You make all the difference

VA Privacy and Information Security Awareness and Rules of Behavior

FY15 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

Using this Document ................................................................. 1

## Module 1: Welcome and Introduction

Who Must Take This Course? ....................................................... 2
Rules of Behavior (ROB) ................................................................. 3
Course Objectives ...................................................................... 4

## Module 2: Privacy and Security Basics

Module Objectives ..................................................................... 5
Protecting Privacy and Information Security ............................. 5
Protecting Privacy ..................................................................... 6
Types of VA Sensitive Information ............................................. 6
What are Records? ................................................................... 7
Information Security ................................................................ 9
Protecting VA Sensitive Information ........................................... 10
VA’s Continuous Readiness in Information Security Program (CRISP) ................................................................. 10
Strong Passwords .................................................................. 10
Personal Identity Verification (PIV) Cards ............................... 11
Who Can Provide Support? ....................................................... 13
Module Summary ..................................................................... 15

## Module 3: How to Recognize and Report Incidents

Module Objectives ..................................................................... 16
Reporting Incidents .................................................................. 16
Impact ...................................................................................... 17
Consequences If You Cause an Incident ................................. 17
Severe Penalties ........................................................................................................ 18
Steps to Report an incident ........................................................................................ 19
More Contacts ............................................................................................................ 19
Module Summary ....................................................................................................... 20

**Module 4: Conversations and Messaging............................................................... 21**
Module Objectives ..................................................................................................... 21
Routine Conversations ............................................................................................... 21
Private Conversations ............................................................................................... 22
Email Encryption ........................................................................................................ 23
Secure Email Practices .............................................................................................. 25
Electronic Calendars ............................................................................................... 26
Instant Messaging and Texting .................................................................................. 27
Module Summary ....................................................................................................... 27

**Module 5: Handling Paper and Electronic Documents Safely ......................... 28**
Module Objectives ..................................................................................................... 28
Requirements for Paper Documents, Records, and Files ........................................... 28
Handling Records and Faxing Paper Documents ...................................................... 30
Requirements for Using Mail and Delivery Services .................................................. 31
Paper Logbook ........................................................................................................... 33
Electronic Media ....................................................................................................... 35
Transporting VA Sensitive Information .................................................................... 36
Microsoft SharePoint .................................................................................................. 36
Module Summary ....................................................................................................... 37

**Module 6: Using VA Systems Securely ................................................................. 38**
Module Objectives ..................................................................................................... 38
Telework Guidance .................................................................................................... 38
Remote Access .......................................................................................................... 39
Wireless Devices and Networks ................................................................. 40
Social Engineering Attacks ........................................................................ 41
Threats to Systems, Software, and Networks ............................................. 42
Insider Threats ............................................................................................. 43
Preventing Attacks ...................................................................................... 44
Using Social Media .................................................................................... 45
Module Summary ........................................................................................ 46

Module 7: Managing Equipment and Electronic devices .................. 47
Module Objectives ....................................................................................... 47
Inventory Control for Electronic Devices ..................................................... 47
Protecting VA Sensitive Information from Theft or Loss ....................... 49
Requirements for VA Mobile Devices ......................................................... 51
Limited Personal Access and Use of VA-Issued Devices ....................... 53
Personal Electronic Devices ..................................................................... 53
Module Summary ........................................................................................ 54

Module 8: Course Summary and Rules of Behavior ........................ 55
Course Summary ........................................................................................ 55
Acknowledge, Accept, and Comply with the ROB ................................. 55
Course Completion ...................................................................................... 56

I. APPENDIX A: Rules of Behavior for VA Employees .............. 58
II. APPENDIX B: Rules of Behavior for VA Contractors .......... 69
III. APPENDIX C: Glossary ................................................................. 75
IV. APPENDIX D: Privacy and Information Security Resources .... 87
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) 2015 (i.e., October 1, 2014 through September 30, 2015).

You should take the online version of this course if possible. However, if you complete the course using this text-only transcript, you must print and sign the appropriate Rules of Behavior (ROB), as well as initial each page in the space provided. Sign Appendix A: Rules of Behavior for Employees if you are an employee; sign Appendix B: Rules of Behavior for Contractors if you are a contractor. 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 this Document

Throughout this document you are able to access more detailed information in the appendices 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 and Introduction

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

Who Must Take This Course?

VA must comply with federal laws about privacy and information security. This course will help you understand your roles and responsibilities for keeping VA sensitive information safe. You must complete this training to use or gain access to VA information systems or VA sensitive information. To maintain your access, you must complete this training each year.

All VA employees who use VA information systems or VA sensitive information must take this training, including:

- Paid employees
- Unpaid employees
- Volunteers

Contractors must also take this training if your contract states that the training is required.

Students or other trainees

If you are a medical 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 (VA TMS ID: 3185966).

Contractors

You must also take this training if your contract states that the training is required.

VHA and VBA employees and contractors

If you have access to Protected Health Information (PHI), you are also required to complete Privacy and Health Insurance Portability and Accountability (HIPAA) Training (VA TMS ID: 10203).
Did You Know?

Many laws require privacy and information security awareness training, including:

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

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

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

You can find more information in **Appendix D: Privacy and Information Security Resources**.

**Rules of Behavior (ROB)**

You must take this course as well as acknowledge and accept the VA **Rules of Behavior (ROB)** every year in order to use or maintain access to VA information systems or VA sensitive information. There are two versions of the ROB: one for VA employees and one for contractors. Both versions of the full ROB are found in the Appendices. Some offices or facilities require more rules and guidelines for increased protection. Always follow the ROB and your local rules.

When you are done with this course, you must acknowledge and accept these rules to earn credit before you exit the course. You can select links in the Applicable ROB boxes to view the specific rules that apply to each section’s content. Contractors may notice ROBs refer to a Contracting Officer’s Technical Representative, or COTR. The COTR is now known as the Contracting Officer Representative (COR). The rules cite the existing policy language.
Question and Answer

Which Rules of Behavior version applies to you?

**Employee**
Employees are all people who work for VA under Title 5 or Title 38, United States Code. This also includes volunteers, without compensation (WOC) employees, and students or other trainees. Employees must complete this training and acknowledge and accept the ROB to use, gain, or maintain access to VA information systems or VA sensitive information.

**Contractor**
Contractors are all non-VA employees who have been authorized to use or have access to VA information resources or VA sensitive information through a contract, agreement, or other legal arrangement. Contractors must complete this training and must acknowledge and accept the ROB to gain or maintain access to VA information systems or VA sensitive information.


**Course Objectives**

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

- Identify the types of VA sensitive information and information systems you are required to protect
- Describe the steps you must take to protect personal privacy, VA sensitive information, and information security
- Recognize the penalties you may face by failing to protect privacy and security
- Explain the process for reporting incidents that can compromise or possibly impact privacy and security
- Acknowledge, accept, and comply with the Rules of Behavior
Module 2: Privacy and Security Basics

Module Objectives

It is important that you understand your role for protecting privacy and information security at VA. When you have finished this module, you will be able to:

- Recall the types of VA sensitive information
- Explain basic ways to protect VA sensitive information
- Recognize common mistakes when communicating VA sensitive information

Now let’s explore the types of information to be protected. Throughout the course, there will be short stories about VA’s most commonly reported privacy and information security incidents. Mishandling of sensitive paper documents is the single most commonly reported type of incident at VA—and it can potentially cause great harm to VA and Veterans. Are you ready to take small steps to make a big difference?

Read this story about one person’s experience.

Know the difference, make a difference: Margie Makes a Difference

It was the end of the day, and I was ready to go home. I had some papers lying in a mess on my desk, and I tossed them in the trash. When I got to the elevator, I remembered there were two unneeded duplicate sheets of a Veteran’s benefit claim information that my supervisor approved for me to destroy. I went back to my desk, pulled the papers out of the trash, and locked them in my desk drawer. This morning I put the information in the shredder bin where it belonged. I’m glad I remembered before putting a Veteran’s information at risk.

Protecting Privacy and Information Security

You have a responsibility to protect Privacy and ensure information security. You must protect all types of VA sensitive information when you are:

- Speaking with others
• Handling paper records or electronic files
• Using email and other types of electronic communication
• Using electronic devices and VA information systems
• Using the Internet and social media

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

Privacy may be violated on purpose or by accident. To protect privacy, do not disclose, alter, or destroy VA sensitive information unless you have permission.

Protecting Privacy

VA sensitive information includes:

- Personally Identifiable Information (PII)
- Sensitive Personal Information (SPI)
- Protected Health Information (PHI)
- Internal Business Information (IBI)

Types of VA Sensitive Information

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

Both PII and SPI are VA sensitive information and refer to information about a specific person, such as:

- Name, address, and phone number
- Social Security number (including the last four digits)
- Date of birth
- Credit card numbers
- Education records
- Financial records
- Criminal and employment histories
Protected Health Information (PHI)

Protected Health Information (PHI) is VA sensitive information that 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

Internal Business Information (IBI)

Internal Business Information (IBI) is VA sensitive information that enables VA to meet its mission but is not public knowledge, such as:

- Pricing information submitted to VA by vendors during bid processes
- Facility or computer room diagrams
- Documentation of IT systems
- Operational business and information reports

What are Records?

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

The Federal Records Act of 1950 and later regulations require federal agencies to make and preserve records. Records document business activities. They are public property and must be managed according to the law. Every work unit at VA must keep a list of items that are records. This list is called a file plan. Records must be kept according to a Records Control Schedule (RCS) that is approved by the National Archives and Records Administration (NARA). The RCS explains how long certain records must be kept and how to dispose of them when they are no longer needed.

A document known as the General Records Schedule has more information about disposition. Records Officers and Records Liaisons manage records across VA administrations and facilities. Work with your local records team if you are creating, transporting, storing, or disposing of records to be sure VA sensitive information is protected.
Find more information about records in the Privacy and Information Security document in Appendix D: Privacy and Information Security Resources.

Did You Know?

Records

Examples of records include:

- Materials made or received by an agency of the U.S. Government under federal law or in connection with the transaction of public business and appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities, or because of the informational value of the data
- Information maintained to document how the organization is organized, its functions, its processes, its relationships with other agencies and to the public, or because the materials contain information that is of value to the agency
- Books, papers, maps, photographs, machine-readable materials, or documentary materials, regardless of physical form or characteristics

Nonrecords

Nonrecords are those items that are usually not included within the scope of official records, as well as documents not required or included on an RCS.

Examples of nonrecords include:

- Drafts and working papers or files that relate to routine program or administrative operations or that contain only corrections, editorial changes, or stylistic changes
- Extra copies of documents kept only for reference
- Stocks of publications and processed documents
- Library or museum materials intended solely for reference or exhibit
Knowledge Check: Types of VA Sensitive Information

What are the types of VA sensitive information? Review each type of specific information and determine what kind of VA sensitive information it is.

For each example listed below, identify whether it is PII, PHI, or IBI.

- Employee date and place of birth (The correct answer is PII)
- Facility or computer room diagrams (The correct answer is IBI)
- Patient payment history (The correct answer is PHI)
- Volunteer’s driver’s license number of birth (The correct answer is PII)
- Operational business and information reports (The correct answer is IBI)
- Patient appointment reminders (The correct answer is PHI)

Information Security

Information security is a set of principles and actions that make sure VA information systems and VA sensitive information are not accessed or changed by unauthorized people or systems and are available when we need them.

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

Did You Know

Confidentiality

Confidentiality means information is not 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.

**Protecting VA Sensitive Information**

Remember, it is your responsibility to keep VA sensitive information safe wherever you are working (e.g., a VA office, a hotel, or at home). VA’s [Continuous Readiness in Information Security Program (CRISP)](https://www.va.gov/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

**Did You Know?**

**VA’s Continuous Readiness in Information Security Program (CRISP)**

VA’s Continuous Readiness in Information Security Program (CRISP) is a program that incorporates security and privacy into everyone’s daily functions and provides ongoing security and privacy practices for VA’s environment.

**Strong Passwords**

VA requires strong passwords to protect VA sensitive information and information systems. To protect your VA-issued devices and your access to VA sensitive information, you must meet VA’s password requirements. Your password must have at least eight characters and have three of the following:

- Uppercase letters
- Lowercase letters
- Numbers (0–9)

**Applicable ROB**

Employee: 2b(8)

Contractor: 2b(8), 2b(9)
- Special characters (such as #, %, @)

**Note:** VA’s computer systems will not let you set a password that does not comply with this policy.

Remember to keep your passwords private. Store any written passwords in a locked drawer or cabinet. You will be required to change your password every 90 days. Never use someone else’s password or allow someone else to use your password or user identity to access a VA system.

**Did You Know?**

**Strong Passwords**

Strong passwords meet VA’s minimum password requirements. Examples of strong passwords include SSEufu6&* and TeLrk#@23g.

Avoid weak passwords that contain any of the following:

- Your username, a real name, or a company name
- Complete dictionary words
- Words that are similar to previous passwords
- Words using increments such as Password 1, Password 2
- Examples of weak passwords include Johndoe#1 and Veteransaffairs#2.

For more information on passwords, refer to VA Handbook 6500, Appendix F, VA System Security Controls.

**Personal Identity Verification (PIV) Cards**

VA employees and contractors who have access to VA buildings, networks, and resources are required to carry a **Personal Identity Verification (PIV) card**. PIV cards are required to increase protection of VA information and information systems. If a card is lost, it must be reported to the PIV office, the ISO, and your management.

An ordinary experience like this can be a security incident. If you lose or misplace your PIV card, you could be giving a dishonest person the opportunity to enter VA facilities or get access to Veterans’ information. A surprising number of people lose or misplace their VA PIV cards every year. Protect your PIV card and associated PIN to avoid becoming one of them!
You must protect your PIV card from loss or theft. Always keep it with you. Be careful not to leave it in the computer keyboard when you are gone, or put it down on chairs or tables in public places where you might forget it.

If an employee or contractor loses a card or leaves VA, his or her PIV card must be revoked in the system right away. If you are a supervisor, make sure to tell your local security office about any staff changes.

Did You Know?

**PIV cards**

- A PIV card, which is also known as a PIV badge, is an identification card that complies with Federal Information Processing Standard (FIPS) 201 and related guidance
- A PIV card contains a photograph and stored identity information so that the identity of the cardholder can be verified physically and electronically
- PIV cards are issued to those requiring routine access to VA facilities or information systems
- PIV cards may be used for encrypting email and digitally signing enabled forms and documents

You can learn more about PIV cards by contacting your local PIV office or security office. See Appendix D: Privacy and Information Security Resources for policy governing PIV cards.

**Knowledge Check: Best Practices**

Review the following question and consider the best answer.

What program includes security and privacy into everyone’s daily functions and provides ongoing security and privacy practices for VA’s environment?

A. Continuous Readiness in Information Security Program (CRISP)
B. VA Privacy Program Handbook 6300
C. Central Office Program
Answer A is correct. CRISP is the VA Information Security Program that incorporates security and privacy into everyone’s everyday functions and provides ongoing security and privacy practices for VA’s environment.

Who Can Provide Support?

Your supervisor, COR, Privacy Officer (PO), and Information Security Officer (ISO) can help you comply with regulations.

- **Supervisor**
- **Contracting Officer (CO)/Contracting Officer Representative (COR)**
- **Privacy Officer (PO)**
- **Information Security Officer (ISO)**

**Supervisor**

Supervisor responsibilities for protecting VA sensitive information and information systems include, but are not limited to:

- Ensuring staff understands IT security and information protection issues
- Ensuring staff complies with security regulations and policies
- Ensuring staff only has access within the scope of their duties
- Verifying staff completes all privacy and information security training requirements
- Ensuring staff signs the ROB each year
- Helping staff report suspected incidents

**Contracting Officer (CO)/Contracting Officer Representative (COR)**

CO/COR responsibilities include, but are not limited to:

- Ensuring contractors sign the Contractor ROB each year
- Maintaining the original or a copy of the signed Contractor ROB. (Some CORs may require paper copies in addition to the electronic acknowledgement at the end of this course)
- Ensuring contractors complete required privacy and information security awareness training before they begin the contract and each year of the contract
- Ensuring contractors know when and how to report security and privacy incidents
Privacy Officer (PO)

Privacy Officer (PO) responsibilities include, but are not limited to:

- Promoting privacy awareness
- Communicating privacy training requirements and deadlines
- Ensuring compliance with federal privacy laws and regulations and VA Directives, handbooks, and other guidance
- Responding to, investigating, and reporting privacy incidents
- Providing support when incidents occur
- Tracking privacy training completion
- Completing annual Privacy Impact Assessments

See the Privacy and Information Security Resources document located in Appendix D: Privacy and Information Security Resources for a link to identify your PO using the PO Locator.

Information Security Officer (ISO)

Information Security Officer (ISO) responsibilities include, but are not limited to:

- Managing local information security programs and providing training
- Monitoring access to VA information systems
- Helping create and maintain information system security plans and emergency plans
- Assessing system risks
- Taking part in security self-assessments and system audits
- Ensuring information security measures are working as intended
- Responding to, investigating, and reporting information security incidents

See Appendix D, Privacy and Information Security Resources for a link to identify your ISO using the ISO Locator.

Knowledge Check: Your Role in Protecting Privacy and VA Sensitive Information

You must protect all types of VA sensitive information when around others. For each scenario, decide if the conversation is appropriate and protects VA sensitive information, or if it is inappropriate and fails to protect VA sensitive information.

Scenario 1 of 3:
Dave asked Mary to meet him at the elevator with a copy of a patient's claim form he needs for a meeting. Mary gives him the form and asks him to call her later if he has questions. She is careful not to mention the patient by name.

Answer: It is appropriate for Mary to suggest they discuss any questions about a patient's claim form on the telephone rather than in the hallway.

**Scenario 2 of 3:**

Carmen has taken her laptop computer to the cafeteria to finish a budget report while she eats lunch. Several friends join her at the table, and she leaves her laptop open while they chat.

Answer: It's inappropriate for Carmen to display information on her computer screen. Always be aware of your surroundings and never allow VA sensitive information to be viewed by others who do not have a need to know.

**Scenario 3 of 3:**

Charles walks away from his desk leaving the computer unlocked with a spreadsheet open. He knows he will be right back.

Answer: It's inappropriate to leave your computer unattended and unlocked. By locking your computer while you are away, you can prevent others from using your computer to access VA sensitive information.

**Module Summary**

Let's sum up the key points of this module. It's important to:

- Protect the four types of VA sensitive information, which include: Personally Identifiable Information, Sensitive Personal Information, Protected Health Information, and Internal Business Information
- Comply with the Rules of Behavior to protect privacy and ensure information security—it's the law
- Make sure you protect VA sensitive information contained in records
- Contact your supervisor, COR, PO, and ISO to help you comply with all regulations
Module 3: How to Recognize and Report Incidents

Module Objectives

Following the ROB and preventing incidents is everyone’s responsibility. When incidents do happen, it is up to you to report them right away so that any damage can be minimized. When you have completed this module, you will be able to:

- Identify common privacy and information security incidents
- Recognize consequences and penalties that may result from incidents
- Recall how to report incidents

Remember: for more information, watch for these headings throughout the course: Did You Know?, Question and Answer, and Rules of Behavior.

Here’s another story about one person’s experience.

Know the difference, make a difference: James Makes a Difference

I was walking out of the canteen the other day when I found a lost PIV card lying on the floor. I picked it up. When I got back to my desk, I reported it to my ISO. A lost PIV card in the wrong hands can put VA facilities and information at risk. I’m glad I spotted that PIV card and knew what to do.

Reporting Incidents

**Incidents** are defined as actual or potential privacy and information security violations. Examples of incidents include:

- Mishandling of VA sensitive information in paper documents
- Missing or stolen equipment
- Mailing VA sensitive information to the wrong recipient
- Accessing unauthorized, electronic VA sensitive information
- Moving IT inventory equipment, such as computers or data cables, from their original location and not accounting for the change
Question and Answer

What should you keep in mind when reporting an incident?

Remember: Anytime you hear or see something that is of concern, report it!

- What? Who? All possible incidents must be reported to your supervisor and ISO or PO immediately.
- When? How? After normal business hours or on weekends, report incidents through the VA National Service Desk and follow your work unit's procedures to notify your supervisor and the VA Network Security Operations Center (NSOC).

Impact

Privacy and information security incidents can affect VA, Veterans, and you.

Some examples of impact include the following:

- VA may lose the public’s trust
- VA may have to report the incident to Congress, especially for breaches involving large numbers of Veterans
- Veterans may be harmed by making sensitive information public, including a financial loss or identity theft
- You could face job loss, fines, and possibly prison if you are the cause of an incident

Consequences If You Cause an Incident

Serious consequences of privacy and information security violations may include:

- Suspension of your access to systems
- Reprimand in your personnel file
- Suspension from your job, demotion, or job loss
- Prosecution at civil or criminal levels
- Fines
- Imprisonment
Severe Penalties

If you steal or intentionally change or destroy federal property or information, you could face:

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

Additionally, if you:

- Destroy or remove records without authorization, you can face $2,000 in fines and three years in prison
- Violate the Privacy Act, you can face up to $5,000 in fines and a year in prison
- Violate laws protecting PHI, more penalties may apply

Violation of federal privacy regulations can incur fines from $100 to $1.5 million with the potential of jail time. Refer to VA Handbook 5021, Employee/Management Relations, or contact your human resources or employee relations representative for more information. See Appendix D, Privacy and Information Security Resources for more information.

Exercise: Common Incidents

Incidents are more serious when many people are affected and the degree of damage is higher. Incidents can damage you, your work unit, Veterans, VA, and our information security. Which of the items below are information security incidents?

- Mishandling of VA sensitive information
- Missing/stolen equipment
- Discussing VA sensitive information in a private office
- Mismailing
- Unauthorized access to electronic information
- Discussing patient information in inappropriate locations
- Missing IT inventory
- Loss of a BlackBerry or other mobile device
- Inappropriate use of removable media
- Locked files and documents left in the office

Answer: The eight incidents to report are the mishandling of VA sensitive information, missing/stolen equipment, mismailings, unauthorized access to electronic information,
discussing patient information in inappropriate locations, missing IT inventory, the loss of a BlackBerry or other mobile device, and the inappropriate use of removable media. The two items that are not incidents are locked files and documents left in the office and discussing VA sensitive information in a private office.

**Steps to Report an incident**

If you notice an activity or situation that could put VA sensitive information or information systems at risk, here are the steps to report it:

Step 1. Write down the details: time of day, situation, who was involved, why you think it may be an incident

Step 2. Report it:

- Employees: Report suspected incidents to your supervisor and ISO or PO immediately. If you are not sure who your ISO or PO is, you can check the locator link provided in Appendix D, Privacy and Information Security Resources. 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 incidents must be reported within the time stated in your contract

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

Additional contact information to report incidents may be found in Appendix D, Privacy and Information Security Resources. The National Service Desk now answers the NSOC number (also found in Appendix D).

**More Contacts**

For times you cannot report an incident to your supervisor, ISO, PO, and/or AOD, here are some more resources:

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

Appendix D: Privacy and Information Security Resources includes more guidance on how to contact the VA National Service Help Desk.

Knowledge Check: Steps to Report an Incident

Review the following question and consider the best answer.

You notice a coworker has grabbed printouts that contain dozens of Veterans’ sensitive information. She places the printouts in her personal gym bag and tells you she is going out for a lunch break.

Should you report this as an incident?

A. No, I will see if she has the printouts when she returns
B. Yes, I suspect that this could be a potential risk to Veteran information
C. No, she will probably shred the VA sensitive information when done using it
D. No, maybe she has permission to take VA sensitive information with her

Answer B is correct. If you suspect or notice an activity or situation that could put VA sensitive information or information systems at potential risk, it must be reported.

Module Summary

Here are the key points to remember about reporting incidents:

• Report incidents or suspected incidents right away
• Report incidents to your supervisor (or COR) and ISO or PO
• Report the 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 4: Conversations and Messaging

Module Objectives

Privacy and information security must be maintained whenever you are talking to someone about VA sensitive information and when you communicate electronically.

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

- Choose correct actions in common situations
- Describe how to protect VA sensitive information in conversations
- Identify how to safely communicate VA sensitive information in electronic messages

Here’s another story about someone who made a difference.

Know the difference, make a difference: Shaina Makes a Difference

As I walked into the exam room, my patient was very upset and immediately began to tell me about a recent problem with alcohol abuse. We had been talking a few minutes before I noticed the exam room door was still open, with other patients and staff nearby. I quickly shut the door. My patient’s privacy is important to me!

Routine Conversations

At VA, you are responsible for protecting Veterans’ information in all situations. Routine conversations can occur face-to-face or on the telephone. Be careful with what you say to prevent disclosing VA sensitive information to anyone who doesn’t have a need-to-know.

Conversations on the phone or in person are so common we hardly think about them. When we’re talking about medical diagnosis or other VA sensitive information, though, we need to be more aware and extra careful. Discussing patient information where you can be overheard by others is an all-too-common security incident.
Did You Know?

Public areas

Discussing Veterans’ sensitive information in waiting areas, hallways, or elevators should never happen. Conversations can be overheard by anyone passing by.

Gossip

Gossip is particularly hard to control. This can damage VA’s reputation and relationships, especially in small communities where everybody knows everybody. It can also harm Veterans who expect their privacy to be respected. That’s why it is important to limit information access to employees whose jobs require the information; that is, they have a need-to-know.

Private Conversations

Sometimes we need to talk with coworkers about VA sensitive information. Remember to speak carefully, just as you would handle documents carefully.

When having conversations in person, be sure to:

- Lower your voice when others are around
- Close office doors or leave areas where others can overhear
- Discuss VA sensitive information in private, such as in a private office
- Avoid talking about VA sensitive information in public places, such as lobbies or elevators

Take these precautions when talking on the phone:

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

Exercise: Unencrypted email

Electronic messages may include email, instant messages, text messages, or even calendar information and may be sent from a variety of devices. Review the items below and determine and identify those that are reportable information security incidents:
Scenario 1 of 3

You receive an encrypted email with an attachment of patient test results.

Answer: This email is secure! Always encrypt emails containing sensitive information. Always check that the attachment or information contained in an email is appropriate for its intended recipients and follows minimum necessary guidance.

Scenario 2 of 3

You send a patient's test results to her personal phone using a text message.

Answer: This text message is at risk! Never text VA sensitive information to an external user. External text messaging is not protected by encryption.

Scenario 3 of 3

You send a calendar invitation containing a patient’s name and address information.

Answer: This calendar invitation is at risk! Never include sensitive information in calendar invites or in the subject lines of emails, as those are not protected by encryption.

Email Encryption

Email messages can expose private information. Emailed information is more secure if it is encrypted. You must encrypt all emails that contain VA sensitive information. VA uses two types of encryption to protect email. Select each link to learn more:

- Public Key Infrastructure (PKI) encryption
- Rights Management Service (RMS)

PKI works for external and internal messaging, while RMS only works internally. VA-issued workstations have the capability to encrypt email through Microsoft Outlook. Mobile devices, such as BlackBerry phones and must have an encryption certificate or an RMS client installed which allows the device to send and receive encrypted emails.

Applicable ROB
Employee: 2b(10), 2b(11).
Contractor: 2b(12)
The Titus toolbar is a new feature of the Outlook tools that permits you to indicate if the content of your email contains VA sensitive information. Using the Titus feature generates a message below your signature to inform readers of sensitive content.

Did You Know?

PKI

You may also hear PKI referred to as S/MIME encryption. 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 (PKI) does not encrypt information sent in the subject line of an email. Never put VA sensitive information in the subject line of an email.

RMS

RMS protects the content of email messages and other Microsoft Office documents. RMS provides additional controls that PKI does not. RMS can prevent forwarding, copying, and Microsoft-provided screen captures of RMS-protected content. You can request external user access to VA’s RMS system. Select the link located in Appendix D: Privacy and Information Security Resources to learn more.

Which to use?

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

Digital Signature

A digital signature helps you 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.
Question and Answer

Where can I learn more about encryption?

Here are some more resources to help you learn more about encryption:

**PKI S/MIME Encryption**—Refer to the TMS course 1256927, *Getting Started with Public Key Infrastructure*, to learn more about PKI encryption.

**RMS Encryption**—Refer to the TMS course 336914, *An Introduction to Rights Management Service—RMS*, to learn more about how to use RMS.

**Secure Email Practices**

Always follow these guidelines when sending emails that contain VA sensitive information:

**Encryption**

- Use RMS or PKI to make sure emails are encrypted
- Do not put VA sensitive information in the subject line
- Include your name and phone number on encrypted emails

**Other Guidelines**

- Confirm all individuals on the distribution list are approved to receive the information
- Consider the audience carefully before using Reply All for an email
- Delete unnecessary emails and attachments containing VA sensitive information as soon as possible. (However, be sure to save any emails and attachments that may be records)
- Ensure the Auto Forward feature to addresses outside of VA’s network is turned off
- Do not use your personal email address to communicate about VA business
Electronic Calendars

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

Never use public electronic calendars, such as Google or Yahoo calendars, for VA business. Public electronic calendars are not VA-approved.

Knowledge Check: Sending Emails with VA Sensitive Information

When you are writing emails, do not put VA sensitive information in the subject line. Review the following scenarios and determine whether the information in the subject line is appropriate or inappropriate for each.

Scenario 1 of 3

The subject line of an email states the following message: Don Peterson Record – Date Of Birth 7/21/1952

Answer: This is an inappropriate subject line. Ensure there is no sensitive information in the subject line of an email. Even when you encrypt email, the subject line is not encrypted.

Scenario 2 of 3

The subject line of an email states the following message: Patient Mike Phillips TB test results are positive

Answer: This is an inappropriate subject line. Never place PHI like this patient name and medical information in the subject line of an email. Even when you encrypt email, the subject line is not encrypted.

Scenario 3 of 3

An encrypted email reply contains an attachment of a patient payment invoice; the subject line states Patient Payment Invoice.
Answer: This subject line is **appropriate**. The subject line does not contain sensitive information. However, because there is an attachment containing sensitive information, the message must be encrypted. Use RMS or PKI to make sure emails are encrypted.

**Instant Messaging and Texting**

VA recently implemented a secure instant message (IM) system within VA’s network. VA allows you to access and use Microsoft Lync as a secure, encrypted way to exchange VA sensitive information. Microsoft Lync may not be available for many of the mobile devices that are coming online.

IMs saved in Microsoft Outlook are not encrypted, so make sure that Microsoft Outlook does not save these IMs in your Conversation History. Contact the VA National Service Desk for help, if needed. IMs are not part of a system of records.

Never use your mobile phone’s text messaging feature to send VA sensitive information or conduct any VA business. All VA sensitive information must be encrypted during transmissions.

Sending VA sensitive information in an unencrypted text message can put VA at risk.

**Module Summary**

Let’s sum up the key points of this module:

- Protect your conversations and electronic messages
- Never put VA sensitive information in the subject line of any email
- Never post VA sensitive information on Outlook Calendars
Module 5: Handling Paper and Electronic Documents Safely

Module 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 finished this module, you will be able to:

- Select the correct actions in common situations when handling paper and electronic documents
- Recognize how to protect VA sensitive information when handling paper documents, records, and files
- Identify how to safely store, transport, and dispose of any media containing VA sensitive information

Here is another story about someone making a difference.

Know the difference, make a difference: Edward makes a difference

Today we had a call from an angry Veteran who had requested a copy of his medical record. The record he was sent included two pages of handwritten notes about another Veteran and a copy of her request form with her social security number, address, diagnoses—lots of her personal information. Our team is starting a peer review process to double-check these highly personal mailings. We won't let this happen again!

Requirements for Paper Documents, Records, and Files

Incorrectly handling paper documents is still one of the most common types of privacy and information security incidents at VA. Some common examples of paper documents include the following:
- Printouts of documents created on the computer
- Handwritten notes
- Work papers

Some other specialty items must also be handled as if they are paper documents, such as faxed information, x-rays, labels, or microfiche. Be sure you know how to handle paper items securely and prevent unauthorized disclosure.

Did You Know?

**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

**Paper Records**

Some paper documents or files may be records identified in the Records Control Schedule (RCS). These records must be available for use or stored as noted in the RCS and must be retained or disposed of properly.

- Ask your supervisor, facility Records Manager, or work center Records Liaison for guidance before you dispose of or destroy any material that may be a record. You can also consult VA Directive and Handbook series 6300 for guidance
- Place a cover sheet indicating sensitive information on top of any records, before sending paper records to anyone. Refer to VA Directive 6609 for instructions on mailing SPI
- Clearly mark any folders in storage boxes if they contain VA sensitive information. If you need to move records to off-site storage, first contact your
Records Liaison. Be sure to clearly mark transfer forms (SF-135 or VA Form 0244) when moving records that contain VA sensitive information.

- Be sure records that are stored off-site are listed on the work center’s file inventory. As long as records are in the legal custody of VA, Records Officers must maintain access control and security for records with VA sensitive information in them. Coordinate with your facility Records Liaison and Privacy Officer.

### Handling Records and Faxing Paper Documents

Every facility has designated individuals who administer or maintain the records program. This role goes by many names across VA administrations. This course refers to Records Liaisons to describe anyone with local responsibilities for maintaining file plans, coordinating storage, and assisting Records Officers with the program.

Be especially careful when it is necessary to transmit paper records or documents via fax machine. VA staff should only use fax machines to send documents with VA sensitive information if there is no other way to meet the request or timeframe. Whenever PII or PHI is sent on a fax machine, VA health care staff need to ensure that the fax machine is not accessible to the general public (e.g., in a secured room that is only available to staff).

### Did You Know?

**Handling paper records**

To handle paper records securely, remember:

- You can be fined or penalized if you do not follow procedures for storing or destroying records. If the records have VA sensitive information, consequences can be even more severe.

- Destruction or disposing of records before the disposition date is illegal, as stated in the GRS or RCS; sometimes materials that are records have not yet been included in an RCS. These unscheduled records cannot be destroyed.

- Records may have special rules apply if they are subject to a legal records freeze or what is termed a litigation hold. Work with your supervisor and your facility Records Liaison to learn more.

- Paper records must not be thrown out in wastebaskets, recycling containers, or dumpsters. Records must be destroyed by shredding, burning, or macerating.
• Records Management Officers should be consulted first before destroying any materials that may be records

Faxing paper documents

The use of faxing has declined in recent years. When using fax technology, be sure to send faxes from a location that is not public, and be sure your recipient also has a secure location or someone is by the receiving machine to collect the information. Fill out a cover sheet including these four items:

• Recipient’s name
• Your name and contact information
• Instructions for the recipient to verify fax receipt
• The following confidentiality 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.

   Source: VA Handbook 6500, Appendix F: VA Password Management

Requirements for Using Mail and Delivery Services

At many VA facilities, a locally approved mail system is used to transfer paper files among staff at the facility.

With thousands of mailings sent individually and as batches of form letters every week, VA has a big challenge to get it right every time. It all starts with the commitment to protect sensitive information and make a difference.

Here is more information about requirements to protect VA sensitive information as it is transmitted through your local system and regular.
Did You Know?

**Internal office mail services**

- Place documents in closed interoffice envelopes
- Place a Notice Sheet in the closed interoffice envelope. (VHA staff must use PA/HIPAA envelopes in addition to the Notice Sheet)
- Place documents with VA sensitive information in sealed envelopes inside the interoffice envelope for added safety
- 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 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 only show 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, UPS, or FedEx. (*Copies* of documents containing VA sensitive information may be sent through the untracked U.S. Postal Service)

**Knowledge Check: Using Mobile Devices**

Review the following question and consider the best answer: true or false.

Special handling is required when VA sensitive information is sent through internal VA interoffice mail.
Answer: True. To protect VA sensitive information sent through internal mail, place a Notice Sheet in the closed interoffice envelope and place documents with VA sensitive information in sealed envelopes inside the interoffice envelope. VHA staff must use PA/HIPAA envelopes in addition to the Notice Sheet.

**Paper Logbook**

Logbooks can be helpful in conducting VA business; however, they must be used safely. Paper logbooks create a high risk for violating privacy because they can be lost or stolen. They are not allowed in most instances. Electronic logbooks are preferred.

Keep this guidance in mind:

- 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.

**Did You Know?**

If the use of a paper logbook is approved, here are more tips for using it securely.

**Data security**

Make sure the information kept in the approved logbook is the least amount of VA sensitive information required.

**Physical security**

Make sure the logbook:

- Is properly protected
Is locked up when not in use
• Meets guidelines according to VA records management when destroying any physical pages

Records management

If your logbook is considered a record, follow your Records Officer’s guidance for retention and disposition

Disposal

Keep sign-in rosters under your control at all times and in their assigned area of use. Shred them using a VA-approved shredder at the end of each business day.

Exercise: Best Practices

Determine if each of the three scenarios describes a situation in which sensitive information is “secure” or “at risk.”

Scenario 1 of 3:

I wonder if I can use the VA-provided USB device to store music I can listen to while I’m working. Would using VA’s USB device to play your music keep information safe or potentially put it at risk?

Answer: At risk! VA-provided media should not be used for personal purposes.

Scenario 2 of 3:

A technician has a small problem: “I need to get this patient payment spreadsheet to Becky right away...but the file is acting so funny. I’ll transfer the patient’s payment spreadsheet and fix this on my personal computer.” Does her decision keep information secure or put it at risk?

Answer: At risk! Personal property and VA property and information must be kept separate. Using VA information on a non-VA system requires a documented agreement, such as a contract.
Scenario 3 of 3:

"I want to bring in my personal tablet or laptop and connect to the network and perform my VA-assigned duties. I would like to take notes in a meeting; I have a program on my laptop that I don’t have on my VA-issued laptop." Does this keep information safe or put it at risk?

Answer: At risk! Do not connect your personal device to VA’s network. Get approval from the Information System Owner, local CIO, or designee before using a personally owned device on-site.

Electronic Media

Many employees may work with electronic media or electronic media storage. Employees with IT responsibilities may also have responsibility for electronic information systems. Privacy and information security rules must be applied when creating, storing, or disposing of electronic media and administering electronic information systems.

Be sure to also consult your Records Officer 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.

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 HTML files, flat files, Word documents, PDF documents
- Electronic media storage: Mag tapes, floppy disks, CDs/DVDs, and external hard drives
- Electronic information systems: VISTA/CPRS, Concur Government Edition (CGE)

Applicable ROB
Employee: 2b(8), 2b(15)
Contractor: 2b(11)
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) and how any electronic devices will be stored while off-site.

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.

Knowledge Check: Transporting VA Sensitive Information

Review the following question and consider the best answer.

You are traveling to another VA site and need to transport your VA-issued laptop. Where should you keep your laptop while traveling through the airport?

A. Pack in your luggage and check in your luggage
B. Keep it under your protection at all times while traveling
C. Place laptop in the overhead compartment of plane

Answer B: Always keep your VA-issued laptop under your protection at all times while traveling. Even before boarding your flight, place your computer on the conveyor belt for the security checkpoint only when you are the next in line, and always keep it under your control.

Microsoft SharePoint

VA has approved Microsoft SharePoint for you to use for online data storage and collaboration. 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 approved to access the information
• Get access to only the sites you need to do your job
• Share only the information your work unit needs to share to do its job
  o Here are some tips to protect records stored on SharePoint: List the SharePoint sites in the work unit’s file inventory
  o Schedule the disposition of these records per General Record Schedules and the VA Record Control Schedule
  o Consult with the facility Records Officer prior to destroying any record in SharePoint

Module Summary

Let’s sum up the key points of this module:

• Protect paper files and prevent unauthorized disclosure when sending faxes, interoffice mail, and regular mail
• Do not keep unauthorized paper logbooks
• Report any strange activity on your computer system to your ISO.
Module 6: Using VA Systems Securely

Module Objectives

Information systems that are used for VA business must be protected. VA depends on you to keep them secure against any kind of attacks that can damage equipment, systems, software, and networks.

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

- Securely access VA systems
- Recognize procedures for telecommuters using VA systems
- Identify threats to VA networks
- Identify how to protect VA electronic devices from attacks

Here’s another story about someone making a difference.

Know the difference, make a difference: Kevin Makes a Difference

My wife’s father is a Veteran and he was admitted to the VA medical center this week. She was really worried about him and asked me to find out what was going on. Even though I am a Systems Analyst with privileged access to medical records, I can’t look up VA sensitive information for personal reasons. I told my wife that we have to ask the doctor, just like everyone else!

Telework Guidance

Teleworking and telecommuting refer to a work flexibility arrangement under which an employee does not commute to a central place of work every day. Instead, the employee works from another approved worksite, such as a home office or a telework center.

Some software tools used when working remotely include:

- VA-approved remote access

Applicable ROB

Employee: 2d(4)
Did You Know?

VA’s telework policy

VA Telework Policy (VA Handbook 5011/26) is known as the Alternative Workplace Arrangement policy. The VA Handbook provides information on VA’s telework program and telework criteria as well as examples of the forms needed to get permission.

The form used in establishing a telework agreement is VA Form 0740. 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 complete VA Telework Training Module for Employees (VA TMS ID: 1367006) and attach your certificate of completion with the telework agreement forms. Start by asking your supervisor for directions to complete the request.

Remote Access

You must only use VA’s approved remote access methods to access VA resources while outside of a VA facility, such as while on travel or teleworking. Contact your ISO for information on how to get a remote access account. You must have written permission from your supervisor or COR and local CIO in order to access VA sensitive information remotely.

You must follow VA’s national and local security policies, procedures, and configuration standards before being allowed access to any VA network. In most cases, to regularly access VA systems remotely, a telework agreement is necessary.

Being granted remote access capabilities means you must:

- Have an approved and signed telework agreement in place to work from home (VA employees)
- Connect via VA-approved remote access tools
- Follow remote access procedures
- Let your supervisor and ISO know when you no longer need remote access
• Never conduct VA business through your personal emails, personal IMs, or personal phone text messages

Did You Know?

RESCUE

Remote Enterprise Security Compliance Update Environment (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 in a VA facility.

Citrix Access Gateway

Citrix Access Gateway (CAG) provides access 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.

Wireless Devices and Networks

Wireless devices and networks can put VA at risk. You should use a hardwired connection to VA's network when possible. If you must use a wireless connection, be sure to use VA-approved remote access and wireless devices. Never set up unapproved wireless networks in VA facilities.

Did You Know?

Wireless Internet access, or Wi-Fi

Hackers can access devices through wireless networks in order to copy unencrypted data, email, contacts, and files.

To protect your VA device:

• Turn off your device's Wi-Fi capability unless you are working from a secure, password-protected network
• Use VA's approved remote access tools to connect to websites on the Internet when you are in airports or other public places (e.g., the library or a coffee shop)
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. 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.

Knowledge Check: Select the Correct Action

Read the following scenario and consider whether it’s true or false.

The Wi-Fi hotspot says it has a secure, password-protected Internet connection. Go ahead and connect to the Wi-Fi hotspot, but make sure you are using VA's VPN to connect to any VA websites.

Answer: True. You are allowed to use a secure, password-protected public Internet connection. Just make sure to use VA’s VPN to access any VA websites. This keeps VA information and systems safe.

Social Engineering Attacks

Social engineering is when someone takes advantage of your trust by asking you to disclose confidential information or gain unauthorized access to VA systems. They may approach you in person, call you, or email you.

Examples of social engineering attacks include:

- Someone asking for your username and password (e.g., in person, over the phone, in a chat room, by email, or by IM)
- Emails that contain harmful content, such as:
  - Attachments with malicious code
  - Embedded links to malicious websites
  - Internet sites with pop-up windows that ask you to reenter your username and password
Threats to Systems, Software, and Networks

VA information systems need daily protection from threats, such as malware, phishing, and spoofing. These threats can allow others to access and expose VA sensitive information. The VA NSOC monitors all network traffic for unusual or unapproved activities.

- 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
- Never give your password to anyone
- Report all suspected threats and warnings on your computer system to your ISO
- Be suspicious of virus alerts on web pages, and never click on untrusted links

Did You Know?

Malware

Examples of malware include 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
- 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

Risks:

- Collects VA sensitive information by pretending to be an honest source. For example, you receive a free offer that requires you to select a link, enter your username and password, and answer "a few simple questions"
- Appears as a link to a real website and takes the user to a fake site (e.g., you receive an email that appears as if it came from a known sender, but it is from a spoofer)

Protection Methods:

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

Note: Phishing links often have one or two characters that are different from the real website (e.g., www.ebay.webs.com [phishing URL] vs. www.ebay.com [real URL]). VA uses filters on all network traffic to combat spoofing.

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 vulnerable 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 to violate privacy and confidentiality undermines Veterans’ good faith in VA. It’s one of the four most common incidents reported at VA last year, and it is something everyone can help to prevent. If you don’t need to know sensitive information to do your job, don’t ask.

Insiders know how a facility operates and may have access to information that they can 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 rules for handling VA sensitive information.
Help protect VA from insider threats by being aware of the ROB. When something a colleague is doing doesn’t seem quite right, report it as an incident.

Did You Know?

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 unintended 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

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 go around 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

Applicable ROB

Employee: 1f, 2f(1), 2f(3)
Contractor: 2b(5)
- Sudden increases in spam or unsolicited email
- Strange attachments in emails

**Exercise: Prevent Social Engineering Attacks**

Today while working you encounter a few potential attacks. Review which social engineering threat could possibly affect you and VA networks.

**Downloading software**

You need to download a program or software from the Internet onto your VA-issued computer. Is this secure?

Answer: No! Never download software from the Internet to your VA-issued computer. Only those authorized by OI&T should install software.

**Conversation between coworkers**

Can you share your password or other account information, even with trusted coworkers?

Answer: No! Never share your password or other account information, even with trusted coworkers.

**Email**

You receive an email that appears as if it came from an unknown sender with a link and an attachment. Should you open the link and attachment?

Answer: No! Attackers may use links or attachments to infect VA computers. If you don’t know the sender, don’t open the link or attachments.

**Using Social Media**

VA has approved some social media tools and technologies for use when doing VA business. These include blogs, Facebook, Twitter, Flickr, and Yammer. When you access and use these tools, be aware that they can be open to attacks, including phishing and social engineering.
Here are some recommended practices when using these social media:

- Be professional and use good judgment when posting pictures and text; you are accountable for the content you publish
- Never comment on VA legal matters, unless you are an official spokesperson and have approval to do so
- Never post any VA sensitive or protected information on any social media site
- Limit the details you reveal in text, which can expose VA sensitive information
- Refrain from posting VA business or VA sensitive information in personal emails or external social media outlets, such as websites, Facebook pages, blogs, and Tweets
- Be aware of the details you reveal in photos
- Refer questions to public affairs, the VA office responsible for managing the facilities’ social media accounts

**Module Summary**

Let’s sum up the key points of this module:

- Use VA-approved remote access tools when you access VA’s network remotely
- Use a hardwired connection to VA’s network whenever possible
- Be aware of possible threats
- Report any strange activity on your computer system to your ISO
Module 7: Managing Equipment and Electronic devices

Module Objectives

Electronic devices that are used for VA business must be protected.

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

- Select the correct actions to protect IT equipment and electronic devices in common situations
- Identify devices that can expose VA sensitive information
- Recognize how to handle personally owned equipment

Here’s another story about someone making a difference.

Know the difference, make a difference: Su-Ling Makes a Difference

I changed jobs six months ago and moved to a different building. I work with patient data and took my laptop with me. My previous site’s IT coordinator contacted me a few weeks later to confirm if I still had the equipment. I didn’t know I had to report the new location before I moved. Now that I know, I’ll do better next time.

Inventory Control for Electronic Devices

VA employees, contractors, and volunteers use VA electronic devices to support their work. VA-issued laptops must have full disk encryption installed and it must be operational. Some of these devices include desktop computers, laptops, BlackBerry devices, Apple internet operating system (iOS) devices, Android devices, USB drives, biomedical equipment, and copy machines.

Applicable ROB

Employee: 2b(16), 2f(4), 2f(5), 2h(4)
Contractor: 2b(14), 2b(16)
Here is what you need to remember to do to keep these devices secure:

- Take care of 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.
- Work with your supervisor to notify IT inventory coordinators that your location has changed when you relocate. 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.
- Do not disable VA-approved security tools.

Note: some laptops that run software for biomedical devices cannot be encrypted. VA needs these devices to treat patients and store patient information.

**Did You Know?**

**Monitoring threats on medical devices**

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

**Recommendations:**

The 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 [Appendix D: Privacy and Information Security Resources](#). 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 the NSOC.
Protecting VA Sensitive Information from Theft or Loss

You must protect information stored on electronic devices. When electronic devices are lost or stolen and don’t have any protection, VA sensitive information may be compromised. Be aware of your surroundings since VA sensitive information can also be viewed by unauthorized individuals while you are working.

Did You Know?

Here is some advice for how to keep many types of equipment and devices safe.

Desktops/laptops

- Use strong passwords
- Log off from your computer or lock your computer and remove your PIV card before leaving your work area
- Use privacy screens in public areas
- Position your screen to face away from where people can see it
- Do not disable VA-approved encryption
- Keep your laptop with you or use a locking cable

Mobile devices (e.g., BlackBerry, iOS, and Android devices)

- Use strong passwords
- Do not disable VA-approved encryption
- Store your device in a secure location

Removable storage devices

- Use password protection
- Do not disable VA-approved encryption
- Use only VA-issued devices and storage (e.g., USB drives/thumb drives, portable hard drives)
- Store your device in a safe place

Other devices with internal memory

- Can include: copiers, medical devices, etc.
• Store your device in a safe place, if possible
• Ask OI&T staff to remove the memory before equipment is replaced or removed from VA’s protected environment

VA-issued devices

• Lock office and conference room doors when leaving computers or other devices behind
• Save and back up data using VA-approved storage, such as network drives or VA-issued thumb drives
• Store VA sensitive information on approved, encrypted devices
• Never leave office doors unsecured, or lower level windows unlocked

Protecting Information on VA Devices

Here are four common types of equipment. Read each item to see if you know how to protect them. Be sure to keep track of your equipment and devices and report if any of them is lost or stolen.

Desktop computer

To protect information on your desktop computer (or laptop) use a strong password. Do not disable VA-approved encryption. Secure your computer by always logging off your computer or lock your computer and remove your PIV card before leaving your work area. If you’re working in a public area, use a privacy screen. Lock office and conference room doors when leaving computers or other devices behind.

Handheld devices (e.g., BlackBerry, iOS, and electronic tablets)

To protect information on your handheld devices, use a strong password. Do not disable VA-approved encryption. Secure your handheld devices by keeping track of your device at all times.

Removable storage devices (e.g., USB drives/thumb drives, portable hard drives)

To protect information on your storage devices, use only VA-issued devices and storage. Do not disable VA-approved encryption. Save and back up data using VA-approved storage, such as network drives or VA-issued thumb drives. Secure your removable storage devices in a safe place.
Equipment with Internal Memory (e.g., copiers, biomedical devices)

To protect information on equipment with internal memory, ask OI&T staff to remove the memory before equipment is replaced or removed from VA’s protected environment. Secure equipment with internal memory in a safe place. Never leave office doors unsecured, or windows unlocked.

Requirements for VA Mobile Devices

Take care of 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. VA supports thousands of mobile devices across the country, and these devices may store, process, or transmit VA sensitive information that needs protection. These devices are easy to transport, adding challenges to ensuring device security.

Work with your supervisor to notify IT inventory coordinators if you relocate. To protect your VA mobile devices, always follow VA instructions to keep your security software up-to-date. Use VA-approved encryption and passwords. Do not disable VA-approved security tools. For more information about encryption for your VA device, contact your ISO or the VA National Service Desk.

Did You Know?

Know the rules

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

Protect patient data and your information

Make sure that your mobile device does not contain the only copy of any VA sensitive information. That way, if your mobile device is lost, broken, or stolen, the information can be restored. 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 unattended. Smaller mobile devices that do not have the ability to use a cable lock should be kept 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 on your person.

Safeguard VA data

Make sure that you do not install any non-approved applications onto your mobile devices if they have not been vetted 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.

Question and Answer

What do you do if you get an email from an unknown sender on your mobile device?

Be aware; hackers may try to gain full remote access to your devices. Do not click on website links or open attachments sent by unknown senders. Instead, report all odd messages and suspected threats and warnings you receive on your mobile device to your ISO.

Knowledge Check: Lost BlackBerry and Other Mobile Devices

Review the following question and consider the best answer.

An employee lost his BlackBerry while on a temporary duty assignment. What should the employee do first to protect the information on his BlackBerry from potential loss and prevent the exposure of sensitive Veteran information?

A. Call the BlackBerry to make sure it is turned off
B. Use the GPS tracking feature to locate the BlackBerry
C. Contact his ISO, PO, and supervisor immediately
D. Contact the cell phone network provider to report the missing BlackBerry
Answer C is correct. Your first step is to contact your ISO, PO, and supervisor immediately to report the BlackBerry is missing. Always keep your BlackBerry with you. Never leave it in the hotel room or office site.

**Limited Personal Access and Use of VA-Issued Devices**

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

- 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**.

**Did You Know?**

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

**Personal Electronic Devices**

VA does not allow users to bring their personally owned equipment into a VA facility and connect to the network. Personally owned devices may only use VA-approved remote access technologies, such as CAG, to access VA resources. If you 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 within the facility.

Here is more guidance for using personal electronic devices:

- Where approved, personally owned devices may only connect to VA’s network using the approved method, Citrix Access Gateway (CAG)
- Never store VA sensitive information on any personal electronic device
- Never store VA sensitive information on a third-party file sharing site (e.g., Google Docs, Dropbox, or others)

**Knowledge Check: Protecting Electronic Devices**

Review the following question and consider the best answer. Which of the following passwords is the most secure?

A. Secure1  
B. Myuejd1!@
C. 98734  
D. Matt0519

Answer B is correct. To protect your VA-issued devices and your access to VA sensitive information, you must meet VA’s password requirements. Your password must have at least eight characters and have three of the following: uppercase letters, lowercase letters, numbers (0–9), and special characters (such as #, %, @).

**Module Summary**

Let’s sum up the key points of this module:

- Keep your equipment with you at all times, or store your items in a secure location
- Use VA-encrypted electronic devices that have been approved by your ISO and CIO
- Make sure your devices are encrypted and password protected
- Use VA-approved remote access solutions when working on personal devices
Module 8: Course Summary and Rules of Behavior

Course Summary

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

- Identify common situations when VA sensitive information is at risk
- Recognize and report incidents
- Take care with private conversations and messaging
- Handle paper and electronic documents safely
- Prevent attacks on information systems and networks
- Take precautions to prevent theft or loss of VA-issued electronic devices

Acknowledge, Accept, and Comply with the ROB

Because you access and use VA information systems or you may come in contact with VA sensitive information, you must accept responsibility for protecting privacy and ensuring information security. You must formally acknowledge, accept, and comply with the ROB for your role. The ROB are the minimum compliance standards for all VA locations. If your location has rules that are stricter, you must obey them. You must acknowledge and accept the ROB 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.

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

Instructions for Signing the Rules of Behavior

Before you complete the signature step, first identify whether you are an employee or a contractor, then print the appropriate ROB document (Appendix A: Rules of Behavior for VA Employees or Appendix B: Rules of Behavior for VA Contractors).
To acknowledge and accept the ROB:

- initial each printed page with your initials where indicated
- sign the last page of the document where indicated.

VA Employee

See Appendix A: Rules of Behavior for VA Employees to review and accept the Employee Rules of Behavior.

Before you complete the signature step: Are you selecting the correct ROB? These rules are for you if you are a VA employee who works for VA under Title 5 or Title 38, United States Code. This also includes volunteers, without compensation (WOC) employees, and students* or other trainees.

VA Contractor

See Appendix B: Rules of Behavior for VA Contractors to review and accept Contractor Rules of Behavior.

Before you complete the signature step: Are you selecting the correct ROB? These rules are for you if you are a non-VA user and your access to VA information resources is provided under a contract, agreement, or other legal arrangement.

Submitting Your Signed ROB

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

- If you are a VA employee and signed the Employee Rules of Behavior, provide the signed copy to your supervisor.
- If you are a VA contractor and signed the Contractor Rules of Behavior, provide the signed copy to your COR.

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.
I. APPENDIX A: Rules of Behavior for VA Employees

DEPARTMENT OF VETERANS AFFAIRS NATIONAL RULES OF BEHAVIOR

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

   a. I understand that an essential aspect of my job is to take personal responsibility for the secure use of VA systems and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g., digital, paper).

   b. I understand that when I use any government information system, I have NO expectation of privacy in any records that I create or in my activities while accessing or using such information system.

   c. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and ISOs. Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized OIG, VA, and law enforcement personnel.

   d. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting of information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

Initials ______
e. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal or civil penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

f. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my VA supervisor, ISO and PO, immediately upon suspicion.

g. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my VA supervisor, local CIO and ISO, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

h. I understand that the VA National ROB do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the U.S. Government.

i. I understand that the VA National ROB do not supersede any policies of VA facilities and other agency components that provide higher levels of protection to VA’s information or information systems. The VA National ROB provide the minimal rules with which individual users must comply.

j. I understand that if I refuse to sign this VA National ROB as required by VA policy, I will be denied access to VA information systems or VA sensitive information. Any refusal to sign the VA National ROB may have an adverse impact on my employment with the Department.
2. SPECIFIC RULES OF BEHAVIOR

a. Basic

(1) I will follow established VA information security and privacy policies and procedures.

(2) I will comply with any directions from my supervisors, VA system administrators, and ISOs concerning my access to, and use of, VA information and information systems or matters covered by these ROB.

(3) I understand that I may need to sign a non-VA entity’s ROB to obtain access to their system in order to conduct VA business. While using their system, I must comply with their ROB. However, I must also comply with VA’s National ROB whenever I am accessing VA information systems or VA sensitive information.

(4) I may be required to acknowledge or sign additional specific or unique ROB in order to access or use specific VA systems. I understand that those specific ROB may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

b. Data Protection

(1) I will safeguard electronic VA sensitive information at work and remotely. I understand that all VA owned mobile devices must be encrypted using FIPS 140-2, Security Requirements for Cryptographic Modules, validated encryption (or its successor) unless encryption is not technically possible, as determined and approved by my local ISO, CIO and the DAS for OIS. This includes laptops, thumb drives, and other removable storage devices and storage media (e.g., CDs, Digital Video Discs (DVD).

(2) I understand that per VA Directive 6609, Mailing of Sensitive Personal Information, the following types of information are excluded from the encryption requirement when mailed according to the requirements outlined in the directive:

Initials ______
(a) Information containing the SPI of a single individual to:

1. That person (e.g., the Veteran’s, beneficiary’s, dependent’s, or employee’s own information) or to that person’s legal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written consent of the individual. Such information may be mailed via U.S. Postal Service regular mail unless tracked delivery service is requested and paid for by the recipient;

2. A business partner such as a health plan or insurance company, after reviewing potential risk;

3. A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding; and

4. Congress, law enforcement agencies, and other governmental entities.

(b) Information containing SPI of one or more individuals to a person or entity that does not have the capability to decrypt information that is encrypted by VA, when sent according to VA Directive 6609.

(3) I understand that I must have approval from my supervisor to use, process, store, or transmit electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), regional offices).

(4) If approved to use, process, store, or transmit electronic VA sensitive information remotely, I must ensure any device I utilize is encrypted using FIPS 140-2 (or its successor) validated encryption. Information systems must use VA’s approved configuration and security control requirements. The local CIO and ISO must review and approve (in writing) the mechanisms used to transport and store the VA sensitive data before it can be removed from the VA facility.

(5) I will ensure that all printouts of VA sensitive information that I work with, as part of my official duties, are physically secured when not in use (e.g., locked cabinet, locked door).
(6) I acknowledge that particular care should be taken to protect SPI aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function.

(7) I recognize that access to certain databases, regional-, or national-level data such as data warehouses or registries containing patient or benefit information, and data from other Federal agencies such as the Centers for Medicare and Medicaid or the Social Security Administration, has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk.

(8) If I have been approved by my supervisor to take printouts of VA sensitive information home or to another remote location outside of a VA facility, or if I have been provided the ability to print VA sensitive information from a remote location to a location outside of a VA facility, I must ensure that the printouts are destroyed to meet VA disposal requirements when they are no longer needed and in accordance with all relevant records retention requirements. Two secure options that can be used are to utilize a shredder that meets VA and NIST’s requirements or return the printouts to a VA facility for appropriate destruction.

(9) When in an uncontrolled environment (e.g., public access work area, airport, or hotel), I will protect against disclosure of VA sensitive information which could occur by eavesdropping, overhearing, or overlooking (shoulder surfing) from unauthorized persons. I will also follow a clear desk policy that requires me to remove VA sensitive information from view when not in use (e.g., on desks, printers, fax machines, etc.). I will also secure mobile and portable computing devices (e.g., laptops, USB thumb drives, PDA).

(10) I will use VA approved encryption to encrypt any e-mail, including attachments to the e-mail that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. I will not encrypt e-mail that does not include VA sensitive information or any e-mail excluded from the encryption requirement under para. b(2).
(11) I will not auto-forward e-mail messages to addresses outside the VA network.

(12) I will take reasonable steps to ensure fax transmissions are sent to the appropriate destination, including double checking the fax number, confirming delivery of the fax, using a fax cover sheet with the required notification message included and only transmitting individually identifiable-information via fax when no other reasonable means exist and when someone is at the machine to receive the transmission or the receiving machine is in a secured location.

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by VA to protect sensitive data. 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. For questions regarding need-to-know and safeguards, I will obtain guidance from my VA supervisor, local CIO, and/or ISO before providing any access.

(14) When using wireless connections for VA business I will only use VA authorized wireless connections and will not transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption.

(15) I will properly dispose of VA sensitive information, either in hardcopy, softcopy, or electronic format, in accordance with VA policy and procedures.

(16) I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee.
c. Logical Access Controls

(1) I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor, local CIO, and/or ISO when the access is no longer needed.

(2) I will only utilize passwords that meet the VA minimum requirements defined in control IA-5: Authenticator Management in VA Handbook 6500, Appendix F, including using compliant passwords for authorized web-based collaboration tools that may not enforce such requirements.

(3) I will protect my verify codes and passwords from unauthorized use and disclosure. I will not divulge a personal username, password, access code, verify code, or other access requirement to anyone.

(4) I will not store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption and I am the only person who can decrypt the file. I will not hardcode credentials into scripts or programs.

(5) I will use elevated privileges (e.g., Administrator accounts), if provided for the performance of my official duties, only when such privileges are needed to carry out specifically assigned tasks which require elevated access. When performing general user responsibilities, I will use my individual user account.

d. Remote Access/Teleworking

(1) I understand that remote access is allowed from other Federal Government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency’s policies.

(2) I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I will use VA-provided IT equipment for remote access when possible.

Initials ______
(3) I agree that I will not have both a VA network connection and any non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my VA supervisor, local CIO, and ISO.

(4) I am responsible for the security of VA property and information, regardless of my work location. VA security policies are the same and will be enforced at the same rigorous level when I telework as when I am in the office. I will keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information.

(5) I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations (e.g., at home and during travel) and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location, pursuant to an approved telework agreement with VA sensitive information, authorized OIT personnel may periodically inspect the remote location for compliance with required security requirements.

(6) I will protect information about remote access mechanisms from unauthorized use and disclosure.

(7) I will notify my VA supervisor, local CIO and ISO prior to any international travel with a mobile device (laptop, PDA) so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.

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

Initials ______
e. Non-VA Owned Systems

(1) I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in writing in advance by my VA supervisor, local CIO, and ISO. I agree that I will not access, transmit, or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

(2) I will only use VA approved solutions for connecting non-VA owned systems to VA’s network.

(3) I will obtain my local CIO’s approval prior to connecting any non-VA equipment to VA’s network at a VA facility. This includes directly connecting to a network port or utilizing remote access capabilities within the VA facility.

f. System Security Controls

(1) I will not attempt to override, circumvent, or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff. I will not attempt to alter the security configuration of government equipment unless authorized.

(2) I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA on VA equipment.

(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 to create, store or use VA information.

(4) I agree to have issued GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.

(5) I will permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.
g. **System Access**

1. 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.

2. I will only use VA approved collaboration technologies for conducting VA business.

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.

4. I will not host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized in writing by my local CIO and approved by my ISO. I will ensure that all such activity is in compliance with Federal and VA policies.

5. I will not attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data.

6. I will only use my access to VA computer systems and/or records for officially authorized and assigned duties. The use must not violate any VA policy regarding jurisdiction, restrictions, limitations or areas of responsibility.

7. I will use my access under VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology, understanding that this Directive does not pertain to accessing VA applications or records. I will not engage in any activity that is prohibited by the Directive.

8. I will prevent unauthorized access by another user by ensuring that I log off or lock any VA computer or console before walking away or initiate a comparable application feature that will keep others from accessing the information and resources available in my computing session.

Initials _____
h. Miscellaneous

(1) I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional role-based security training required, based on my roles and responsibilities.

(2) I will take precautions as directed by communications from my ISO and local OIT staff to protect my computer from emerging threats.

(3) I understand that while logged into authorized Web-based collaboration tools I am a representative of VA and I will abide by the ROB and all other policies and procedures related to these tools.

(4) I will protect government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

3. ACKNOWLEDGEMENT AND ACCEPTANCE

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

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

_________________________  ______________________  ________________
Print or type your full name   Signature           Date

_________________________  ______________________
Office Phone               Position Title
II. APPENDIX B: Rules of Behavior for VA Contractors

CONTRACTOR RULES OF BEHAVIOR

This User Agreement contains rights and authorizations regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the Department of Veterans Affairs (VA). This User Agreement covers my access to all VA data whether electronic or hard copy (“Data”), VA information systems and resources (“Systems”), and VA sites (“Sites”). This User Agreement incorporates Rules of Behavior for using VA, and other information systems and resources under the contract.

1. GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS and ACTIVITIES UNDER THE CONTRACT:

   a. I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.

   b. I consent to reviews and actions by the Office of Information & Technology (OI&T) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.

   c. I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OI&T, VA, and law enforcement personnel.

   Initials ______
d. I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal government systems; deny access to Federal government systems; accrue resources for unauthorized use on Federal government systems; or otherwise misuse Federal government systems or resources are prohibited.

e. I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

f. I agree that OI&T staff, in the course of obtaining access to information or systems on my behalf for performance under the contract, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers (ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.

g. I understand I must comply with VA’s security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer’s Technical Representative (COTR). If the contractor believes the policies and guidance provided by the COTR is a material unilateral change to the contract, the contractor must elevate such concerns to the Contracting Officer for resolution.

h. I will report suspected or identified information security/privacy incidents to the COTR and to the local ISO or Privacy Officer as appropriate.

2. GENERAL RULES OF BEHAVIOR

a. Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job.
b. The following rules apply to all VA contractors. I agree to:

(1) Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the contract.

(2) Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.

(3) I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the contract. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.

(4) Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the contract.

(5) Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the contract or at the direction of the COTR or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not confer me unrestricted access or use, nor the authority to bypass security or other controls except as expressly permitted by the VA CIO or CIO’s designee.

(6) Contractors’ use of systems, information, or sites is strictly limited to fulfill the terms of the contract. I understand no personal use is authorized. I will only use other Federal government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal law still apply.

(7) Grant access to systems and information only to those who have an official need to know.

(8) Protect passwords from access by other individuals.

Initials ______
(9) Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.

(10) Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA.

(11) Follow VA Handbook 6500.1, Electronic Media Sanitization to protect VA information. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR’s orders.

(12) Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.

(13) Not host, set up, administer, or run an Internet server related to my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA unless explicitly authorized under the contract or in writing by the COTR.

(14) Protect government property from theft, destruction, or misuse. I will follow VA directives and handbooks on handling Federal government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the COTR.

(15) Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR’s orders regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with VA.

Initials ______
(16) Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated with my performance of services under the contract terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the COTR.

(17) Understand that restoration of service of any VA system is a concern of all users of the system.

(18) Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

3. ADDITIONAL CONDITIONS FOR USE OF NON-VA INFORMATION TECHNOLOGY RESOURCES

a. When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.

b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.

c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.

d. I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given contract or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same.

4. STATEMENT ON LITIGATION

This User Agreement does not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

Initials ______
5. ACKNOWLEDGEMENT AND ACCEPTANCE

I acknowledge receipt of this User Agreement. I understand and accept all terms and conditions of this User Agreement, and I will comply with the terms and conditions of this agreement and any additional VA warning banners, directives, handbooks, notices, or directions regarding access to or use of information systems or information. The terms and conditions of this document do not supersede the terms and conditions of the signatory’s employer and VA.

[Print or type your full name]  
Signature

Last 4 digits of SSN  
Date

Office Phone  
Position Title

Contractor’s Company Name  

Please complete and return the original signed document to the COTR within the timeframe stated in the terms of the contract.
III. APPENDIX C: Glossary

A

**Availability** — Able to be used or possible to get. Availability is timely and reliable access to and use of information. Source: VA Handbook 6500

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

C

**Confidentiality** — State or condition of being kept private. Confidentiality is to preserve authorized restrictions on information access and disclosure. Source: VA Handbook 6500

**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

**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

D

**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
**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

**Encryption**—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

**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

**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

**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

**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 public property
and must be managed according to laws and regulations. Source: http://www2.ed.gov/policy/gen/leg/fra.html

File plan—Local documentation identifying how records are categorized and grouped, how they may be retrieved, and where they are located.

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/

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/

G

General Records Schedule—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)

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 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/publications_detail3.asp?ID=2621
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 Administration Simplification 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/

Incident—An event that puts VA information or systems at risk. An incident is a situation involving a violation of either privacy or information security requirements as defined in related VA policies: (1) Any event that has resulted in: unauthorized access to, or disclosure of, VA sensitive information; unauthorized modification or destruction of system data; reduced, interrupted, or terminated data processing capability; introduction of malicious programs or virus activity; the degradation or loss of the system’s confidentiality, integrity, or availability; or the loss, theft, damage, or destruction of any equipment containing VA data. Source: VA Handbook 6500.2. (2) An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The term incident means security incident as defined in 38 U.S.C. § 5727(18). Source: VA Handbook 6500

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

Instant message—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

Integrity—To make sure VA information is correct. Integrity is the guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Source: VA Handbook 6500
Internal Business Information (IBI)—Knowledge or facts owned by an organization, including assets such as future product designs, customer/price lists, and internal policies not intended for public consumption. Sometimes also referred to as Proprietary Information. Source: Carnegie Mellon Software Engineering Institute

J—N/A

K—N/A

L—N/A

M

Macerating—To soften. Macerating is the act of becoming soft or separated into constituent elements by or as if by steeping in fluid; to soften and wear away especially as a result of being wetted or steeped. Source: Merriam-Webster Online Dictionary

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

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

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

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
**N**

**Notice Sheet**—A sheet of paper for internal mail that contains VA sensitive information. A notice sheet 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

**O—N/A**

**P**

**Paper logbook**—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 comprised of data, which 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

**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

**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/
**Personally Identifiable Information (PII)**—Any information that can be used to distinguish or trace an individual's identity, such as their 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 “Sensitive Personal Information” is synonymous and interchangeable with “Personally Identifiable Information.”

**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

**Privacy**—Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information. Source: American Institute of Certified Public Accountants (AICPA)

**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

**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

**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.

**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

**Q**—N/A

**R**

**Records**—Records are defined by 44 USC as 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 (see 44 U.S.C. Ch. 33, Sec. 3301).

**Records Control Schedule (RCS)**—A chart describing how VA records must be kept and for how long they must be kept. A Records Control Schedule (also known as a Records Disposition Schedule) is a document providing mandatory instructions for what to do with records that are no longer needed for current VA use. Records Control Schedules are required by statute. All VA records and information must be identified by records series and be listed in a Records Control Schedule. Source: VA Handbook 6300.1

**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

**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

**Rules of Behavior (ROB)**—A document that explains your duties as a VA system user. The ROB describes a VA information system user's responsibilities and expected behavior with regard to information system usage. All individuals who use or gain access to VA information systems must read, understand, and acknowledge and accept the VA National ROB before they are granted access to VA information systems. Source: VA Handbook 6500

**S**

**Sensitive Personal Information (SPI)**—The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (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. SPI is a subset of VA sensitive information/data. SOURCE:
38 U.S.C. § 5727. NOTE: The term “Sensitive Personal Information” is synonymous and interchangeable with “Personally Identifiable Information.”

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

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

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

T

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

Titus toolbar—TITUS Classification for Microsoft Office is a security and governance solution that enables organizations to ensure consistent and proper handling of their Microsoft Office documents. With a wide range of customizable functionality, this solution can force users to easily identify the sensitivity of every document, warn users of policy violations, and scan message content for PII and other sensitive information. The user’s classification selection is stored with the Office document as persistent metadata, which organizations can use to increase the accuracy and effectiveness of DLP, archiving, and perimeter security solutions. Source: http://www.titus.com/software/document-classification/index.php

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

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

**U**

**User**—Individual or (system) process acting on behalf of an individual, authorized to access an information system. At VA, users are Department personnel, employees, contractors working under an approved contract, business associates working under approved business associate agreements, and any other individuals providing services or performing functions for, to, or on behalf of VA who have been authorized by VA to access VA information or information systems. To access VA sensitive information or VA information systems, these individuals must complete VA-approved security and privacy training, sign the VA National ROB or Contractor ROB, and complete appropriate background screening before such access may be granted. Source: NIST SP 800-53; SP 800-18; CNSSI-4009

**V**

**VA sensitive information/data**—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 applicable confidentiality provisions. SOURCE: 38 USC § 5727. NOTE: The term “Personally Identifiable Information” is synonymous and interchangeable with “Sensitive Personal Information.”

**W—N/A**

**X—N/A**

**Y**

**Yammer**—A web-based site that allows people within a group to discuss ideas. Yammer is a microblogging social network, discussion board, and knowledge base service intended for businesses. Yammer networks are created for organizational use with everyone using the same company email address. Private groups within the company can also be organized. Access is available via a desktop application, the Web,
email, instant and text messaging, as well as iPhone and BlackBerry smartphones. Source: PCMag.com Encyclopedia

Z—N/A
IV. APPENDIX D: Privacy and Information Security Resources

Table 1. VA Phone Numbers

**Office of Inspector General (IG) Hotline** (to report fraud, waste, or mismanagement of resources)
(800) 488-8244

**VA National Service Desk** (to request computer, network, or access support; or to report security incidents to the Network Security Operations Center [NSOC])
(800) 877-4328

Table 2. VA Web Links

**CRISP Information** *
http://vaww.sde.portal.va.gov/oitauditprep/SitePages/Home.aspx

**Information Security Portal** *
https://vaww.infoprotection.va.gov/

**ITWD’s Role-based Training** *
### Table 2. VA Web Links

<table>
<thead>
<tr>
<th>Locator to Identify ISOs and POs*</th>
<th><a href="https://vaww.infoprotection.va.gov/index.aspx">https://vaww.infoprotection.va.gov/index.aspx</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>PIV Cards</td>
<td><a href="http://www.va.gov/PIVPROJECT/index.asp">http://www.va.gov/PIVPROJECT/index.asp</a></td>
</tr>
</tbody>
</table>

*These links are only accessible on VA’s Intranet

### Table 3. VA TMS Courses

<table>
<thead>
<tr>
<th>Available at: <a href="https://www.tms.va.gov/">https://www.tms.va.gov/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>TMS ID 10203, Privacy and HIPAA Training</td>
</tr>
<tr>
<td>TMS ID 336914, An Introduction to Rights Management Service – RMS</td>
</tr>
<tr>
<td>TMS ID 1256927, Getting Started with Public Key Infrastructure</td>
</tr>
<tr>
<td>TMS ID 2626967, Social Networking and Security Awareness</td>
</tr>
</tbody>
</table>

### Table 4. Privacy Laws and Regulations

<table>
<thead>
<tr>
<th>Available at: <a href="http://www.privacy.va.gov/privacy_resources.asp">http://www.privacy.va.gov/privacy_resources.asp</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Freedom of Information Act (FOIA)</strong></td>
</tr>
<tr>
<td>Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions.</td>
</tr>
<tr>
<td>Table 4. Privacy Laws and Regulations</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
</tbody>
</table>

**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 use of personal medical information for marketing purposes and increases fines for unauthorized disclosures of health information.

**Health Insurance Portability and Accountability Act (HIPAA)**
Establishes requirements for protecting privacy of personal health information.

**Paperwork Reduction Act**
Establishes the governance framework and the general principles, concepts, and policies that guide the federal government in managing information and its related resources, including records.

**Privacy Act**
Requires federal agencies to establish appropriate safeguards to ensure the security and confidentiality of the records they maintain about individuals, establishes restrictions on the disclosure and use of those records by federal agencies, and permits individuals to access and request amendments to records about themselves.

<table>
<thead>
<tr>
<th>Table 5. Information Security Laws, Regulations, and Related Statutes/Specifications</th>
</tr>
</thead>
</table>

**Federal Information Security Management Act (FISMA)**
Requires federal agencies to have a program to assess risk and protect information and information security assets that support agency operations.
### Table 5. Information Security Laws, Regulations, and Related Statutes/Specifications

<table>
<thead>
<tr>
<th><strong>Federal Records Act</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>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.</strong></td>
</tr>
<tr>
<td><strong><a href="http://www2.ed.gov/policy/gen/leg/fra.html">http://www2.ed.gov/policy/gen/leg/fra.html</a></strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Internal Revenue Code (IRC) Specifications</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IRC at 26 U.S.C.A. § 6103 (p)(4).</strong></td>
</tr>
<tr>
<td><strong><a href="http://www.patentofficelawsuit.info/irs_6103.htm">http://www.patentofficelawsuit.info/irs_6103.htm</a></strong></td>
</tr>
<tr>
<td><strong>Requires specific security protection for income tax return information [as 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.</strong></td>
</tr>
<tr>
<td><strong>IRC at 26 U.S.C.A. §§ 7213, 7431.</strong></td>
</tr>
<tr>
<td><strong><a href="http://www.patentofficelawsuit.info/irs_7431.htm">http://www.patentofficelawsuit.info/irs_7431.htm</a></strong></td>
</tr>
<tr>
<td><strong>Describes penalties for disclosing tax return information without permission from the individual.</strong></td>
</tr>
</tbody>
</table>
### Table 5. Information Security Laws, Regulations, and Related Statutes/Specifications


**Title 38 U.S.C. § 5701: VA Claims Confidentiality Statute**


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

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


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

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


Health records with respect to an individual’s drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or Sickle Cell Anemia are extremely sensitive.

### Table 6. Selected VA Privacy Handbooks and Directives

Available at: [http://www1.va.gov/vapubs/index.cfm](http://www1.va.gov/vapubs/index.cfm)

VA Directive 6066, Protected Health Information (PHI)

VA Directive 6371, Destruction of Temporary Paper Records

VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act

VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act System of Records
### Table 6. Selected VA Privacy Handbooks and Directives

<table>
<thead>
<tr>
<th>Handbook/Program</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Handbook 6300.6/1</td>
<td>Procedures for Releasing Lists of Veterans’ and Dependents’ Names and Addresses</td>
</tr>
<tr>
<td>VA Handbook 6500.1</td>
<td>Electronic Media Sanitization</td>
</tr>
<tr>
<td>VA Handbook 6500.2</td>
<td>Management of Security and Privacy Incidents</td>
</tr>
<tr>
<td>VA Handbook 6502</td>
<td>VA Enterprise Privacy Program</td>
</tr>
<tr>
<td>VA Handbook 6502.4</td>
<td>Privacy Act Review</td>
</tr>
<tr>
<td>VA Handbook 6512</td>
<td>Secure Wireless Technology</td>
</tr>
<tr>
<td>VA Handbook 6609</td>
<td>Mailing of Personally Identifiable and VA Sensitive Information</td>
</tr>
<tr>
<td>VHA Directive 1605</td>
<td>VHA Privacy Program</td>
</tr>
<tr>
<td>VHA Handbook 1605.1</td>
<td>Privacy and Release of Information</td>
</tr>
<tr>
<td>VHA Handbook 1605.2</td>
<td>Minimum Necessary Standard for Protected Health Information</td>
</tr>
</tbody>
</table>

### Table 7. Additional Selected VA Handbooks and Directives

<table>
<thead>
<tr>
<th>Directive/Program</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Directive 0701</td>
<td>Office of Inspector General Hotline Complaint Referrals</td>
</tr>
<tr>
<td>VA Directive 6515</td>
<td>Use of Web-based Collaboration Technologies</td>
</tr>
<tr>
<td>VA Handbook 5011/5</td>
<td>Hours of Duty and Leave</td>
</tr>
</tbody>
</table>
### Table 7. Additional Selected VA Handbooks and Directives

<table>
<thead>
<tr>
<th>Handbook/Memo</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Handbook 5021.3</td>
<td>Employee/Management Relations</td>
</tr>
<tr>
<td>VA Handbook 5021.6</td>
<td>Employee/Management Relations, Appendix A</td>
</tr>
<tr>
<td>VA Handbook 6300.1</td>
<td>Records Management Procedures</td>
</tr>
<tr>
<td>VA Handbook 6500</td>
<td>Appendix F, VA Password Management</td>
</tr>
<tr>
<td>VA Handbook 6500.6</td>
<td>Contract Security and Appendix D, Contractor Rules of Behavior</td>
</tr>
</tbody>
</table>