errors. Sending a prescription to the wrong person would expose a Veteran's personal information, and it could also be harmful or even fatal to the recipient.

## Consolidated Mail Outpatient Pharmacy (CMOP)

In addition to forms, letters, and other documents, VA also mails several million prescriptions and medications to Veterans each week through its Consolidated Mail Outpatient Pharmacy (CMOP). If you handle CMOP-related packages and materials in your job, it is especially important to follow mailing procedures precisely.

### More Information

VA has a tremendous record of very few errors in handling CMOP mailings. However, even one small mistake in handling or mailing a CMOP package is not only a security and privacy violation, it could also be damaging or even fatal to the recipient. Always double-check the recipients' names and addresses if you ever handle CMOP packages and materials.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Sensitive Information**

***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. SOURCE: SC-13

***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

## Electronic Files

Many of us work with electronic media or electronic storage. If you work for IT, you may also have responsibility for electronic information systems. Privacy and information security rules must be followed when creating, storing, or disposing of electronic media and when accessing electronic files or administering electronic information systems, such as Microsoft SharePoint®.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Electronic Data Protection**

***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)). 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

**Sensitive Information**

***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. 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

## Electronic Records

Just like paper files and documents, electronic files may be records. Be sure to also consult your designated records management official before disposing of any electronic media, media storage, or electronic information systems that may be records. Records may not be destroyed before the date noted in the RCS or GRS. Never destroy records without permission. All types of electronic media, storage, or systems that may contain VA sensitive information must be sanitized or destroyed when no longer in use.

Ask your ISO for help with the sanitization and disposal or redistribution of electronic media. Here are some examples of these items:

- Electronic media: Emails, Excel and Access spreadsheets; JPEG, TIF, and HTML files; flat files; Word documents, PDF documents
- Electronic media storage: Magnetic tapes, floppy disks, CDs/DVDs, and external hard drives
- Electronic information systems: Concur Government Edition (CGE), VA electronic time and attendance system, VATAS or WEB TA

### Rules of Behavior

**1. COVERAGE**

1d. 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.

**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

***I Will Not:***

- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8

## Microsoft SharePoint

VA has approved Microsoft SharePoint for you to use for online data storage and collaboration to share documents and files with those who are allowed to access them. SharePoint is found on the VA Intranet.

Your ISO, CIO, and PO can help you determine which types of information can be shared on specific SharePoint sites.

Here are some tips to protect VA sensitive information on SharePoint:

- Share VA sensitive information only on sites where access is limited to individuals who are approved to access the information
- Request access only for the sites you need to use to do your job
- Share only the information your work unit needs to share to do its job
- Remove content from SharePoint periodically as it becomes outdated

Protect records stored on SharePoint in these ways:

- List the SharePoint sites in the work unit's file inventory

- Ask your designated records management official to schedule the disposition of these records if they are unscheduled
- Consult with your designated records management official prior to destroying any information that may be a record stored in SharePoint

### Rules of Behavior

**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

## Transporting VA Sensitive Information

You must get written permission from your supervisor, CIO, and ISO before you can remove any VA sensitive information from a VA facility or office. They must also approve how the information will be removed (i.e., electronic or paper format) and how any electronic devices will be stored while off-site.

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**Electronic Data Protection**

***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)). SOURCE: SC-13

**Sensitive Information**

***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)). SOURCE: UL-2

| Knowledge Check: Transporting Information |
| --- |
| Consider the following question by selecting the best answer. |
| Who must give permission to remove VA sensitive information from a VA facility or office?<br><br>A. PM, Quality Management, or HR<br>B. HR, ISO, and System Administrator<br>C. Supervisor, CIO, and ISO<br>D. Network Administrator, System Administrator, or CIO |
| The correct answer is C. You must get written permission from your supervisor, CIO, and ISO before you can remove any VA sensitive information from a VA facility or office. They must also approve how the information will be removed and how any electronic devices will be stored while off-site. |

## Connecting Points

Here are the connecting points to recall when handling documents and files:

- Protect VA sensitive information when handling documents and files
- Prevent mismailing by following procedures and checking recipients and addresses are correct
- Use only approved methods to store or transport electronic documents

# Module 8. Recognizing and Reporting Incidents

## Objectives

Throughout this course, we've shown you examples of threats and risks to VA privacy and security and tips for preventing privacy or information security incidents. But what do you do if prevention doesn't work? What if you suspect a rules violation is putting information at risk in your work team? What if you get an email from an external source claiming to be an ISO asking for personal information? Who do you contact if you suspect someone has tried to access your VA-issued laptop?

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

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

## What Are Incidents?

Incidents are defined as actual or potential privacy and information security violations. The threats and risks that were described in previous topics are situations that can result in incidents. VA takes all incident reports seriously, even if they are only suspected incidents.

Examples of suspected incidents that should be reported include:

- Finding a folder that contains VA sensitive papers on a copier
- Finding two loose mailing labels on the ground that are addressed to patients
- Receiving a call from a Veteran that his CMOP package contained the wrong amount of pills
- 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

Incidents that threaten privacy and security affect VA, Veterans, and you.

### More Information

***Examples of the impact***

- Veterans may be harmed if their Sensitive Personal Information is made public; they could have a financial loss, loss of privacy, loss of benefits, emotional distress, or possibly even identity theft
- If you violate the ROB resulting in an incident, you could face job loss, fines, and possibly prison if there is great harm caused by the violation

- VA may lose the public's trust
- VA may have to report the incident to Congress, especially if the incident is an information data breach affecting a large number of Veterans
- VA resources that could be spent to serve Veterans must be spent instead to correct mistakes
- Certain kinds of incidents could threaten our national security

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**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

## Consequences if You Cause an Incident

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:

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

### Rules of Behavior

**2. COMPLIANCE**

2a. 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.

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**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

## Severe Penalties

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

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

Other penalties

- Penalties for mishandling records: The maximum penalty for the willful and unlawful destruction, damage, or alienation of federal records is a $2,000 fine, 3 years in prison, or both
- Penalties for violating the Privacy Act: You can face up to $5,000 in fines and a year in prison
- Penalties for HIPAA violations: You can face fines from $100 to $1.5 million and potential jail time
- More penalties may apply for violating laws protecting PHI

### More Information

***Penalties***

These penalties are defined in 36 Code of Federal Regulation (CFR) § 1228.102.

### Rules of Behavior

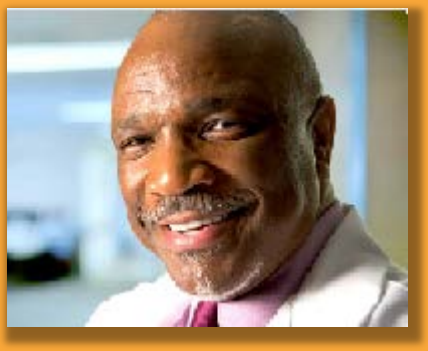
**2. COMPLIANCE**

2a. 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.

## Making the Connection: Dr. Sawyer's Story

### Reporting a Policy Violation

Yesterday when I left work at the VA medical center, I saw a stack of computer printouts sitting next to a dumpster. There were lists of patient names and addresses in that stack.



I immediately reported it as an incident. I took the box and delivered it to the VA security officer at the security desk in the lobby. He took it from there. I'm glad I was able to connect with someone who knew how to handle the situation.

Taking action when you see possible incidents can prevent major consequences.

## Steps for Reporting Suspected Incidents

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

Step 1. Note the details. What happened? Where did it happen? When did it happen? Who was involved? Why do you think it might be a rules violation?

Step 2. Report it:

- Employees: Report suspected or identified incidents to your supervisor and ISO or PO immediately. If you do not know the name of your ISO or PO, you can check the locator link provided in the Resources section. If you work in VHA, you can also report incidents to your Administrator of the Day (AOD)
- Contractors: Report every incident to your ISO or PO and also to your COR and Project Manager. All suspected or identified incidents must be reported immediately

### More Information

Your ISO or PO must report the incident to VA NSOC within one hour of being discovered or reported.

Report to NSOC by calling the VA National Service Desk (see the Resources section for contact information).

### Rules of Behavior

**4. INFORMATION SECURITY RULES of BEHAVIOR**

**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

| Knowledge Check: Steps for Reporting Suspected Incidents |
| --- |
| Consider the following question by selecting the best answer. |
| To whom can you report if you witness a suspected incident?<br><br>A. Your supervisor and ISO (or COR and Project Manager if you are a contractor)<br>B. Your PO<br>C. NSOC through the VA National Service Desk<br>D. Any of the above |
| The correct answer is D. Any of the above. Report suspected or identified incidents to your supervisor and ISO, PO, or NSOC through the VA National Service Desk. If you are a contractor, also report incidents to your COR and Project Manager. If you notice anything that may put VA sensitive information or information systems at risk, report it. |

## Other Resources to Report Incidents

If you are unable to report an incident to your supervisor, ISO, PO, or VHA Administrative Officer of the Day (AOD), here are some more resources:

- To report security incidents directly to VA NSOC, contact the VA National Service Desk
- If you suspect an unethical or criminal act is occurring, contact local VA police, the VA Office of Inspector General (OIG), and your supervisor (or COR), ISO, and/or PO
- If you suspect fraud, waste, or mismanagement of resources, contact the VA OIG
- If you suspect your supervisor is involved in the incident, report the incident to your ISO and/or PO

## Connecting Points

Here are the connecting points to recall to help you when reporting incidents:

- Report any suspected or identified incident right away

- Report suspected or identified incidents to your supervisor (or COR) and ISO or PO
- Report an incident directly to NSOC by contacting the VA National Service Desk, if your supervisor or COR, ISO, and/or PO are not available

Never be afraid to report an incident. Any time you hear or see something of concern, report it immediately.

# Module 9. Course Summary and Rules of Behavior

## Course Summary

Privacy and information security policies, guidelines, and best practices are here to help protect you, VA, Veterans, and their families. To protect privacy and ensure information security, remember to:

- Protect VA sensitive information
- Recognize how technologies and applications can compromise VA sensitive information
- Prevent attacks on information systems and networks
- Take precautions to prevent theft or loss of VA-issued electronic devices
- Take care with private conversations and messaging
- Handle paper and electronic documents and records safely
- Recognize and report incidents

## Acknowledge, Accept, and Comply With the ROB

Your last step to complete this course is to review, sign, and accept the Rules of Behavior.

Working for VA, you may access and use VA information systems or you may come in contact with VA sensitive information. This means you must accept responsibility for protecting privacy and ensuring information security. The ROB are the minimum compliance standards for VA personnel in all locations. If your location has rules that are stricter than the Information Security rules, you must obey them. You must complete training and formally acknowledge, accept, and comply with the ROB each year to receive and retain access to VA sensitive information or information systems.

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

To complete this training, you must initial and sign the ROB.

### Instructions for Signing the Rules of Behavior

In order to complete the signature step, first print the ROB document, Appendix A: VA Information Security Rules of Behavior.

To acknowledge and accept the ROB:

- Initial each printed page with your initials where indicated

- Sign the last page of the document where indicated

### Submitting Your Signed ROB

Once you have completed initialing and signing the ROB document, you must submit the signed document to your supervisor or designee for documentation of course completion.

## Course Completion

Congratulations! When you have signed and submitted the ROB, you have successfully completed the VA Privacy and Information Security Awareness and Rules of Behavior training.

Now that you have completed this course, you should be able to:

- Identify the types of information that must be handled carefully to protect privacy
- Describe what you are required to do to protect privacy when handling VA sensitive information
- Describe what you are required to do to protect privacy when using electronic devices
- Recognize privacy and information security laws and the penalties for non-compliance
- Explain the process for reporting incidents.

You should now be prepared to protect privacy, ensure the security of VA sensitive information, and comply with the Rules of Behavior.

### Rules of Behavior

**3. ACKNOWLEDGE**

3a. 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.

# APPENDIX A: Department of Veteran Affairs Information Security Rules of Behavior

## 1. COVERAGE

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

b. *Organizational* users are identified as VA employees, contractors, 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.

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

_____
Initials

## 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

_____
Initials

- 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 01&T employee. SOURCE: MP-4
- Attempt to override, circumvent, alter or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff. SOURCE: CM-3

**Electronic Data Protection**

***I Will:***

- Only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA. SOURCE: SI-3
- Safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using FIPS 140-2 validated encryption (or its

_____
Initials

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

_____
Initials

- 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 OI&T to perform maintenance on IT components, including installation or removal of hardware or software. SOURCE: MA-5
- Sign specific or unique ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity's ROB to conduct VA business. While using their system, I must comply with their ROB. SOURCE: PL-4

_____
Initials

**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

_____
Initials

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. SOURCE: IA-5 (1) (c)
- 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

_____
Initials

**5. ACKNOWLEDGEMENT AND ACCEPTANCE**

a. I acknowledge that I have received a copy of VA information Security Rules of Behavior.
b. I understand, accept and agree to comply with all terms and conditions of VA Information Security Rules of Behavior.

_____ _____

Print or type your full name Signature Date

_____ _____

Office Phone Position Title

_____

Initials

# APPENDIX B: Glossary

### A

**Active Directory Rights Management Service (RMS) Encryption—**VA-approved program that 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

**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.**

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

**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.**

### B

**Blog—**An online journal. A blog (shortened from "Web log") is an online journal that may be personal or topical, which the author makes regular entries that appear in reverse chronological order and can be read by the general public. Source: Wordsmith Educational Dictionary and Thesaurus

**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.**

**Breach**—The loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. SOURCE: 38 U.S.C. § 5727 May or may not be a breach under the HIPAA Privacy and Security Rules, which define “breach” as the unauthorized acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Under these Rules, breach of PHI excludes a. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the covered entity or business associate and does not result in further use or disclosure; b. Any inadvertent disclosure from an individual who

is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and c. Any such information received as a result of such disclosure is not further acquired, accessed, or used. Source: VA Handbook 6500

**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.**

## C

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

**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.**

**Cloud—**A computing model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The model has essential characteristics (on-demand self-service broad network access, resource pooling, rapid elasticity, and measured service), three service models (software as a service, platform as a service, and infrastructure as a service), and four deployment models (private cloud, community cloud, public cloud, and hybrid cloud). Source: NIST Special Publication 800-145, The NIST Definition of Cloud Computing

**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.**

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

**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.**

**Continuous Readiness in Information Security Program (CRISP)—**A program launched by VA's Office of Information and Technology designed to transform how VA accesses, protects, and transfers information within and outside of VA. The program standardizes how VA monitors and controls onboarding, offboarding, appropriate access, and training compliance for all VA system users. Source: VA Memorandum VAIQ #7227211, Continuous Readiness in Information Security Program (CRISP) Sustainment Phase

**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.**

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

**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.**

**D**

**Designated Records Management Official—**A person designated to serve as the records officer for an organization, with oversight responsibilities for the management, retention, and disposition of VA records for his or her respective organization, to include Central Office program offices and respective field facilities that fall under his or her purview. Note that the title of this official may vary from one organization to the next. Other titles include, but are not limited to, Records Officer, Records Liaison Officer, Records Management Officer, Records Management Technician, and Records and Information Management Specialist. This designated official works in cooperation and coordination with the VA Records Officer. Source: Adapted from VA Handbook 6300.1

**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.**

**Disclosure—**The act of making VA knowledge or facts known. 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: VA Directive 6502

**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.**

**E**

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

**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.**

**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. Source: W3C Glossary

Dictionary

**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.**

**F**

**Facebook—**A web-based social network site. Facebook is a social utility that connects people with friends and others who work, study, and live around them. People use Facebook to keep up with friends, upload an unlimited number of photos, post links and videos, and learn more about the people they meet. Source: Facebook

**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.**

**Federal Information Processing Standard (FIPS) 201—**Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors was developed to establish standards for identity credentials. This standard specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems. Source: NIST

**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.**

**Federal Information Security Management 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: NIST SP 800-63

**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.**

**Federal Records Act—**A law that requires VA to maintain a system of records. The Federal Records Act requires federal agencies to make and preserve records that have adequate and proper documentation of their organizations, functions, policies, decisions, procedures, and essential transactions. These records are federal property and must be maintained and managed according to laws and regulations. Source: http://www2.ed.gov/policy/gen/leg/fra.html

**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.**

**File plan—**A document containing the identifying number, title or description, and disposition authority of files held in an office. The file plan should contain up-to-date and accurate disposition authorities and retention periods for all records and nonrecord

materials maintained in the office. Source: http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/

**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.**

**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: http://www.flickr.com/help/general/

**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.**

**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: http://www.foia.va.gov/

**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.**

## G

**General Records Schedule (GRS)—**General Records Schedules (GRS) are issued by the Archivist of the United States to provide disposition authorization for records common to several or all agencies of the federal government. They include records relating to civilian personnel, fiscal accounting, procurement, communications, printing, and other common functions and certain nontextual records. They also include records relating to temporary commissions, boards, councils, and committees. These records comprise an estimated one-third of the total volume of records created by federal agencies. Source: National Archives and Records Administration (NARA)

**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.**

**Google**+—A web-based social network site that lets users with similar interests share links, videos, pictures, and other content. Source: Google+

**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.**

## H

**Health Information Technology for Economic and Clinical Health Act (HITECH)—**A law that describes when and how VA hospitals and doctors can exchange a person's health information. The HITECH Act of the American Recovery and Reinvestment Act imposes more stringent regulatory requirements under the security and privacy rules of Health Insurance Portability and Accountability Act (HIPAA), increases civil penalties for a violation of HIPAA, provides funding for hospitals and physicians for the adoption of health information technology, and requires notification to patients of a security breach.

These broad new requirements will necessitate compliance by covered entities, business associates, and related vendors in the health care industry. Source: http://www.nixonpeabody.com/117927

**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.**

**Health Insurance Portability and Accountability Act (HIPAA) and HIPAA Privacy Rule (1996)—**A law that requires VA to keep a person's health information private.

HIPAA establishes requirements for protecting privacy of personal health information. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system. Source: http://www.hipaa.com/

**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.**

I

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

**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.**

**Incident**—An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Source: VA Handbook 6500

**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.**

**Information Security—**Keeping VA sensitive information safe. Information security is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. Source: VA Handbook 6500

**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.**

**Instagram—**A web-based photo sharing site. Users share images, graphics, photos, and short videos with friends. Source: Instagram

**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.**

**Instant message (IM)—**Used to send a real-time note to another Internet user. Instant message (IM) allows users to see the current availability of others and to start a real-time, online conversation with them. Source: Microsoft

**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.**

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

**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.**

**J—N/A**

**K—N/A**

**L**

**Local area network (LAN)—**A data communication system allowing a number of independent devices to communicate directly with each other, within a moderately sized geographic area over a physical communications channel of moderate rates. Source: VA Handbook 6500

**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.**

**M**

**Malware—**Software designed to harm a computer or system. Malware is a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. Source: NIST SP 800-83

**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.**

**Microsoft Lync—**Software used to instantly communicate with colleagues. Microsoft Lync is an enterprise-ready unified communications platform. Lync provides a consistent, single client experience for presence, instant messaging, voice, and video. Source: Microsoft

**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.**

**Microsoft Outlook Calendar—**Software used to chart daily, weekly, monthly, or yearly events. Microsoft Outlook Calendar is the calendar and scheduling component of Outlook and is fully integrated with email, contacts, and other features. Source: Microsoft

**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.**

**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: Microsoft

**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.**

**N**

**Non-organizational users—**Are identified as all information system users other than VA users explicitly categorized as organizational users. Source: VAIQ 7714283, Modified VA Information Security Rules of Behavior, August 24, 2016

**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.**

**Notice Sheet—**A sheet of paper for internal mail that is a cover sheet that accompanies documents sent through interoffice mail that contain VA sensitive information. However sent, every individual article or grouping of mail that contains VA sensitive information and is sent from VA to any VA personnel must be accompanied by a notice sheet containing language that explains there are penalties for violations of the Privacy Act and the Health Insurance Portability and Accountability Act Privacy Rule. These notice sheets must be inserted as cover sheets to the document. Source: VA Directive 6609

**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.**

**O**

**Organizational users**—Are identified as VA employees, contractors, researcher, students, volunteers, and representatives of federal, state, local, or tribal agencies. Source: VAIQ 7714283, Modified VA Information Security Rules of Behavior, August 24, 2016

**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.**

**P**

**Paper logbooks—**A written, non-electronic record intended to track information for someone's personal use. Paper logbooks for personal use include any record of activity or events comprising data that may uniquely identify an individual or contain sensitive personal information and are maintained over a period of time for the purpose of tracking information or creating a historical record for one's own use. Source: VA Memorandum VAIQ #7092263, Prohibition of Written Logbooks

**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.**

**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

**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.**

**Personal Identity Verification (PIV) cards—**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: http://www.va.gov/pivproject/

**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.**

**Personally Identifiable Information (PII)—**PII is any information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security number, biometric records, etc., alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be Personally Identifiable Information. Source: Office of Management and Budget (OMB) Memorandum 07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information (May 22, 2007) Note: The term Personally Identifiable Information is synonymous and interchangeable with Sensitive Personal Information.

**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.**

**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

**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.**

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

**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.**

**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 twelve 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: http://www.justice.gov/opcl/privacyact1974.htm

**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.**

**Privacy Impact Assessment (PIA)—**A PIA is an analysis that seeks to identify and mitigate the privacy and security risks associated with the use of PII by a program, system, or practice. A PIA provides a framework for examining whether privacy, security, and other vital data issues have been identified, addressed, and incorporated into the plan, design, operation, maintenance, and disposal of electronic information systems. PIAs are required to be performed in the conceptualization phase of the system life cycle and updated whenever a system change could create a new privacy risk. Source: VA Directive 6508

**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.**

**Privacy Screen—**A screen that can be fastened to a computer monitor to keep data out of view. A privacy screen is a panel that limits a computer screen's angle of vision to a front view so that visitors in the room cannot casually see the display. Also called a "privacy filter," it is attached directly over the screen, which helps prevent scratches and abrasions. Source: PCMag.com Encyclopedia

**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.**

**Privacy Threshold Analysis (PTA)**—A PTA is used to identify IT systems, rulemakings for privacy risks, programs, or projects that involve PII, and other activities that otherwise impact the privacy of individuals as determined by the Director or VA Privacy Service and to assess whether there is a need for a Privacy Impact Assessment (PIA). A PTA includes a general description of the IT system, technology, rulemaking, program, project, or other Department activity and describes what PII is collected (and from whom) and how that information is used. Source: VA Handbook 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment

**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.**

**Prohibited activities—**Using VA-issued devices for inappropriate actions. Prohibited activities include, but are not limited to, uses that causes congestion, delay, or disruption to any system or equipment; use of systems to gain unauthorized access to other systems; the creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings; use for activities that are illegal, inappropriate, or offensive to fellow employees or the public; the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials; the creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, or other illegal or prohibited activities; use for commercial purposes or "for profit" activities or in support of outside employment or business activities, such as consulting for pay, sale or administration of business transactions, or sale of goods or services; engaging in outside fundraising activity, endorsing any product or service, or engaging in any prohibited partisan activity; participating in lobbying activity without authority; use for posting agency information to external news groups, bulletin boards, or other public forums without authority; use that could generate more than minimal expense to the government; and the unauthorized acquisition, use, reproduction, transmission, or distribution of privacy information, copyrighted, or trademarked property beyond fair use, proprietary data, or export-controlled software or data. Source: VA Directive 6001

**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.**

**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: 45 C.F.R. § 160.103; VA Directive 6066

**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.**

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

**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.**

**R**

**Records—**Formal written facts about a person or VA. Records are defined differently in the Privacy Act and the Federal Records Act. Both definitions must be considered in handling VA records. (1) Records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them. Source: Federal Records Act (44 U.S.C. 3301). (2) Record means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history, which contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. Source: VA Handbook 6300.1 and VA Handbook 6300.5

**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.**

**Records Control Schedule (RCS)—**A document that contains the retention and disposition rulings as approved by NARA that describes how long scheduled VA records must be maintained before being disposed of. A Records Control Schedule is required by statute. All VA records and information must be identified by records series and be listed in the aforementioned Records Control Schedule. Source: Adapted from VA Handbook 6300.1

**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.**

**Records inventory—**A descriptive listing of each record series or system, together with an indication of location and other pertinent data. It is not a list of each document or each folder but rather of each series or system. Its main purpose is to provide the information needed to develop the schedule. It also helps identify various records management problems. These include inadequate documentation of official actions, improper applications of recordkeeping technology, deficient filing systems and maintenance practices, poor management of nonrecord materials, insufficient identification of vital records, and inadequate records security practices. When completed, the inventory should include all offices, all records, and all nonrecord materials. An inventory that is incomplete or haphazard can only result in an inadequate schedule and loss of control over records. Source: http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/

**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.**

**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

**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.**

**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 800-53

**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.**

**Remote Enterprise Security Compliance Update Environment (RESCUE)**—A program used by VA to provide employees with remote access using government-furnished equipment (GFE). Source: https://rescue.vpn.va.gov/FAQ

**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.**

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

**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.**

## S

**SafeNet MobilePASS—**SafeNet MobilePASS soft token is the alternative for non-PIV enabled devices (e.g., no USB port or card reader) to satisfy two-factor authentication requirements for access. The application installs a token on the device and makes the device the something you have in two-factor authentication. Source: Modified from VA FSS Bulletin No. 270, VA Remote Access: Citrix Access Gateway (CAG): Two-Factor Authentication Implementation Schedule

**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.**

**Sensitive Personal Information (SPI)—**The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records. NOTE: The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information." Source: 38 U.S.C. § 5727

**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.**

**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

**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.**

**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. This form of media does not include email. Source: VA Directive 6515

**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.**

**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

**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.**

**T**

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

**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.**

**Tweets—**Brief messages sent through Twitter. Tweets are small bursts of information that are no more than 140 characters long. Additionally, users can include and see photos, videos, and conversations directly in Tweets to get the whole story at a glance and all in one place. Source: Twitter

**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.**

**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: Twitter

**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.**

**Two-factor authentication—**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: Modified from NIST Special Publication 800-63-2, Electronic Authentication Guideline

**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.**

**U—N/A**

## V

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

**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.**

**VA Pulse—**A web-based social networking site for VA employees. VA Pulse is a collaborative platform for staff to share best practices, connect with colleagues to solve problems, and discover ideas to help improve the Veteran experience. Source: VA Pulse

**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.**

**VA sensitive information—**VA sensitive information/data is all Department information and/or data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under various confidentiality provisions. Source: 38 U.S.C. Section 5727

**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.**

**VAntage Point**—The official blog of VA. VA employees provide information to Veterans in posts and articles featured on VAntage Point. Others can also contribute and submit content for publication. Source: http://www.blogs.va.gov/VAntage/about/

**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.**

**Virtual local area network (VLAN)—**A network of physical networks divided into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through configuration of Ethernet switches. Source: NIST Special Publication 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security

**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.**

**Virtual Private Network (VPN)**—A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Source: Virtual Private Network Consortium

**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.**

**W**

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

**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.**

**Wireless Network—**A network of computers that are 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: http://compnetworking.about.com/cs/wireless/f/whatiswireless.htm

**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.**

**X—N/A**

**Y—N/A**

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

Source: YouTube. (n.d.). Dictionary.com Unabridged. Retrieved May 26, 2015, from Dictionary.com

**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.**

**Z—N/A**

# APPENDIX C: Privacy and Information Security Resources



| Table 1. VA Phone Numbers |
| --- |
| **Identity Theft Help Line** (to report an identity theft incident involving a Veteran) (855) 578-5492 |
| **Office of Inspector General (IG) Hotline** (to report fraud, waste, or mismanagement of resources)<br>(800) 488-8244 |
| **VA National Service Desk** (to request computer, network, or access support; or to report security incidents to the Network Security Operations Center [NSOC])<br>(855) 673-4357.<br>Select option 6 for Computer, Network, or Access Support. Select option 4 for NSOC. |

| Table 2. VA Web Links |
| --- |
| *These links are only accessible on the VA Intranet |
| **CRISP information***<br>https://vaww.sde.portal.va.gov/oitauditprep/SitePages/Home.aspx |

| Table 2. VA Web Links |
|---|
| **FSS HISD SharePoint site for MDPP guidance*** https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/HISD.aspx |
| **Information Security Portal*** https://vaww.portal2.va.gov/sites/infosecurity/index.aspx |
| **ITWD's role-based training*** http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Pages/default.aspx |
| **Locator to identify ISOs*and POs** https://vaww.portal2.va.gov/sites/infosecurity/ISO-PO-Locator/default.aspx |
| **PIV cards** http://www.va.gov/PIVPROJECT/index.asp |
| **Remote access solutions*** https://vpnportal.vansoc.va.gov/Default.aspx?strSource=u+ICXXnt3TlrIVosSsqAABgr Af O5euqrcalEYQjZ0d7TQ+n8hKoNYUEUKNucaA2wE7Cdxa4vj6MmCL1waoAFIw |
| **Rights Management Service (RMS)*** http://vaww.help.portal.va.gov/RMS/Lists/External%20RMS%20Enabling%20Request/AllItems.aspx |
| **Role Definitions PDF document*** http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Shared%20Documents/ Role%20Definitions.pdf |

| Table 3. VA TMS Courses |
|---|
| Available at: https://www.tms.va.gov/ |
| TMS ID 10203, Privacy and HIPAA Training |
| TMS ID 336914, An Introduction to Rights Management Service—RMS |

| Table 3. VA TMS Courses |
| --- |
| TMS ID 1256927, Getting Started with Public Key Infrastructure |
| TMS ID 2626967, Social Networking and Security Awareness |
| TMS ID 3858544, Social Engineering—Hacking Human Nature |
| TMS ID 3926743, Mobile Training: Apple Native Email Client |
| TMS ID 3926744, Mobile Training: Security of Apps on iOS Devices |

| Table 4. Privacy Laws and Regulations |
| --- |
| Available at: http://www.privacy.va.gov/privacy_resources.asp |
| **Freedom of Information Act (FOIA)**<br>Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions. |
| **Health Information Technology for Economic and Clinical Health Act (HITECH)** Describes when and how hospitals, doctors, and certain others may safely exchange individuals' health information. It also limits the use of personal medical information for marketing purposes and increases fines for unauthorized disclosures of health information. |
| **Health Insurance Portability and Accountability Act (HIPAA)**<br>Establishes requirements for protecting privacy of personal health information. |
| **Paperwork Reduction Act**<br>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. |
| **Privacy Act**<br>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 |

| Table 4. Privacy Laws and Regulations |
| --- |
| about themselves. |
| **Freedom of Information Act (FOIA)**<br>Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions. |
| **Health Information Technology for Economic and Clinical Health Act (HITECH)** Describes when and how hospitals, doctors, and certain others may safely exchange individuals' health information. It also limits the use of personal medical information for marketing purposes and increases fines for unauthorized disclosures of health information. |

| Table 5. Information Security Laws, Regulations, and Related Statutes/Specifications |
| --- |
| **Federal Information Security Modernization Act(FISMA)**<br>http://www.dhs.gov/files/programs/gc_1281971047761.shtm<br>Requires federal agencies to have a program to assess risk and protect information and information security assets that support agency operations. |
| **Federal Records Act of 1950**<br>http://www2.ed.gov/policy/gen/leg/fra.html<br>Describes federal agency responsibilities for making and preserving records and for establishing and maintaining active, continuing programs for the economic and efficient management of the records agency. (Related regulations: 44 U.S.C. Chapters 21,29,31,33 and 35 (Federal Records Act); 36 CFR Chapter XII, Subchapter B - Records Management Part 1220-1238;and OMB Circular A-130 Management of Federal Information) |
| **Internal Revenue Code (IRC) Specifications IRC at 26 U.S.C.A. § 6103 (p)(4).**<br>http://www.patentofficelawsuit.info/irs_6103.htm<br>Requires specific security protection for income tax return information (as |

| Table 5. Information Security Laws, Regulations, and Related Statutes/Specifications |
|---|
| defined in§ 6103 [b] [2]) that is provided to VA electronically under income verification matching (IVM) agreements with the Internal Revenue Service and the Social Security Administration. Tax information submitted to VA by the taxpayer is protected by the Privacy Act, but does not require the specialized care specified by §6103. |
| **Federal Information Security Modernization Act (FISMA)**<br>http://www.dhs.gov/files/programs/gc_1281971047761.shtm<br>Requires federal agencies to have a program to assess risk and protect information and information security assets that support agency operations. |
| **FIPS 140-2**<br>Security Requirements for Cryptographic Modules |
| **Federal Records Act of 1950**<br>http://www2.ed.gov/policy/gen/leg/fra.html<br>Describes federal agency responsibilities for making and preserving records and for establishing and maintaining active, continuing programs for the economic and efficient management of the records agency. (Related regulations: 44 U.S.C. Chapters 21,29,31,33 and 35 (Federal Records Act); 36 CFR Chapter XII, Subchapter B - Records Management Part 1220-1238;and OMB Circular A-130 Management of Federal Information) |

| Table 6. Selected VA Privacy Handbooks and Directives |
|---|
| Available at: http://www1.va.gov/vapubs/index.cfm |
| VA Directive 6066, Protected Health Information(PHI) |
| VA Directive 6300, Records and Information Management |
| VA Directive 6371, Destruction of Temporary Paper Records |
| VA Handbook 6300.4, Procedures for Processing Requests for Records Subject |

| Table 6. Selected VA Privacy Handbooks and Directives |
| --- |
| to the Privacy Act |
| VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act System of Records |
| VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program and Appendix D, VA National Rules of Behavior |
| VA Handbook 6500.1, Electronic Media Sanitization |
| VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information |
| VA Handbook 6502, VA Enterprise Privacy Program |
| VA Handbook 6502.4, Privacy Act Review |
| VA Handbook 6512, Secure Wireless Technology |
| VA Handbook 6609, Mailing of Personally Identifiable and VA Sensitive Information |
| VHA Directive 1605, VHA Privacy Program |
| VHA Handbook 1605.1, Privacy and Release of Information |
| VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information |

| Table 7. Additional Selected VA Handbooks and Directives |
| --- |
| Available at: http://www1.va.gov/vapubs/index.cfm |
| VA Directive 0701, Office of Inspector General Hotline Complaint Referrals |
| VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program |
| VA Directive 6515, Use of Web-Based Collaboration Technologies |

| Table 7. Additional Selected VA Handbooks and Directives |
| --- |
| VA Handbook 5011/5, Hours of Duty and Leave |
| VA Handbook 5011/26, August 9, 2013 Hours of Duty and Leave |
| VA Handbook 5021/3, Employee/Management Relations |
| VA Handbook 5021.6, Employee/Management Relations, Appendix A |
| VA Handbook 6300.1, Records Management Procedures |
| VA Handbook 6500, Appendix F, VA System Security Controls |
| VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior |
| VA Directive 0701, Office of Inspector General Hotline Complaint Referrals |
| VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program |
| VA Directive 6515, Use of Web-Based Collaboration Technologies |

| Table 8. Forms and Memorandums |
| --- |
| Available at: http://vaww.va.gov/vaforms/ |
| VA Form 0244, Records Transmittal and Receipt |
| VA Form 0740 New Telework Request Agreement, Aug 2013 |
| VA Form 7468, Request for Disposition of Records |
| VAIQ 7581492, Use of Personal Email |
| VAIQ 7633050, Mandatory Use of PIV Card Authentication for VA Information System Access |
| VAIQ 7714283, Modified VA Information Security Rules of Behavior, August 24, 2016 |