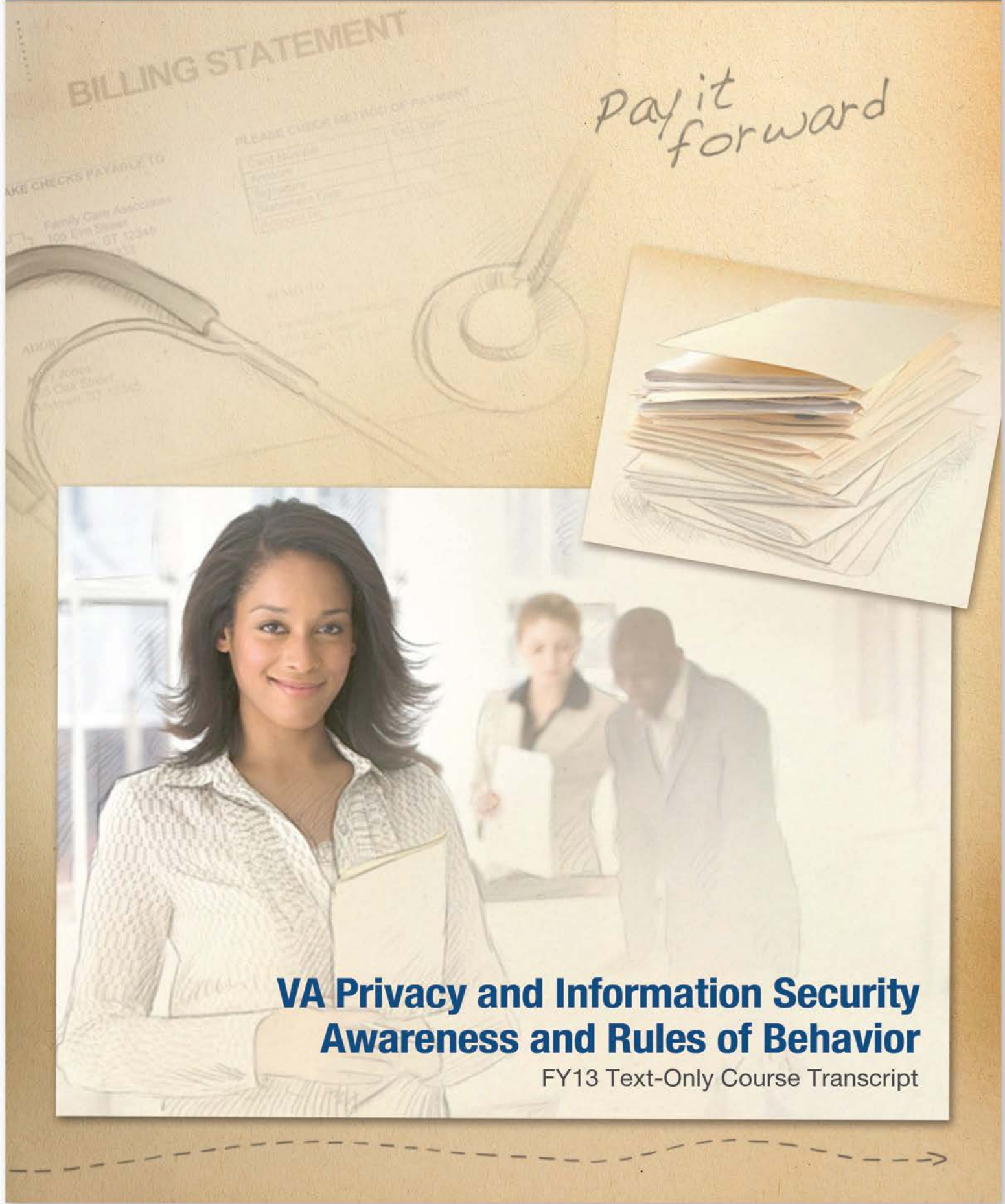


# U.S. Department of Veterans Affairs

Office of Information and Technology, IT Workforce Development



## **VA Privacy and Information Security Awareness and Rules of Behavior**

FY13 Text-Only Course Transcript

## Table of Contents

<b>Table of Contents</b> .....	<b>2</b>
<b>Purpose of this Document</b> .....	<b>5</b>
Using this Document.....	5
<b>Welcome</b> .....	<b>6</b>
Why am I Taking this Training?.....	6
Rules of Behavior (ROB).....	7
Course Objectives.....	9
Pay it Forward .....	9
Prologue: Helping Veterans (Fictional Scenario) .....	10
<b>Overview of Privacy and Information Security</b> .....	<b>11</b>
Introduction (Fictional Scenario) .....	11
Objectives .....	11
Protecting Privacy and Information Security .....	12
Privacy: What to Protect .....	13
Determining What is Sensitive and What is Not.....	14
Information Security: How to Protect It.....	14
What Can You Do to Protect VA Sensitive Information?.....	15
The Continuous Readiness in Information Security Program (CRISP) .....	17
Summary.....	19
<b>Protecting Private Conversations and Paper Records and Files</b> .....	<b>20</b>
Introduction (Fictional Scenario) .....	20
Objectives .....	20
Protecting VA Sensitive Information in Person and by Phone.....	21
What Are Records?.....	21
Protecting Paper Documents, Records, and Files .....	22
Protecting Records .....	25
Misdirected Mail .....	26
Written Log Books Containing VA Sensitive Information .....	26
Searching for an Alternative.....	28

Summary.....	28
<b>Privacy in Electronic Communication Formats.....</b>	<b>30</b>
Introduction (Fictional Scenario) .....	30
Objectives .....	30
Email.....	31
Microsoft Communicator .....	32
Outlook Calendar .....	32
Microsoft SharePoint.....	33
Communicating with Colleagues.....	33
Threats and Methods to Protect Mobile Devices.....	35
Lost Mobile Device.....	36
<b>Privacy when Storing, Transporting, and Disposing of Information .....</b>	<b>38</b>
Introduction (Fictional Scenario) .....	38
Objectives .....	38
Protecting VA Sensitive Information from Theft, Loss, and Unauthorized Access .....	39
Guidelines for Protecting VA Sensitive Information on VA-issued Devices.....	40
Leaving for Lunch .....	41
Transporting VA Sensitive Information.....	41
Guidelines for Transporting VA Sensitive Information.....	42
A Case of Theft.....	43
Storage and Disposal of Records .....	43
Guidelines for Disposing of Paper and Electronic Media .....	45
Retiring Old Files and Media.....	46
Summary.....	47
<b>Protecting VA-Issued Electronic Devices .....</b>	<b>48</b>
Introduction (Fictional Scenario) .....	48
Objectives .....	48
VA-Issued Devices.....	49
Personal Identity Verification (PIV) Cards.....	49
Limited Personal Use of VA-Issued Devices.....	50
Personal Use .....	51

Password Requirements .....	51
Remote Access .....	53
Wireless Devices and Networks .....	53
Telework Arrangement Approved .....	54
Social Engineering Attacks .....	54
Threats to Systems, Software, and Networks .....	55
Preventing Attacks .....	58
Use of Personal Devices .....	58
Summary .....	60
<b>Reporting Incidents.....</b>	<b>61</b>
Introduction .....	61
Objectives .....	61
Defining Incidents .....	62
Impact .....	62
Consequences .....	63
Civil and Criminal Penalties .....	63
The Steps to Report an Incident .....	64
Additional/Alternate Contacts .....	65
Filing a Report .....	66
Summary .....	67
<b>Course Summary and ROB .....</b>	<b>68</b>
Course Summary .....	68
Sign and Comply with the ROB .....	68
Course Completion .....	69
<b>APPENDIX A: Rules of Behavior for VA Employees .....</b>	<b>70</b>
<b>APPENDIX B: Rules of Behavior for VA Contractors.....</b>	<b>81</b>
Contractor Rules of Behavior .....	81
<b>APPENDIX C: Glossary.....</b>	<b>87</b>
<b>APPENDIX D: Privacy and Information Security Resources .....</b>	<b>101</b>



### Purpose of this Document

This text-only course transcript was designed to accommodate users in the following manner:

- 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) 2013 (i.e., October 1, 2012 through September 30, 2013).

You should take the online version of this course if possible. If you complete the course using this text-only transcript, you must sign the appropriate Rules of Behavior (ROB), as well as initial each page, in the space provided. 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.

For more information on the use of this document to fulfill the annual training requirement, Information Security Officers (ISOs), supervisors, and CORs should reference the “Instructions for Alternative Training Methods: VA Privacy and Information Security Awareness and Rules of Behavior” document on the VA intranet at:  
<http://vaww.infoshare.va.gov/sites/ittrainingacademy/prv-sec-training/Shared%20Documents/Instructions%20for%20Alternative%20Training%20Methods%20VA%20Privacy%20and%20Information%20Security%20Awareness%20and%20Rules%20of%20Behavior.pdf>

## Welcome

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

### Why am I Taking this Training?

Several laws and regulations require training. When you complete this training and sign the Rules of Behavior, you help VA comply with these laws. The laws and regulations requiring annual privacy and information security awareness training include the following:

- [The Privacy Act of 1974](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\)](#)
- [Federal Information Security Management Act \(FISMA\)](#)
- [Federal Records Act](#)
- [Freedom of Information Act \(FOIA\)](#)

#### Applicable ROB\*

Employee: [2h\(1\)](#)

Contractor: [2b18](#)

Refer to the Glossary and the Privacy and Information Security Resources listed in Appendices C and D to learn more about these laws and regulations.

VA must comply with several federal laws related to privacy and information security. This course is required for all [employees](#) and [contractors](#) to ensure you understand your roles and responsibilities for protecting privacy and ensuring information security.

Refer to the Glossary in Appendix C to learn more about employees and contractors.

Additionally, you will acknowledge and accept the [Rules of Behavior \(ROB\)](#) to confirm your understanding of these roles and responsibilities. These annual requirements are necessary for you to gain or maintain access to VA systems.

Refer to the Glossary in Appendix C to learn more about the ROB.

If you are a VA employee, your supervisor will ensure you:

- Complete the required privacy and information security training
- Sign Rules of Behavior (ROB).

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Refer to [Appendix A: Rules of Behavior for VA Employees](#) to read the ROB for employees. After you read this document, you will be required to acknowledge and accept these rules by signing and submitting a hard copy to your ISO.

If you are a contractor, your Contracting Officer Representative (COR) will ensure you:

- Complete the required privacy and information security training
- Sign Rules of Behavior (ROB).

Refer to [Appendix B: Rules of Behavior for VA Contractors](#) to read the ROB for contractors. After you read this document, you will be required to acknowledge and accept these rules by signing and submitting a hard copy to your COR.

Contractors must complete this VA Privacy and Information Security Awareness and Rules of Behavior training and read and sign the ROB before they are granted access to information systems.

Please note that the following personnel are also required to complete the more detailed privacy course, “Privacy and HIPAA Training” (TMS 10203):

- Employees with access to the Compensation and Pension Records Interchange (CAPRI)
- Veterans Health Administration (VHA) clinicians and personnel who have access to VHA systems containing VA sensitive information

### Rules of Behavior (ROB)

#### Applicable ROB\*

Employee: [1j](#), [2a\(2\)](#)

Contractor: [2b18](#)

The ROB describes the actions everyone MUST take to protect privacy and keep information secure. Some offices or facilities may require even more protection. Always follow the ROB and your local rules.

Remember, there are two versions of the ROB: one is for employees and one is for contractors. At the end of the course, you will acknowledge and accept the ROB by signing and submitting a hard copy to your ISO or COR, as appropriate. This will allow you to gain or maintain your access to VA information and information systems.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

### Employees

Employees include all individuals who are employed under Title 5 or Title 38, United States Code. This also includes volunteers, without compensation (WOC) employees, and students or other trainees.

To reference the Rules of Behavior for employees during this training:

- Select the links to the ROB applicable in each section of this document, or
- Turn to Appendix A to view a complete list of ROB.

When you complete this training, acknowledge and accept the Rules by signing and submitting a hard copy to your ISO.

### Contractors

Contractors include all non-VA users with access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must complete this VA Privacy and Information Security Awareness and Rules of Behavior training, which includes reading and signing the ROB, before they are granted access to information systems.

To reference the Rules of Behavior for contractors during this training:

- Select the links to the ROB applicable in each section of this document, or
- Turn to Appendix B to view a complete list of ROB.

When you complete this training, acknowledge and accept the Rules by signing and submitting a hard copy to your COR.

**Note:** The role referred to as the Contracting Officer's Technical Representative (COTR) in the ROB is now referred to as the COR.



### Course Objectives

This course is required because everyone who works for VA needs to understand why we care about privacy and information security. You need to know your role to help protect privacy and keep information safe.

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

- Recall the types of information that must be handled carefully to protect privacy
- Recognize the required information security practices to protect privacy when handling VA sensitive information, Personally Identifiable Information (PII), and Protected Health Information (PHI)
- Recognize the required information security practices to protect privacy when using personal and VA-issued electronic devices
- Recognize the legal requirements for privacy and information security and the associated consequences and penalties for non-compliance
- Identify the process for reporting incidents.

### Pay it Forward

When you do the right thing, you affect the lives of Veterans. This course is about how you can protect privacy and ensure information security to pay it forward.

What does it mean to “pay it forward?”

It’s simple. When you do the right thing, you give everyone around you the right idea. Your good choices set an example. You see a coworker do the right thing, and you’re inspired to do the right thing, too. We can’t always pay back the person who inspired us, but we can pay it forward.

The Rules of Behavior state what everyone must do. Read the Rules and be sure to follow them in your job every day. Protect Veterans and VA by protecting privacy, handling information carefully, and using information systems securely.

It’s all about serving Veterans. Veterans have protected all of us, now it’s our turn. We protect Veterans and their families – and VA – by protecting privacy and information security.

Make it your goal to pay it forward!

### **Prologue: Helping Veterans (Fictional Scenario)**

Sarah, a medical receptionist, is holding a folder of patient records as she walks down the hall. As she gets to the lobby area, she sees a Veteran on crutches struggling to pick up an envelope that he's dropped on the floor. She puts the folder on a nearby table to pick up the envelope. As Sarah puts the folder down, the cover of the folder becomes visible. The cover is a white sheet with red lines around the border. The word "CONFIDENTIAL" appears in red across the cover on a slant. Sarah hands the Veteran's envelope back to him. Harry is standing nearby in the lobby.

Sarah: Here you go.

Injured Veteran: Thanks. I appreciate it.

Sarah turns to walk away. Tom, another Veteran waiting for his appointment, saw Sarah put the patient records on the table. Tom notices that Sarah forgot to pick up the patient records and calls out to Sarah to hand them to her.

Tom: Miss...I believe these are yours? I didn't want you to forget them.

Sarah: Oh. Thank you. I almost forgot.

Harry, who was standing nearby, observed Tom reminding Sarah to never leave sensitive information unprotected in a public area. What will Harry do to pay it forward?

## Overview of Privacy and Information Security

### Introduction (Fictional Scenario)

Earlier in the day, Harry watched Tom remind Sarah to never leave sensitive information unprotected in a public area. Now, Harry is sitting in a chair next to the desk of his coworker, Patrice. The desk is covered with envelopes and papers. Samantha is standing in the doorway of Patrice's office.

Patrice: These have to go out today and it looks like we are missing a few. I don't know how that could have happened. I batch printed the statements.

Harry: Maybe they were put in the wrong envelope. Let's take a look.

Harry holds up an envelope with two letters

Harry: Here's one.

Patrice: Wow! That could have been bad.

Harry: Yeah, let's check the rest of these—better safe than sorry.

Samantha, who was standing in the doorway of Patrice's office, observed Harry help Patrice to protect sensitive information by verifying that the name and address on the envelopes and statements matched so they would be mailed to the right Veteran. How will Samantha protect Veteran information and pay it forward?

### Objectives

Let's get started with a closer look at what you need to do to protect privacy and ensure information security. We will explore the types of information to be protected. We'll also review what else you need to know about the laws and regulations.

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

- Recall your responsibilities to protect privacy and ensure information security
- Recognize the legal requirements for privacy and information security
- Recall the types of information that are considered sensitive and require protection.

### Protecting Privacy and Information Security

You and everyone you work with have a responsibility to protect [privacy](#) and keep information safe. To protect privacy and ensure [information security](#), you must:

- Protect VA sensitive information when talking with others and when using paper records or files
- Protect VA sensitive information when you use email and other electronic communication
- Protect VA sensitive information when you store, transport, and dispose of information in all formats
- Protect electronic devices issued by VA
- Report [incidents](#).

#### Applicable ROB\*

Employee: [1a, 2b\(13\)](#)

Contractor: [2b14](#)

Refer to the Glossary in the Appendix C for more information about privacy, information security, and incidents.

You are legally required to uphold these responsibilities and follow the law. Failure to do so can result in reprimand or job loss. Failure can even result in hefty fines, criminal prosecution, and prison. If you comply with the ROB, you will follow the law. Privacy and Information Security Laws and Regulations include:

- The Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA)
- [Health Information Technology for Economic and Clinical Health Act \(HITECH\)](#)
- Federal Information Security Management Act (FISMA)
- Federal Records Act
- Freedom of Information Act (FOIA)
- [VA Confidentiality Statutes \(38 U.S.C. 5701, 5705, 7332\).](#)

Refer to the Glossary and the Privacy and Information Security Resources in Appendices C and D to learn more about these laws and regulations.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



### Privacy: What to Protect

Privacy refers to what you must protect. To protect privacy, you must protect [VA sensitive information](#) that belongs to Veterans, their families, VA employees, and VA. VA sensitive information includes both private information about individuals and VA's internal business information.

Refer to the Glossary in Appendix C for more information about VA sensitive information.

Privacy may be violated by accident or with malicious intent. To protect privacy, do not allow VA sensitive information to be disclosed, altered, or destroyed unless it is authorized.

The three types of VA sensitive information include:

- [Personally Identifiable Information \(PII\)](#)
- [Protected Health Information \(PHI\)](#)
- [Internal Business Information.](#)

Personally Identifiable Information (PII) relates to a specific person, such as:

- Names, addresses, and phone numbers
- Social Security numbers (including the last four digits)
- Dates and places of birth
- Credit card numbers
- Education records
- Financial records
- Criminal and employment histories.

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

- Patient medical records and diagnoses
- Patient payment histories.

Internal Business Information communicates VA information that is not public knowledge, such as:

- Pricing information submitted to VA by vendors during bid processes
- Facility or computer room diagrams
- IT systems infrastructures used for servers, desktops, and laptops

- Operational business and information reports.

Refer to the Glossary in Appendix C for more information about Personally Identifiable Information (PII), Protected Health Information (PHI), and Internal Business Information.

### **Determining What is Sensitive and What is Not**

In this situation, can you identify what is sensitive and what is not?

Janice is cleaning up her desk at the end of the day. Before she leaves, she must sort through the items on her desk and determine which items contain VA sensitive information and which do not.

Which of the following items contain VA sensitive information?

- A. A completed medical history form
- B. A credit card number in a patient record
- C. A VA facility address
- D. All of the above
- E. Only A and B

The correct answer is E. The medical history form and credit card number are examples of items containing sensitive information. The VA facility address is public information and not considered sensitive.

### **Information Security: How to Protect It**

Information security refers to how you protect privacy and keep VA sensitive information safe. To ensure information security, you must maintain confidentiality, integrity, and availability.

Information security refers to how you protect VA sensitive information. To protect VA sensitive information, follow federal laws and regulations and the ROB.

You ensure information security when you maintain the following:

- [Confidentiality](#)—means information is not disclosed to people who do not have permission to know it. For example, VA sensitive information should not be made public.
- [Integrity](#)—means all information is kept from being damaged and is not altered to lose its intended meaning.
- [Availability](#)—means people with permission can access information systems and networks when they need it.

Refer to the Glossary in Appendix C for more information about confidentiality, integrity, and availability.

### What Can You Do to Protect VA Sensitive Information?

When you see VA sensitive information, do you know what to do to protect it?

Remember, you must keep VA sensitive information safe in all of your work locations. That includes VA facilities, remote offices, and your home.

#### Applicable ROB\*

Employee: [2a\(1\)](#), [2b\(4\)](#), [2b\(13\)](#), [2g\(6\)](#)

Contractor: [2b1](#), [2b2](#)

To protect VA sensitive information, follow these guidelines:

Always	Never
<ul style="list-style-type: none"><li>• Follow information security and privacy policies and procedures.</li><li>• Complete required training on time.</li><li>• View, access, and collect only the information you need to do your job.</li><li>• Encrypt VA sensitive information when stored on VA-issued devices or sent via VA email services.</li></ul>	<ul style="list-style-type: none"><li>• Throw VA sensitive information in the trash.</li><li>• Discuss VA sensitive information in public or share it with anyone who shouldn't have it.</li><li>• Share VA sensitive information with anyone who does not have a need to know.</li></ul>

**Note:** You will learn more tips for protecting VA sensitive information throughout this course.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

### Who Can Provide Support?

Don't hesitate to reach out to these individuals who can help you with questions or concerns about privacy and security. Your supervisor, PO, ISO, and/or CO/COR help you comply with all regulations.

#### Applicable ROB\*

Employee: [2a\(2\)](#), [2c\(1\)](#), [2h\(2\)](#)

Contractor: [1h](#)

### Privacy Officer (PO)

Some PO responsibilities are to:

- Promote privacy awareness
- Ensure compliance with federal laws and regulations and VA Directives
- Respond to privacy incidents
- Provide support when incidents occur
- Communicate privacy training requirements and deadlines
- Track privacy training completion.

To identify your PO use the ISO-PO-locator on the VA Intranet at <https://vaww.infoprotection.va.gov/index.aspx>

### Information Security Officer (ISO)

Some ISO responsibilities are to:

- Manage local information security programs and provide training
- Monitor access to VA information systems
- Help create and maintain information system security plans and emergency plans
- Assess system risks
- Take part in security self assessments and system audits
- Make sure information security measures are working as intended
- Respond to information security incidents.

To identify your PO use the ISO-PO-locator on the VA Intranet at <https://vaww.infoprotection.va.gov/index.aspx>

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



### Contracting Officer (CO)/Contract Officer Representative (COR)

Some CO/COR responsibilities are to:

- Ensure contractors sign the Contractor ROB each year
- Maintain the original or a copy of the Contractor ROB
- Be sure that contractors complete the required privacy and information security awareness training before they begin the contract and each year of the contract
- Be sure that contractors know when and how to report security and privacy incidents.

**Note:** The role referred to as the Contracting Officer's Technical Representative (COTR) in the ROB is now referred to as the COR.

### Supervisor

Some supervisor responsibilities are to:

- Ensure staff understand IT security and information protection issues
- Ensure staff comply with security regulations and policies
- Verify staff complete all privacy and information security training requirements
- Ensure staff sign the ROB each year
- Help staff report suspected incidents.

### The Continuous Readiness in Information Security Program (CRISP)

You may have heard about the Continuous Readiness in Information Security Program or CRISP. Here's more about what CRISP means to you.

The [Continuous Readiness in Information Security Program \(CRISP\)](#) emphasizes what each of us should do to protect VA sensitive information. The program ensures:

- The right people have the right access to the right IT systems
- You have the tools and training you need to protect privacy and information security.

If you are in a job with significant information security responsibilities, you must complete role-based information security training related to your role.

*“The trust Veterans have in us as a Department and as individuals depends on our ability to constantly and consistently protect their information from exposure and ever-increasing cyber risks. Security information is the responsibility of everyone. I encourage all VA employees, contractors, and affiliates to help us implement CRISP. Together we can and will safeguard the information that is vital to serving our Veterans.”*

—Secretary Eric Shinseki

CRISP Made Simple, VAnguard, March/April 2012

To learn more about CRISP, refer to the following on the VA intranet:

- CRISP website available at  
<http://vaww.sde.portal.va.gov/oitauditprep/SitePages/Home.aspx>
- ITWD's Role-based Training website available at  
<http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/default.aspx>
- Role Definitions PDF document available at  
<http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Shared%20Documents/Role%20Definitions.pdf>

Refer to the Glossary in Appendix C for more information about CRISP.

### Summary

Now that you have completed this module, you are aware of your role in protecting VA sensitive information and the federal laws and regulations requiring its protection and should be able to:

- Recall your responsibilities to protect privacy and ensure information security
- Recognize the legal requirements for privacy and information security
- Recall the types of information that are considered sensitive and require protection.

Key points from this module include the following:

Always	Never
<ul style="list-style-type: none"><li>• Follow information security and privacy policies and procedures.</li><li>• View, access, and collect only the information you need to do your job.</li><li>• Share VA sensitive information with only those who have a need to know.</li><li>• Secure VA sensitive information in all areas and all forms in all environments.</li><li>• Follow local procedures to dispose of VA sensitive information you no longer need.</li></ul>	<ul style="list-style-type: none"><li>• Throw VA sensitive information in the trash.</li><li>• Discuss VA sensitive information in public or share it with anyone who shouldn't have access to it.</li><li>• Share VA sensitive information with anyone who does not have a need to know.</li></ul>

## Protecting Private Conversations and Paper Records and Files

### Introduction (Fictional Scenario)

Earlier in the day, Samantha watched Harry help Patrice protect sensitive information by verifying the names and addresses on the envelopes matched the statements so they would be mailed to the right Veteran. Now, Samantha is talking to a nurse in the cafeteria about their frustrating morning. Gabe is standing nearby.

Nurse: I am so glad to see you! I have had such a crazy morning. I was in helping Mr. ...

Samantha: I've had a rough day too. Before we go into too much detail, let's go to a conference room where we can discuss things more privately.

The nurse and Samantha head out of the cafeteria. Gabe, who was standing nearby and overheard the conversation, observed Samantha stop the nurse from disclosing personally identifiable information in public. What will Gabe do to continue to protect PII and pay it forward?

### Objectives

In this module, you will learn how to protect VA sensitive information when you are talking with others or when you are using paper records and files.

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

- Recognize how to protect VA sensitive information, PII, and PHI in private conversations and paper records and files
- Recognize common mistakes when communicating VA sensitive information
- Choose the appropriate actions to protect privacy and ensure information security in private conversations and paper records and files.



### Protecting VA Sensitive Information in Person and by Phone

To protect VA sensitive information in person or when you use the phone, follow these guidelines:

#### Applicable ROB\*

Employee: [2b\(9\)](#)

Contractor: [1g](#), [2b10](#)

#### In Person

Always	Never
<ul style="list-style-type: none"><li>• Discuss VA sensitive information in private.</li><li>• Be aware of people around you.</li><li>• Close office doors or leave areas where others can overhear.</li><li>• Lower your voice or point to VA sensitive information instead of saying it aloud.</li></ul>	<ul style="list-style-type: none"><li>• Talk about VA sensitive information in public places, such as lobbies or elevators.</li></ul>

#### On the Phone

Always	Never
<ul style="list-style-type: none"><li>• Do the same things you do to protect your in-person conversations.</li><li>• Say things like, "I have a question about a client," when leaving voicemail.</li></ul>	<ul style="list-style-type: none"><li>• Give VA sensitive information over the phone to someone you don't know.</li><li>• Leave VA sensitive information on voicemail.</li></ul>

### What Are Records?

#### Applicable ROB\*

Employee: [2b\(8\)](#)

Contractor: [2b14](#)

Some of the information you work with may be part of [records](#). Be sure you know how to protect information contained in records.

Federal agencies must keep official copies of materials that show the work they do. These are known as records. These materials can be paper documents, electronic data, photographs and images, audio and video tapes, and other media.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Every work unit at VA must keep a list of the items that are considered records. This list is called a file plan. It says what the records are and where they are located.

Records must be maintained according to a [Records Control Schedule \(RCS\)](#) established by the National Archives and Records Administration (NARA). The RCS says how long official records must be kept and whether they are to be stored or destroyed when they are no longer needed.

Refer to the Glossary in Appendix C for more information about records and Records Control Schedules.

The Federal Records Act of 1950, as amended, 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.

Records are broadly defined by statute and regulation to include all recorded information, regardless of medium or format, made or received by VA under federal law or in connection with the transaction of public business, either preserved or appropriate for preservation because of their administrative, legal, fiscal, or informational value. Records serve as VA's memory; they are of critical importance in ensuring that VA continues to function effectively and efficiently.

### Protecting Paper Documents, Records, and Files

You need to know how to protect VA sensitive information when you use paper documents, records, and files. Remember, paper documents, records, and files refer to all non-electronic forms of information, such as x-rays, labels, and microfiche, etc.

#### Applicable ROB\*

Employee: [2b\(2\)\(a\)](#), [2b\(12\)](#)

Contractor: [1g](#)

### Paper Files

Some VA information is stored in paper format, in paper files. Follow these tips to protect paper files that contain sensitive information.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

To protect paper files:

- Do not leave files out in areas such as:
  - Public spaces
  - Private offices
  - Conference rooms
  - Copy machines
  - Fax machines
  - Mailboxes
  - Wall trays.
- Lock files and documents away when you are not in your work area.
- Always get written permission before you remove sensitive information from VA locations.
- Transport sensitive documents in locked containers or briefcases.

### Paper Records

Some paper files may include records that are identified in the Records Control Schedule.

- Always follow procedures for retaining or destroying records, and also follow procedures whenever transporting paper records that contain sensitive information.
- As long as paper records are actively used, protect sensitive information as with any other paper document.
- When transporting paper records to temporary or permanent storage, sort items into records which contain sensitive information and records which do not.
- Before shipping, place a cover sheet indicating sensitive information on top of any records containing sensitive information.
- Always ask your supervisor or office records administrator before you dispose of or destroy any material that may be a record.

Refer to VA Directive and Handbook series 6300 for more information about proper handling of paper records.

### Faxes

To protect faxes:

- Fill out a cover sheet and list these four items:

1. The name of the recipient
2. Your name and contact information
3. Instructions for the recipient to verify fax receipt
4. The confidentiality statement per VA Handbook 6500, Information Security Program:

*"This fax is intended for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by the 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 phone number listed above."*

Refer to the Glossary in Appendix C for more information about disclosure.

### Inter-Office Mail

To protect inter-office mail:

- Place documents in closed inter-office envelopes
  - For added safety, put VA sensitive documents in sealed envelopes inside the inter-office envelope
- Place a [Notice Sheet](#) in the closed inter-office envelope
  - Include the name of the recipient and verify his or her mail center address
- Hand out inter-office mail right away
- Transport sensitive documents in locked containers or briefcases.

Refer to the Glossary in Appendix C for more information about Notice Sheets.

### Regular and Courier Mail

To protect regular and courier mail:

- 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 that envelopes are securely sealed.
  - Make sure mass production 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.
- Ship original documents and media that contain VA sensitive information through a shipping service, such as UPS or FedEx, with tracking capabilities.
  - Ship copies of documents containing VA sensitive information through the United States Postal Service (USPS).

Refer to VA Directive 6609, Mailing of Sensitive Personal Information, for more information about handling mail.

### Protecting Records

#### Applicable ROB\*

Employee: [2b\(5\)](#), [2b\(9\)](#)

Contractor: [1g](#), [2b10](#)

Even a moment away from your desk can put information at risk. Consider this scenario.

Jenny is at her desk filing a stack of paper records that contain VA sensitive information. Her desk is located in an uncontrolled area with public access. Tanya, her

supervisor, asks Jenny to step into her office for a few minutes to discuss a new project.

What should Jenny do to protect the records while she is away?

- A. Turn the papers over on the desk
- B. Store the papers in a locked container, file cabinet, or desk drawer before she leaves the area
- C. Nothing. She won't be gone long

The correct answer is B. In this situation, Jenny cannot leave paper records that contain VA sensitive information unattended. She should store them in a locked container, file cabinet, or desk drawer while she is away from her desk.

If Jenny worked in a controlled area that did not allow public access, she would be able to secure the records by turning them over on her desk. Then, at the end of the day, the records should be secured in a locked container, briefcase, or file cabinet.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## Misdirected Mail

When you send VA sensitive information in the mail, it's important to pay attention to detail. Here's another scenario.

### Applicable ROB\*

Employee: [2b\(2\)\(a\)](#), [2b\(2\)\(b\)](#)

Samuel is a claims processing coordinator. He must mail original benefits documents to Veteran Joe Smith. What steps should Samuel take to make sure these documents are mailed in a secure manner?

- A. Verify the person's name on the envelope matches the name on the documents inside the envelope
- B. Double check that the envelope is sealed and Joe's name and mailing address are correct
- C. Mail the documents through shipping service, such as UPS or FedEx
- D. All of the above

The correct answer is D. Mail under VA control must be shipped in the most secure way possible. In this situation, Samuel should verify the person's name on the envelope matches the name on the documents inside the envelope, verify the envelope is sealed, make sure Joe's name and address are correct, and send the documents through a shipping service, such as UPS or FedEx.

**Note:** Copies of documents can be mailed using USPS. Original documents that are difficult to replace, such as service records, passports, and birth certificates, must be mailed through a shipping service with tracking capabilities.

## Written Log Books Containing VA Sensitive Information

### Applicable ROB\*

Employee: [2b\(6\)](#)

It may be tempting to use paper log books to take notes that you plan to enter into an electronic file later. Don't do it. Log books containing VA sensitive information can be lost or stolen.

VA does not allow the use of [paper log books for personal use](#). VA also discourages the use of paper log books in any situation where an electronic solution exists. This includes the use of paper log books in clinics and medical centers. Log books containing VA sensitive information must be maintained in electronic files on authorized VA systems.

Refer to the Glossary in Appendix C for more information about paper log books for personal use.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Sometimes federal directives require the use of a physical log. Here are some examples:

- Police logs
- Sign-in rosters to document appointments

Always	Never
<ul style="list-style-type: none"><li>• Work with your ISO to ensure the information is properly protected.</li><li>• Destroy the physical pages according to VA Records Management guidelines.</li><li>• Keep sign-in rosters in your sight and shred them using a VA-approved shredder at the end of each business day.</li></ul>	<ul style="list-style-type: none"><li>• Move sign-in rosters away from their area of use.</li></ul>

To maintain a paper log book, you must demonstrate a compelling business need and have it approved by the Facility or Program Director.

To get approval to use a paper log book, follow these steps:

1. Work with your PO or ISO to identify alternatives.
2. Make every effort to secure the log electronically on systems with appropriate security controls.
3. Have supervisors, Service Chiefs, or other responsible parties attest to the business requirement, location, and content.
4. Gain approval from the Facility or Program Director.

### Searching for an Alternative

Consider this scenario. A small lab team must end their use of a paper log book for patient sign-in. What should this lab team do with their patient log book?

**Applicable ROB\***

Employee: [2b\(6\)](#)

- A. Keep the paper log book, but log the entries in an electronic file on an authorized VA system
- B. Work with their PO or ISO to identify their options and make every effort to find an electronic alternative
- C. Keep the paper log book, but destroy the pages at the end of each day

The correct answer is B. In this situation, the best choice for this lab team is to work with their PO or ISO to identify their options and make every effort to find an electronic alternative.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

### Summary

Now that you have completed this module, you know some ways to protect VA sensitive information in paper records and files and when you are talking to other people in person or by phone.

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

- Recognize how to protect VA sensitive information, PII, and PHI in private conversations and paper records and files
- Recognize common mistakes when communicating VA sensitive information
- Choose the appropriate actions to protect privacy and ensure information security in private conversations and paper records and files.

Key points from this module include the following:

Always	Never
<ul style="list-style-type: none"><li>• Be aware of your surroundings and keep conversations private.</li><li>• Protect paper files and prevent unauthorized disclosure when sending faxes, inter-office mail, and regular mail.</li></ul>	<ul style="list-style-type: none"><li>• Discuss VA sensitive information, like PII or PHI, in public places in person or by phone.</li><li>• Keep unauthorized paper log books.</li></ul>



## Privacy in Electronic Communication Formats

### Introduction (Fictional Scenario)

Earlier in the day, Gabe watched Samantha stop a nurse from disclosing personally identifiable information in public. Now, Gabe is visiting a coworker, Victoria. Adam is sitting with Victoria at her desk.

Victoria: How was your meeting?

Gabe: Good. It was about email security—or lack of. Did you know that Outlook appointments aren't encrypted, meaning anyone can read them? Neither is the subject line of emails, even if they are encrypted. So, including sensitive information in the subject line, or in an invite, puts Veteran information at risk.

Victoria: Perfect timing for that bit of information. I was about to send this email with sensitive information in the subject line. I'll change it right away. Thanks!

Victoria turns back to her computer to fix the email that she was about to send. Adam heard Gabe sharing important information about e-mail security. As Adam continues through his day, what will he do to pay it forward?

### Objectives

In this module, you will learn how to protect VA sensitive information in electronic communications.

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

- Recognize how to protect VA sensitive information, PII, and PHI in electronic communications
- Recognize common mistakes when communicating private or VA sensitive information using electronic forms of communication
- Choose the appropriate actions to protect privacy and ensure information security when using electronic communication.

## Email

Email messages have the potential to be exposed. That is why you need to protect every email you send.

Information is safer if it is encrypted. VA uses [public key infrastructure \(PKI\) encryption](#) to keep email contents safe. PKI encryption prevents unintended recipients from being able to read information contained in email messages and their attachments. It also prevents others from intercepting that information while it is in transit.

PKI encryption does not prevent others from intercepting information sent in the subject line of email messages. Do not send VA sensitive information in the subject line of any email. Contact your local ISO or IT staff to request more information or to have PKI encryption installed.

Refer to the Glossary in Appendix C for more information about public key infrastructure (PKI) encryption.

To protect VA sensitive information in email:

### Applicable ROB\*

Employee: [2b\(10\)](#), [2b\(11\)](#), [2b\(13\)](#)

Contractor: [2b12](#)

Always	Never
<ul style="list-style-type: none"> <li>• Include your name and phone number in an email.</li> <li>• Confirm all individuals on the distribution list (a.k.a., contact group) are approved to receive the information.</li> <li>• Delete unnecessary emails and attachments containing VA sensitive information as soon as possible.</li> <li>• Save emails and attachments that may be official records.</li> </ul>	<ul style="list-style-type: none"> <li>• Autoforward e-mail messages to addresses outside the VA network.</li> <li>• Send VA sensitive information in the subject line of an email.</li> <li>• Send unencrypted VA sensitive information to an address outside of VA without approval.</li> <li>• Disable PKI encryption on any device.</li> </ul>

VA-issued laptops and mobile devices such as BlackBerry smart phones and iPads should also have PKI encryption installed to encrypt email.

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Refer to TMS course 1256927, Getting Started with Public Key Infrastructure to learn more about PKI encryption.

### Microsoft Communicator

**Applicable ROB\***

Employee: [2b\(13\)](#)

Contractor: [2b12](#)

Do not use [instant message](#) (IM) functionality to send VA sensitive information. Sending PII or PHI in an IM can put VA and Veterans at risk.

Any VA sensitive information you may communicate in an IM could also be information that must be contained in a system of records, such as a patient's health or claims record. Using IM instead of documenting patient or claims information in the official [system of records](#) creates a risk for VA. VA could incur fines and other penalties.

Any data transmitted via instant message must be de-identified. For more information about de-identification of data, refer to VHA Handbook 1605.1, Privacy and Release of Information.

Refer to the Glossary in Appendix C for more information about instant message (IM) and systems of records.

### Outlook Calendar

Be careful not to reveal VA sensitive information when you use electronic calendars. Do not enter VA sensitive information into a [Microsoft Outlook Calendar](#) item. It does not have proper security control.

**Applicable ROB\***

Employee: [2b\(13\)](#), [2e\(1\)](#), [2g\(2\)](#)

Contractor: [2b10](#), [2b12](#)

Only use secure electronic formats, such as encrypted email. If you work within VHA, you can also use VistA. Never use public electronic calendars, such as Google or Yahoo calendars. Public electronic calendars are not VA-approved.

Refer to the Glossary in Appendix C for more information about Microsoft Outlook Calendar.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## Microsoft SharePoint

### Applicable ROB\*

Employee: [2b\(13\)](#), [2g\(2\)](#)

Contractor: [2b10](#), [2b12](#)

[Microsoft SharePoint](#) helps you share information. Be sure you take these steps to protect VA sensitive information when using SharePoint.

VA has approved Microsoft SharePoint for you to use for online data storage and collaboration. SharePoint is found

on VA's intranet.

Your ISO and/or PO can help you determine which types of information can be shared on SharePoint. Do not share VA sensitive information on sites where everyone in VA has access.

Refer to the Glossary in Appendix C for more information about Microsoft SharePoint.

To protect VA sensitive information on SharePoint:

Always	Never
<ul style="list-style-type: none"><li>• Get access to only the sites you need to do your job.</li><li>• Share only the information your department needs to do its job.</li></ul>	<ul style="list-style-type: none"><li>• Share VA sensitive information on unrestricted sites or sites that do not require a log-in and password.</li><li>• Store unencrypted PII or PHI on a SharePoint site.</li></ul>

## Communicating with Colleagues

Always keep privacy and information security in mind when you are communicating with others. Consider this scenario.

Maureen works as a nurse for Dr. Danner. The doctor is very busy today. Dr. Danner sends Maureen an IM to ask her to review a patient chart and reply with the results of a recent blood test. Maureen reviews the chart and replies with the test results.

Is this use of instant messaging allowed?

- A. Yes
- B. No

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

The correct answer is B. Information about this patient's blood test is PHI and should not be communicated by IM. Also, the patient information shared in the IM in this example must be documented in the approved system of records, the patient's medical record.

### Using Social Media

VA supports the use of social media tools and internet technologies. To use them safely, follow policies and guidelines.

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 use these tools, be aware that they can be vulnerable to attacks, including [phishing](#) and [social engineering](#). Also, you are accountable for the content you publish.

VA Directive 6515, Use of Web-Based Collaboration Technologies, provides guidance for appropriate use of these tools. To protect VA sensitive information in Social Media:

#### Applicable ROB\*

Employee: [2e\(1\)](#), [2g\(2\)](#), [2h\(3\)](#)

Contractor: [2b12](#)

Always	Never
<ul style="list-style-type: none"><li>• Be professional and use good judgment when posting pictures and text.</li><li>• Limit the amount of information you reveal in text. Too many details revealed over a period of time can expose VA sensitive information.</li><li>• Be aware of the details you reveal in photos.</li><li>• Make it clear that you are not speaking as a representative of VA, unless you are the official spokesperson.</li></ul>	<ul style="list-style-type: none"><li>• Comment on VA legal matters unless you are the official spokesperson. (If you are the spokesperson, get approval from management first.)</li><li>• Post VA business or VA sensitive information in personal emails or external social media outlets, such as websites, Facebook pages, blogs, and Tweets.</li></ul>

Refer to the Glossary in Appendix C for more information about social media, blogs, Facebook, Twitter, Flickr, Yammer, phishing, social engineering, and Tweets.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



## Threats and Methods to Protect Mobile Devices

Criminals can target mobile devices such as BlackBerry smart phones and iPads. Be sure to use VA-approved [encryption](#) and passwords to protect any mobile devices you use for VA business. You should also follow these guidelines.

### Applicable ROB\*

Employee: [2b\(1\)](#), [2b\(14\)](#)

Contractor: [2b10](#)

Device	Threat	Protection
Wireless internet access or Wi-Fi	Hackers can access your device through <a href="#">wireless networks</a> to copy unencrypted data, email, contacts, and files.	<ul style="list-style-type: none"> <li>• Turn off the Wi-Fi option on your device unless you are using it at work or at home.</li> <li>• Only connect to websites on the Internet using VA's virtual private network (VPN) when you are in airports or other public places such as the library or coffee shop.</li> </ul>
Wireless Telephone Headsets	Other people can listen to phone conversations and download your data when you use an unencrypted wireless headset.	<ul style="list-style-type: none"> <li>• Use an encrypted headset or a wired headset. Please note that local policies may prohibit the use of wireless headsets.</li> </ul>
Text Messaging	Be aware, hackers may send you links to malicious websites in a text message. Experienced hackers can even send malware through text messages to gain full remote control of your device.	<ul style="list-style-type: none"> <li>• Do not send VA sensitive information via text messaging.</li> <li>• Do not click on website links or open attachments sent by unknown senders.</li> <li>• Use VA's approved security software to block malware.</li> </ul>

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Refer to the Glossary in Appendix C for more information about encryption, wireless networks, virtual private networks (VPN), and malware.

### Lost Mobile Device

Using a mobile device has risks. Consider this scenario.

Kim leaves his encrypted, password-protected BlackBerry on a table in a coffee shop. When he realizes it is missing, he returns to the shop to get it. His BlackBerry is not on the table and has not been turned in to the coffee shop's Lost and Found.

What is the level of risk for unauthorized access and inappropriate disclosure of information in this situation?

- A. High
- B. Medium
- C. Low

The correct answer is C. Because this VA-issued device is encrypted and password-protected, the risk of inappropriate disclosure is relatively low. However, Kim should report this incident to his supervisor, and his PO or ISO immediately. His supervisor, PO, and ISO will then notify the VA National Security Operations Center (NSOC). If no one is available, Kim can report directly to the VA NSOC by calling the VA Helpdesk at 800-877-4328. To identify his PO or ISO, he can use the ISO-PO locator on the VA intranet at <https://vaww.infoprotection.va.gov/index.aspx>.

#### Applicable ROB\*

Employee: [1f](#), [2d\(4\)](#)

Contractor: [2b10](#)

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

### Summary

Now that you have completed this module, you know some of the actions you can take to protect VA sensitive information in electronic communications and be able to:

- Recognize how to protect VA sensitive information, PII, and PHI in electronic communications
- Recognize common mistakes when communicating VA sensitive information using electronic forms of communication
- Choose the appropriate actions to protect privacy and ensure information security when using electronic communication.

Key points from this module include the following:

Always	Never
<ul style="list-style-type: none"><li>• Be aware of common threats to VA-issued mobile devices.</li><li>• Use VA-issued devices that are encrypted and password-protected.</li><li>• Be aware of the risks and guidelines for using social networking and collaboration tools.</li></ul>	<ul style="list-style-type: none"><li>• Disable VA-approved encryption.</li><li>• Send VA sensitive information in the subject line of any email.</li><li>• Discuss or post VA sensitive information in unsecured shared calendars or on social networking sites.</li></ul>

## Privacy when Storing, Transporting, and Disposing of Information

### Introduction (Fictional Scenario)

Earlier in the day, Adam heard Gabe sharing information about the lack of encryption in email subject lines. Now, Adam stops by a conference room to ask Carlos, a coworker, if he wants to go to get coffee. Yvette is sitting in a chair next to Carlos. She is working on her laptop.

Adam: Ready for coffee?

Carlos: Absolutely. I could really use some; this spreadsheet is giving me a headache. I can't believe how long it's taking to compile this research.

Adam: Should you lock your computer?

Carlos: We're just heading down the hall.

Adam: I know; it's just the right thing to do. It's a lot of sensitive information.

Yvette, who was sitting next to Carlos, overheard Adam remind Carlos to protect Veteran information by locking his computer. How will Yvette pay it forward?

### Objectives

In this module, you will learn how to store, carry, and dispose of paper and electronic files containing VA sensitive information.

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

- Recognize how to protect VA sensitive information when storing, transporting, and disposing of information in all media formats
- Recognize common mistakes in the storage, transportation, and disposition of files and records
- Choose the appropriate actions to protect privacy and ensure information security in the storage, transportation, and disposition of files and records.

## Protecting VA Sensitive Information from Theft, Loss, and Unauthorized Access

You must protect VA sensitive information stored on any devices you use. Some devices are more secure than others.

### Applicable ROB\*

Employee: [2b\(1\)](#), [2c\(2\)](#), [2g\(8\)](#), [2h\(4\)](#)

Contractor: [2b14](#)

Devices	Risks	Protection
Desktop and laptop computers	<ul style="list-style-type: none"> <li>• Loss</li> <li>• Theft</li> <li>• Unauthorized access to VA sensitive information through the use of a device or by someone seeing the computer screen</li> </ul>	<ul style="list-style-type: none"> <li>• Use passwords that meet VA's minimum requirements for password strength.</li> <li>• Log off your computer or lock your computer by pressing Ctrl + Alt + Delete on your keyboard then selecting "Lock this computer" before leaving the area.</li> <li>• Use privacy screens in public areas.</li> <li>• Position your screen to face away from passersby.</li> <li>• Do not disable VA-approved encryption.</li> <li>• Keep your laptop with you or use a locking cable.</li> </ul>
Mobile Devices (e.g., BlackBerry, iPad)	<ul style="list-style-type: none"> <li>• Loss</li> <li>• Theft</li> <li>• Unauthorized access to VA sensitive information through the use of device</li> </ul>	<ul style="list-style-type: none"> <li>• Do not disable VA-approved encryption.</li> <li>• Use password protection to meet VA's minimum requirements for password strength.</li> <li>• Store your device in a secure location.</li> </ul>

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



Devices	Risks	Protection
Removable Storage Devices	<ul style="list-style-type: none"> <li>• Loss</li> <li>• Theft</li> <li>• Unauthorized access to VA sensitive information by someone who does not have permission to access it</li> </ul>	<ul style="list-style-type: none"> <li>• Use only VA-issued devices and storage (e.g., USB drives/thumb drives, portable hard drives).</li> <li>• Do not disable VA-approved encryption.</li> <li>• Use password protection.</li> <li>• Store your device in a safe place.</li> </ul>
Other Devices with Internal Memory (e.g., biomedical equipment, copy machines)	<ul style="list-style-type: none"> <li>• Loss</li> <li>• Theft</li> <li>• Unauthorized access to VA sensitive information</li> </ul>	<ul style="list-style-type: none"> <li>• Store your device in a safe place (when possible).</li> <li>• Ask OIT staff to remove the memory before equipment is replaced or removed.</li> </ul>

Refer to the Glossary in Appendix C for more information about passwords and privacy screens.

## Guidelines for Protecting VA Sensitive Information on VA-issued Devices

Here are a few ways to protect VA sensitive information stored on your devices:

### Applicable ROB\*

Employee: [2b\(1\)](#), [2e\(1\)](#), [2h\(4\)](#)

Always	Never
<ul style="list-style-type: none"> <li>• Keep VA-issued devices safe from loss or theft.</li> <li>• Lock office and conference room doors when leaving computers or other devices behind.</li> <li>• Save and back up data using VA-approved storage, such as network drives or VA-issued thumb drives.</li> </ul>	<ul style="list-style-type: none"> <li>• Leave office doors or window unlocked.</li> <li>• Store VA sensitive information on unapproved, unencrypted devices or media.</li> </ul>

\*Source: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior

## Leaving for Lunch

### Applicable ROB\*

Employee: [2g\(8\)](#)

Contractor: [2b14](#)

Before you step away from your workstation, take steps to protect VA sensitive information. Consider this scenario.

Chad is leaving his office to go to lunch. What should Chad do before he leaves to protect VA sensitive information that can be accessed using his computer?

- A. Log off his computer
- B. Turn off his monitor
- C. Lock his screen by pressing Control + Alt +Delete and "Lock this computer"
- D. A or C

The correct answer is D. In this situation Chad should log off of his computer or lock his computer by pressing Ctrl + Alt + Delete on his keyboard then selecting "Lock this computer."

Turning off his monitor is not sufficient; it will only prevent people from seeing VA sensitive information on the screen when it is turned off. It does not prevent someone from turning the monitor back on to access VA sensitive information via his computer and network accounts.

## Transporting VA Sensitive Information

VA has many different types of work locations. You may work at one VA location, travel to remote offices, or even work from home. Take care to prevent the loss or theft of VA sensitive information when moving documents and devices between locations. Consider this scenario.

### Applicable ROB\*

Employee: [2h\(4\)](#), [2b\(9\)](#), [2h\(4\)](#)

Dana is traveling to another VA facility by airplane. She takes her briefcase along. It contains a VA-issued laptop and papers with VA sensitive information. She places the briefcase in the overhead compartment during the flight and forgets to take it with her when she gets off the plane.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

What should Dana have done to protect the VA sensitive information she was carrying?

- A. Placed a lock on her briefcase
- B. Stored her briefcase under the seat in front of her
- C. Checked the briefcase at baggage claim
- D. A and B
- E. A and C

The correct answer is D. When you travel, keep laptops and papers containing VA sensitive information with you at all times in a locked bag or briefcase. Never check these items as baggage.

Also, at the hotel use a VA-issued cable lock to secure your laptop if you leave it in the room. You should also follow the “clear desk policy.” That is, put away papers or CDs and media containing VA sensitive information so others can't see them in your room, hotel work centers, etc.

**Note:** VA does not provide locking bags or cases. People may purchase their own locking bag or case or buy a lock for a bag or case they already own.

### Guidelines for Transporting VA Sensitive Information

When you are carrying VA sensitive information from one place to another, follow these guidelines:

#### Applicable ROB\*

Employee: [2b\(4\)](#), [2h\(4\)](#)

Contractor: [2b10](#)

Always	Never
<ul style="list-style-type: none"><li>• Get written permission to take VA sensitive information outside of a VA facility.</li><li>• Use encrypted, VA-issued devices.</li><li>• Transport items in a locked bag or a secured case.</li><li>• Keep your items with you at all times in a locked bag or case, or store your items in a secure location.</li></ul>	<ul style="list-style-type: none"><li>• Store VA sensitive information on unapproved, unencrypted devices.</li><li>• Take VA sensitive information home without written permission.</li></ul>

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## A Case of Theft

### Applicable ROB\*

Employee: [1f](#), [2d\(5\)](#), [2e\(1\)](#)

Lost or stolen laptops containing VA sensitive information can put information at risk. Consider this scenario.

Evan is a researcher who is driving to work at a VA facility. Evan uses his personal laptop for work, and he has his laptop with him in the car. Evan stops at a coffeehouse to pick up breakfast. When he returns to his car, Evan finds that someone has broken into his car and stolen his laptop. Evan failed to have his personal laptop encrypted with VA-approved encryption.

In this situation, what is the risk that someone could get the information on Evan's laptop?

- A. High
- B. Medium
- C. Low

The correct answer is A. In this situation, Evan's laptop is a high risk for unauthorized access.

You must have VA-approved encryption installed on any personal or VA-issued device used to conduct VA business. If a device is lost or stolen, report the incident to your supervisor and your PO or ISO immediately.

**Note:** You must have written permission from your ISO to use any personal devices to conduct VA business.

## Storage and Disposal of Records

### Applicable ROB\*

Employee: [2b\(8\)](#), [2b\(15\)](#)

Contractor: [2b11](#), [2b14](#)

Some documents are records. Be sure you know how to store or transport them safely.

Every VA office must inventory its records and have an approved Records Control Schedule (RCS). The RCS states how long records must be kept. A local file plan

states the location of records.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

It is illegal to destroy or dispose of records before the disposition date stated in the RCS. Keep in mind:

- When records have been kept as long as required, they must be destroyed by one of the approved methods
- Sometimes records that are no longer being used must be moved to National Archives and Records Administration (NARA) storage
- Records containing sensitive information must be protected during transfer to storage.
- You can be fined or penalized if you do not follow procedures for keeping or destroying records. If the records contain VA sensitive information, consequences can be even more severe.

Consult your records officer before destroying or moving records to storage.

VA Directive 6300, Records and Information Management, and the related handbook series provide guidance for proper handling of records at VA. VA Handbook 6300.1, Records Management Procedures, identifies procedures to follow for using and disposing of records in all work units.



## Guidelines for Disposing of Paper and Electronic Media

To dispose of paper and electronic media, you should follow these guidelines:

### Applicable ROB\*

Employee: [2b\(8\)](#), [2b\(15\)](#)

Contractor: [2b11](#)

Media Type	Method	Guidelines
Paper Files	Destruction	<ul style="list-style-type: none"> <li>Printed forms of VA sensitive information must be destroyed by a VA-approved shredder.</li> <li>Documents must be placed in locked shredding bins or containers so the contents may be shredded.</li> </ul>
Paper Records	Destruction	<ul style="list-style-type: none"> <li>Paper records may only be destroyed when stated in the RCS.</li> <li>Sometimes materials that are records have not yet been included in an RCS. These “unscheduled” records cannot be destroyed. Before destroying any materials that may be records, first consult your records custodian or facility records officer.</li> <li>Paper records must not be thrown out in wastebaskets or dumpsters. They must be destroyed by shredding, burning, or <a href="#">macerating</a>.</li> </ul>
Electronic Media	Sanitation and Disposal	<ul style="list-style-type: none"> <li>All electronic media that contain VA sensitive information must be sanitized or destroyed when it is no longer being used.</li> <li>Ask your ISO for help with the sanitization and disposal or redistribution of media.</li> </ul>

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## Retiring Old Files and Media

### Applicable ROB\*

Employee: [2b\(15\)](#)

It's important to know what you need to do to dispose of old files and media. Consider this scenario.

Frieda has been a VA employee for 25 years. She will retire next month. She has many drawers full of paper documents, CDs, videos, and USB drives. All of these items contain VA sensitive information.

What should Frieda do with these materials before she retires?

- A. Frieda should sort materials by paper or digital media, box up everything, and stack it neatly for the next occupant of her office
- B. Frieda should take home a few souvenirs of projects she worked on and just leave the rest where it is
- C. Frieda must work with her supervisor and records officer to identify which materials are records and what to do with them
- D. Frieda should consult Human Resources for advice

The correct answer is C. Frieda must work with her supervisor and records officer to ensure any materials that are records are identified, included in the RCS, and properly stored or destroyed. Records must be retained for the period of time required in the RCS. Records must not be removed from VA.

---

\*Source: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior

### Summary

Now that you have completed this module, you know more about how to safely store, transport, and dispose of paper and electronic files containing VA sensitive information and should be able to:

- Recognize how to protect VA sensitive information when storing, carrying, and disposing of papers or electronic files
- Recognize what not to do in the storing, carrying, and disposing of files and records
- Choose the correct way to protect privacy and information security in the storing, carrying, and disposing of files and records.

Key points from this module include the following:

Always	Never
<ul style="list-style-type: none"><li>• Use password protection and encryption on VA-issued devices.</li><li>• Log off or lock your computer before leaving the area.</li><li>• Transport sensitive items in a locked bag or secured case with a locking cable.</li><li>• Follow VA policies and procedures for disposing of VA sensitive information in paper or electronic form.</li></ul>	<ul style="list-style-type: none"><li>• Take VA sensitive information home unless you have written permission.</li></ul>

## Protecting VA-Issued Electronic Devices

### Introduction (Fictional Scenario)

Earlier in the day, Yvette overheard Adam remind Carlos to protect Veteran information by locking his computer. Now, Yvette is talking with a receptionist at the front desk. The receptionist is writing on a yellow sticky note; revealing her password.

Yvette: Good morning. I have a quick question for you on the schedule for today.

Receptionist: Give me one second. I just changed my password; I had to write it down so I wouldn't forget it.

Yvette: I have the same problem. I write mine down and lock it in a drawer in my office until I have it memorized. That way no one else can access it or accidentally see it.

Receptionist: Oh, good point. I'll do that instead.

As Yvette and the receptionist discuss how to keep passwords safe, the receptionist turns to put the yellow sticky with her password on it in a desk drawer with a lock. Tom, a Veteran, walked by.

Tom observed Yvette sharing a better method for protecting passwords. It's the little things we do every day that help protect Veteran information. What will you do to pay it forward?

### Objectives

In this module, you will learn how to protect VA-issued devices. You will also learn about VA's policies for teleworking, using remote access, and using personal equipment.

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

- Recognize how to protect VA-issued electronic devices from attacks that can damage equipment, systems, software, and networks
- Recall procedures for teleworking and obtaining written permission to take work off site
- Recognize common mistakes when using VA-issued electronic devices
- Choose the correct way to protect privacy and ensure information security when using VA-issued electronic devices
- Recall VA policies regarding the use of personal equipment.

### VA-Issued Devices

It is important to protect your VA-issued devices from loss, theft, and misuse. VA employees, contractors, and volunteers use a variety of VA-

issued devices to support their work. Examples of VA-issued devices include desktop computers, laptops, BlackBerry smart phones, USB drives, bio-medical equipment, and copy machines.

#### Applicable ROB\*

Employee: [2b\(16\)](#), [2f\(1\)](#), [2f\(3\)](#), [2f\(4\)](#), [2f\(5\)](#), [2h\(4\)](#)

Contractor: [2b5](#), [2b14](#), [2b16](#)

Always	Never
<ul style="list-style-type: none"><li>• Have government furnished equipment scanned and serviced by VA authorized personnel.</li><li>• Permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.</li><li>• Protect them from loss, theft, damage, and misuse.</li><li>• Sign for them upon receipt and return them when you don't need them anymore.</li></ul>	<ul style="list-style-type: none"><li>• Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee.</li><li>• Disable VA-approved security tools.</li></ul>

### Personal Identity Verification (PIV) Cards

VA employees and contractors use personal identity verification cards. All VA employees and contractors who have physical access to VA buildings, networks, and resources are required to carry [Personal Identity Verification \(PIV\) cards](#).

To get a PIV card, you must complete paperwork confirming your identity. Ask your supervisor for guidance.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



Always	Never
<ul style="list-style-type: none"> <li>• Protect your card from loss or theft.</li> <li>• Report loss or theft immediately to your ISO.</li> </ul>	<ul style="list-style-type: none"> <li>• Share your card with anyone.</li> </ul>

Refer to the Glossary in Appendix C for more information about Personal Identity Verification (PIV) Cards.

A PIV card, which is also known as a PIV badge, is an identification card that complies with FIPS 201 and related guidance.

A PIV card contains a photograph and stored identity information so that the claimed identity of the cardholder can be verified by another person or an automated process.

PIV badges are issued to persons requiring routine access to VA facilities or information systems.

A non-PIV badge is a VA ID card containing a photograph issued to persons who do not require a PIV Badge but need unaccompanied, infrequent access to VA facilities or information systems for a period not to exceed six (6) months.

Visit <http://www.va.gov/PIVPROJECT/index.asp> or contact your ISO to learn more about the use of PIV cards.

## Limited Personal Use of VA-Issued Devices

There are limitations on use of government equipment for personal activities.

Employees may use VA-issued devices for personal activities as long as this use:

- Doesn't interfere with work
- Involves minimal cost
- Doesn't affect productivity
- Doesn't violate standards of ethical conduct.

Contractors do not have limited personal use unless it is stated in the terms of the contract.

### Applicable ROB\*

Employee: [1d](#), [2a\(4\)](#), [2g\(7\)](#)

Contractor: [2b6](#)

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

No one may use VA-issued devices for [prohibited activities](#). Prohibited activities include, but are not limited to:

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

Review the Glossary in Appendix C for more information about prohibited activities.

### Personal Use

Employees may use VA-issued devices for certain kinds of personal activities. Consider this scenario.

Greta's husband is celebrating his 50th birthday next month. She is planning a big party for him. Greta uses her VA-issued laptop and email account to send a birthday party invitation to her husband's friends, family, and co-workers.

Is it appropriate for Greta to use her VA-issued laptop and email account to send out this party invitation?

- A. Yes
- B. No

The correct answer is B. In this situation, Greta is sending out a mass email. According to VA's policy regarding limited personal use, you may not use VA resources and devices to support unapproved mass mailing.

**Applicable ROB\***

Employee: [2g\(7\)](#)

---

\*Source: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior

## Password Requirements

### Applicable ROB\*

Employee: [2c\(2\)](#), [2c\(3\)](#), [2c\(4\)](#)

Contractor: [2b8](#), [2b9](#)

Strong passwords are difficult to guess or attack using brute force. They help to protect VA sensitive information from unauthorized access.

Passwords must be used on all VA information systems. To protect your VA-issued devices and your access to VA sensitive information, you must meet the password requirements for length and character types. For example, your password must contain at least eight characters from three of the following four categories:

- English uppercase letters
- English lowercase letters
- Digits 0–9
- Special characters (e.g., #, %, @)

Always	Never
<ul style="list-style-type: none"><li>• Use passwords that meet VA's character and length standards.</li><li>• Keep your passwords private.</li><li>• Store written passwords in a locked drawer or cabinet.</li><li>• Change your passwords every 90 days.</li></ul>	<ul style="list-style-type: none"><li>• Share your password with anyone.</li><li>• Store your password on a piece of paper near your computer or on an electronic device.</li><li>• Falsify, obscure, destroy, or replace someone else's password or user identity.</li></ul>

Strong passwords must meet VA's minimum password requirements. Examples of strong passwords include PuPe4u&Mi\* and LEvRg\$hM.

Weak passwords may contain:

- Your username, a real name, or company name
- Complete dictionary words
- Words that are similar to previous passwords
- Words using increments such as Password 1, Password 2.

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Examples of weak passwords include Johndoe#1 and Veteransaffairs#2.

Refer to the Glossary in Appendix C and VA Handbook 6500, Appendix F, VA Password Management for more information about passwords.

### Remote Access

Connecting to VA's network from locations outside of VA facilities can make equipment, systems, and networks more vulnerable to attack.

#### Applicable ROB\*

Employee: [2b\(1\)](#), [2b\(2\)](#), [2d\(1\)](#), [2d\(2\)](#), [2d\(3\)](#), [2d\(6\)](#)

Contractor: [3a](#), [3b](#), [3c](#)

To access VA's network from outside a VA facility, you need a [remote access](#) account. Your remote access account connects you to VA's network through a secure [virtual private network \(VPN\)](#).

Contact your ISO for information on how to obtain a remote access account. You must have written permission from your supervisor or COR, ISO, and local CIO in order to access VA sensitive information remotely.

Always	Never
<ul style="list-style-type: none"><li>Follow remote access procedures.</li><li>Let your supervisor and ISO know when you no longer need remote access.</li></ul>	<ul style="list-style-type: none"><li>Connect to non-VA systems when you are connected to VA's network.</li></ul>

Refer to the Glossary in Appendix C for more information about remote access and virtual private networks (VPNs).

### Wireless Devices and Networks

#### Applicable ROB\*

Employee: [2b\(14\)](#), [2d\(2\)](#), [2g\(4\)](#)

Contractor: [3a](#)

Using wireless devices and networks in public places can be risky. It is more difficult to protect VA sensitive information accessed outside of VA locations.

Wireless networks and devices can put VA at risk.

You should use a hard-wired connection to VA's network when possible.

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

If you must use a wireless connection, be sure to use VA-approved remote access and wireless devices.

Always	Never
<ul style="list-style-type: none"><li>• Use a hard-wired connection to connect to VA's network when possible.</li><li>• Use VA-approved remote access and wireless devices to connect to networks.</li></ul>	<ul style="list-style-type: none"><li>• Establish unapproved wireless networks in VA facilities.</li></ul>

### Telework Arrangement Approved

Consider this scenario. Robert has just received permission to telework from his home twice a week. However, he must frequently access and transmit VA sensitive information as part of his job.

#### Applicable ROB\*

Employee: [2b\(4\)](#), [2b\(8\)](#), [2d\(4\)](#)

Contractor: [2b3](#), [2b14](#)

What should he do to protect VA sensitive information when he works from home?

- A. Get permission to access and transmit VA sensitive information from outside a VA facility
- B. Identify a secure cabinet or desk drawer he can use to store documents containing VA sensitive information
- C. Identify a secure location for his personal shredder so he can dispose of documents containing VA sensitive information
- D. Only A and B
- E. All of the above

The correct answer is D. Robert should get written permission from his supervisor, ISO, PO and/or CIO to access VA sensitive information from outside a VA facility. He should also find a safe place to store sensitive information when he is not at his desk. This location must be separate from his personal files.

Robert must not use a personal shredder to shred VA sensitive documents. He must transport these items to a VA facility in a locked bag or container and dispose of them in a locked shredder bin for VA-approved shredding.

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



## Social Engineering Attacks

### Applicable ROB\*

Employee: [2c\(3\)](#), [2g\(3\)](#)

Contractor: [2b8](#)

Social engineering can be a big threat to VA. People can trick you into giving them information by taking advantage of your trust.

Social engineers may approach you in person or call or email you to get information. They can use your responses to get access to VA sensitive information.

Examples of social engineering attacks include:

- An individual asking for your username and password (in-person, over the phone, or via IM message)
- Pop-up windows that ask you to re-enter your username and password
- Emails with appealing subject lines that contain harmful content, for example:
  - Attachments with malicious code
  - Embedded hyperlinks to malicious web sites.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## Threats to Systems, Software, and Networks

Watch for threats to VA sensitive information stored on VA systems, software, and networks. Read about the common threats listed below to learn how you can protect VA sensitive information from attacks.

### Applicable ROB\*

Employee: [2f\(1\)](#), [2f\(2\)](#), [2f\(3\)](#), [2g\(1\)](#)

Contractor: [2b15](#), [2b16](#)

Threat	Risk	Protection Methods
<a href="#">Malware</a> <ul style="list-style-type: none"> <li>Viruses</li> <li>Worms</li> <li>Trojan horses</li> <li>Spyware</li> </ul>	<ul style="list-style-type: none"> <li>Interrupts computer function</li> <li>Collects VA sensitive information</li> <li>Gains unapproved access to computer systems</li> <li>Alters or deletes VA information</li> </ul>	<ul style="list-style-type: none"> <li>Only use VA-approved security software.</li> <li>Don't open suspicious email attachments or websites.</li> <li>Don't select links inside pop-ups.</li> <li>Don't download unapproved software, free trials, etc. (Always check with confirmation by your ISO to make sure it is VA-approved software)</li> </ul> <p>Note: The VA Network Security Operations Center (NSOC) monitors all network traffic for unusual or unapproved activities.</p>
<a href="#">Peer-to-Peer (P2P) File Sharing</a> software, such as: <ul style="list-style-type: none"> <li>Bit Torrent</li> <li>Kazaa</li> <li>Google Documents</li> </ul>	<ul style="list-style-type: none"> <li>Allows people to connect and trade files</li> </ul>	<ul style="list-style-type: none"> <li>Don't download P2P fileshare software.</li> <li>P2P file sharing is not allowed on VA-issued devices or networks. Regular network scans detect P2P programs.</li> </ul>

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Threat	Risk	Protection Methods
<a href="#">Phishing</a>	<ul style="list-style-type: none"> <li>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.”</li> </ul>	<ul style="list-style-type: none"> <li>Right click the suspicious link to display the URL.</li> <li>Note: Phishing links often have one or two characters that are different from the real website. For example. <a href="#">www.ebay.webs.com</a> (phishing URL) vs. <a href="#">www.ebay.com</a> (real URL).</li> </ul>
<a href="#">Spoofing</a>	<ul style="list-style-type: none"> <li>Appears as a link to a real website and takes user to a fake site. For example, you receive an email that appears as if it came from a known sender, but it is from a spoofer.</li> </ul>	<ul style="list-style-type: none"> <li>Ensure you have VA-approved encryption on your devices.</li> <li>Type in the website address instead of selecting links provided.</li> <li>Note: OIT staff combat spoofing by using filters on all network traffic.</li> </ul>

Refer to the Glossary in the Appendix to learn more about malware, P2P file sharing software, phishing, and spoofing.

## Preventing Attacks

They say an ounce of prevention is worth a pound of cure. This is certainly true when it comes to preventing attacks or limiting the amount of damage these attacks can cause.

### Applicable ROB\*

Employee: [1f](#), [2c\(3\)](#), [2f\(1\)](#), [2f\(2\)](#), [2f\(3\)](#), [2g\(5\)](#)

Contractor: [2b8](#), [2b15](#), [2b16](#)

Always	Never
<ul style="list-style-type: none"> <li>• Use VA-approved security software and update it on a regular basis.</li> <li>• Avoid strange websites.</li> <li>• Report anything odd on your computer system, such as: <ul style="list-style-type: none"> <li>○ Weird characters in documents or email</li> <li>○ Missing data</li> <li>○ Sudden increases in spam or unsolicited email</li> <li>○ Emails with strange attachments.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Share your passwords with anyone.</li> <li>• Download unapproved software.</li> <li>• Open strange emails or attachments.</li> <li>• Disable security software.</li> <li>• Probe systems or exploit system controls to access VA sensitive information—unless specifically authorized by the VA CIO.</li> </ul>

## Use of Personal Devices

Before you can use personal devices, such as personal laptops, you must first get written permission.

### Applicable ROB\*

Employee: [2e\(1\)](#), [2e\(2\)](#), [2e\(3\)](#), [2g\(1\)](#)

Personally owned portable and mobile devices must meet VA and the facility's security policies, procedures, and configuration standards before being allowed access to any VA network. These devices include portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, PDAs, cellular telephones, digital cameras, and audio recording devices).

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

To use a personal device to conduct VA business:

Always	Never
<ul style="list-style-type: none"><li>• Get written permission from your supervisor and local CIO.</li><li>• Use VA-approved security software.</li><li>• Allow OIT staff to examine your device.</li></ul>	<ul style="list-style-type: none"><li>• Store VA sensitive information on a personal device unless you have written permission.</li><li>• Access or transmit VA sensitive information on a personal device without VA-approved encryption.</li><li>• Charge your personal smart phone using a VA computer.</li></ul>



### Summary

Now that you have completed this module, you know some ways to protect VA-issued devices from attack. You should also be aware of VA's policies for teleworking, using remote access, and using personal devices, and you should be able to:

- Recall VA policies regarding the use of personal equipment
- Recognize how to protect VA-issued electronic devices from attacks that can damage equipment, systems, software, and networks
- Recall procedures for teleworking and obtaining written permission to take work off site
- Recognize common mistakes when using VA-issued electronic devices
- Choose the appropriate actions to protect privacy and ensure information security when using VA-issued electronic devices.

Key points from this module include the following:

Always	Never
<ul style="list-style-type: none"><li>• Avoid odd websites and weird emails and attachments.</li><li>• Report any strange activity on your computer system.</li><li>• Ensure your VA-approved security software is enabled.</li><li>• Ensure your devices are encrypted and password-protected.</li><li>• Sign for devices upon receipt and return them when you no longer need them.</li></ul>	<ul style="list-style-type: none"><li>• Share your passwords with anyone.</li><li>• Take, use, or store sensitive documents in a home office without written permission.</li><li>• Give VA-issued hard drives or other storage devices to anyone other than authorized OIT personnel.</li><li>• Override, bypass, or disable security controls on VA-issued devices without written permission.</li></ul>

## Reporting Incidents

### Introduction

Throughout the course, you've seen individuals doing the right thing and paying it forward. If left unchanged, the events in each of these scenarios could have led to incidents. Incidents such as:

- Medical records exposed to access by unauthorized individuals
- Letter with PII/PHI sent to wrong person
- Private information discussed in public
- Sensitive information disclosed in an email subject line
- Password exposed to theft
- Information systems exposed to access by unauthorized individuals.

### Objectives

In this module, you will learn the steps to report incidents. You will also learn about the consequences that can result when incidents occur.

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

- Recall the steps to report incidents
- Recognize the range of consequences and penalties that may result from incidents
- Choose the right actions to protect privacy and ensure information security by following the steps to report incidents.

### Defining Incidents

You have a duty to report all incidents. Anytime you hear or see something that is of concern, report it.

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

#### Applicable ROB\*

Employee: [1f](#), [1g](#)

Contractor: [1h](#)

- Hearing one person share VA sensitive information with another person who should not have access to that information
- Seeing someone access files and records that he or she should not access
- Seeing someone change or delete data without permission
- Receiving a piece of mail or an email you should not receive
- Finding documents and devices that have VA sensitive information
- Noticing computer systems that are not working well
- Experiencing issues with malware or viruses
- Witnessing or experiencing loss, theft, damage, or destruction of equipment.

**Remember:** Any time you hear or see something that is of concern, report it! All possible incidents should be reported.

### Impact

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 national security

Incidents can have a negative impact on:

- **Veterans**—by causing embarrassment, financial loss, or identity theft. Veterans can lose confidence in VA. As a result, they may avoid seeking medical treatment or other benefits. This can lead to a reduced quality of life for them.
- **VA**—by causing the loss of public trust. This could cost millions of dollars to notify individuals and repair our reputation.
- **You**—by resulting in disciplinary actions, job loss, fines, and criminal charges or imprisonment if you are the cause of an incident.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

### Consequences

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

**Applicable ROB\***

Employee: [1e](#)

Serious consequences of privacy and information security violations may include:

- Required training
- Suspension of your access to systems
- Reprimand in your personnel file
- Suspension from your job, demotion, or job loss
- Civil or criminal prosecution
- Fines
- Imprisonment.

### Civil and Criminal Penalties

**Applicable ROB\***

Employee: [1e](#)

Contractor: [1e](#)

Unfortunately, some people try to use VA sensitive information for personal gain. Theft, fraud, and unauthorized disposal or destruction of federal property or information can result in fines and other 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 3 years in prison
- Violate the Privacy Act, you can face up to \$5,000 and a year in jail per occurrence.

VA could also face fines up to \$1.5 million per year per instance for these types of violations.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Refer to Appendix A of VA Handbook 5021.6, Employee/Management Relations available on the VA intranet at [http://vaww1.va.gov/ohrm/directives-handbooks/direct\\_hand.htm](http://vaww1.va.gov/ohrm/directives-handbooks/direct_hand.htm), or contact your Human Resources or Employee Relations representative for more information.

### The Steps to Report an Incident

Do you know what to do if you witness an incident or suspect an incident has occurred?

If you see or hear something that is of concern, report it! All possible incidents should be reported.

To report an incident, follow these steps:

1. Call your supervisor and your PO or ISO right away! Report all actual and potential incidents. **Note:** if you are a contractor, you should also report every incident to your COR and Project Manager.
2. Communicate the following details:
  - What happened (e.g., what information was shared)?
  - Who was involved?
  - When did it happen?

Your PO or ISO will report the incident to VA's Network Security Operations Center (NSOC). He or she must report incidents to the VA NSOC within one hour of being discovered or reported.

**Note:** If the incident occurs after hours, on the weekend, or over a holiday, you should call the VA Helpdesk at 800-877-4328 to report what happened.

#### Applicable ROB\*

Employee: [1f](#), [1g](#)

Contractor: [1h](#)

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



## Additional/Alternate Contacts

If you can't reach your supervisor, Information Security Officer, or Privacy Officer, here are other ways to report an incident.

### Applicable ROB\*

Employee: [1f](#), [1g](#)

Contractor: [1h](#)

If...	Then...
Your supervisor, ISO, and PO are not available	Call the VA Helpdesk at 800-877-4328 to report the incident directly to the VA NSOC.
An incident occurs after hours or on a weekend	Call the VA Helpdesk and follow your work unit's procedures to notify your supervisor and VA NSOC.
You suspect an unethical or criminal action has occurred	Contact local VA police and the Office of Inspector General (IG) as well as your supervisor (or COR) and ISO or PO.
You suspect fraud, waste, or mismanagement of resources	Call the IG Hotline at 800-488-8244.
You suspect your supervisor is involved in the incident	Report the incident to your ISO or PO.

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## Filing a Report

### Applicable ROB\*

Employee: [1d](#), [1f](#)

Contractor: [1h](#)

Any time you hear or see something that is of concern, it's important to report it. Consider this scenario.

Susan is planning to take a week of vacation. Sharon, her supervisor, asks if she is still having difficulty with her ulcer medications. Susan suspects Sharon has been looking at her medical record without authorization.

What should Susan do?

- A. Confront her supervisor
- B. Call her ISO or PO
- C. Call the police

The correct answer is B. Susan should call her ISO or PO to report the incident and describe what happened, when it happened, and who was involved.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

## Summary

Now that you have completed this module, you know more about the steps to report incidents and the consequences that can result when incidents occur and should be able to:

- Recall the steps to report incidents
- Recognize the range of consequences and penalties that may result from incidents
- Choose the appropriate actions to protect privacy and ensure information security by following the steps to report incidents.

Key points from this module include the following:

Always	Never
<ul style="list-style-type: none"><li>• Report incidents or suspected incidents right away.</li><li>• Contact your supervisor (or COR) and your PO or ISO.</li><li>• If your supervisor (or COR), PO, and ISO are not available, report the incident directly to the NSOC by calling the VA Helpdesk: 800-877-4328.</li></ul>	<ul style="list-style-type: none"><li>• Be afraid to report an incident—any time you hear or see something of concern, report it!</li></ul>

## Course Summary and ROB

### Course Summary

Know that the work you do is important. When you do the right thing by protecting VA information, you are protecting Veterans and their families as well as VA and its employees.

To protect privacy and ensure information security:

- Protect private conversations and paper records and files
- Protect privacy in electronic communication formats
- Protect privacy when storing, transporting, and disposing of information in all media
- Protect VA-issued electronic devices
- Report incidents.

### Sign and Comply with the ROB

#### Applicable ROB\*

Employee: [1a](#), [1i](#), [1j](#), [3a](#), [3b](#)

Contractor: [5](#)

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

Everyone at VA must accept responsibility for protecting privacy and ensuring information security by accepting, acknowledging, and complying with the

ROB. The ROB are the minimum compliance standards for all VA locations. Local policies may require even more protection. You must accept and acknowledge the ROB to receive or maintain access to VA information or information systems.

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

To complete this training, locate the Rules of Behavior in the Appendix that are right for you.

- [Appendix A](#) provides the Rules of Behavior for VA Employees.
- [Appendix B](#) provides the Rules of Behavior for VA Contractors.

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

**Note:** Employees are defined as all individuals who are employed under Title 5 or Title 38, United States Code. This also includes volunteers, without compensation (WOC) employees, and students or other trainees. Contractors are defined as all non-VA users with access to VA information resources through a contract, agreement, or other legal arrangement.

Employees and contractors must read and sign the ROB to be granted access or maintain current access to VA information systems.

### Course Completion

Congratulations! You have successfully completed the VA Privacy and Information Security Awareness and Rules of Behavior training.

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

- Recall the types of information that must be handled carefully to protect privacy
- Recognize the required information security practices when handling VA sensitive information, PII, and PHI
- Recognize the required information security practices when using personal and VA-issued electronic devices
- Recognize the legal requirements for privacy and information security and the associated consequences and penalties for non-compliance
- Identify the process for reporting incidents.

You should also be prepared to comply with the ROB.

**Note:** The following personnel are also required to complete the more detailed privacy course, Privacy and HIPAA Training (TMS 10203):

- Employees with access to the Compensation and Pension Records Interchange (CAPRI)
- Veterans Health Administration (VHA) clinician and personnel who have access to VHA systems containing VA sensitive information

---

\*Sources: VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior



## 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.

Initials \_\_\_\_\_

(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:

(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;

Initials \_\_\_\_\_

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.

Initials \_\_\_\_\_

(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.

**Initials** \_\_\_\_\_



(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.

Initials \_\_\_\_\_

(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.

(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.

Initials \_\_\_\_\_

(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.

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.

Initials \_\_\_\_\_

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.

Initials \_\_\_\_\_

(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.

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.

Initials \_\_\_\_\_



### 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

## 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.
- 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.

Initials \_\_\_\_\_

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.

Initials \_\_\_\_\_

- (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.
- (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.

Initials \_\_\_\_\_

(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.

(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.

Initials \_\_\_\_\_



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.**

## 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 or diary that may be personal or topical, in which the author makes regular entries that appear in reverse chronological order and can be read by the general public. Source: Wordsmyth 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 VA information security program. CRISP is a three-pronged approach to improve the way VA looks at information security. First, the program will ensure that those who are on VA systems have the appropriate level of access. Second, the program will establish clear, documented contingency plans for data breaches, which will be regularly tested and improved. Last, the program will launch accessible, tailored, online information security training for all VA employees, volunteers, contractors, and affiliates. Source: Office of Information Technology, CRISP Strategic Communication Plan

**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**—Hides text in secret code. Encryption is the cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. Source: WC3 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 Security Management Act (FISMA)**—A law that requires VA to have an information security program. FISMA requires federal agencies to have a program to assess risk and protect information and information system assets that support agency operations. Specifically, FISMA requires federal departments and agencies to maintain an inventory of information systems, perform periodic system risk assessments, implement policies and procedures to reduce risk to an acceptable level, periodically test and evaluate information security controls, provide appropriate information security training to employees and contractors, implement plans and procedures for security incident response and continuity of operations, and report annually on information security status. Source:

<http://www.fisma1.net/whatisFISMA.shtml>

**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>

**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 give 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

N/A—Not Applicable

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](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 Administrative 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/>

## I

**Incident**—A situation that potentially or actually puts VA information at risk. There are two types of incidents – security incidents and privacy incidents.

Security incidents occur when there is a potential or actual breach in Department security procedures, but VA data has not been accessed or compromised. Examples include 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. Security incidents are investigated by the ISOs and the NSOC.

Privacy incidents occur when there is an actual or potential unauthorized access to or disclosure of PII in electronic, print, or any other format. They may or may not also involve a security incident or multiple security incidents. Privacy incidents are investigated by the ISO and the Privacy Officer.

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 you 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**—Knowledge or facts owned by VA. Internal Business information is information intended for use by employees when conducting the daily operation of VA business. Source: VA Handbook 6500

J

N/A

K

N/A

L

N/A

M

**Macerating**—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 VA 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 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 e-mail, contacts, and other features. With Outlook You can view a day, week, or month at once. Source: Microsoft

**Microsoft SharePoint**—Software used to store documents on an Intranet site. Use Microsoft SharePoint to set up collaborative sites to share information with others, manage documents from start to finish, and publish reports to help everyone make better 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. Every individual article or grouping of mail, however sent, 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 Logbooks for Personal Use**—A written record of information for a person's own use. A non-electronic record intended to track information for someone's personal use. Paper logbooks for personal use include any written (not electronic) 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. Any instance of an individual maintaining a physical logbook which contains or refers to patient or employee SPI or other VA protected data is considered a breach of security. Individuals are prohibited from compiling historical documentation containing SPI which is not in direct relation to their duties. Under no circumstances should personal copies of logbooks containing SPI be maintained. 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

**Peer-to-Peer (P2P) File Sharing**—Software that allows users to share files over the Internet. P2P File Sharing is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster, Gnutella, and Kazaa are examples of this kind of peer-to-peer software. Source: Network Dictionary

**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)**—Facts or data you can use to identify a person. PII is any information which 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.

Source: VA Handbook 6500.2

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

**Privacy Act of 1974**—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 absent 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>

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



**Prohibited Activities**—Using VA-issued devices for inappropriate doings. 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)**—Facts or data about a person’s health status. PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Source: VA Handbook 6500.2

**Public Key Infrastructure (PKI) Encryption**—VA-approved software that hides text in secret code. PKI encryption is VA-approved software that is used to secure the delivery of electronic services to VA employees, contractors, and business partners. PKI encryption is part of an overall security strategy 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**—Formal written facts about a person or VA. Records are defined differently in the Privacy Act and the Federal Records Act. Both definitions must be considered in handling VA records.

Records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them. Source: Federal Records Act (44 U.S.C. 3301)

“Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. Source: Privacy Act

**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 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

**Records Custodian**—A person who is responsible for managing VA records. A records custodian, who is also known as a records officer, is a person designated responsibility for managing and coordinating a records management program for his or her respective organization. This includes Central Office program offices and respective field facilities that fall under the officer’s purview. This officer works in cooperation with the VA Records Officer. 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

**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 agree by signature to adhere to the VA National ROB before they are granted access to VA information systems. Source: VA Handbook 6500

### S

**Social Engineering**—To get someone to break security rules. Social engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Source: NIST SP 800-61

**Social Media**—Web and mobile-based tools that allows 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. These media do not include email. Source: VA Directive 6515

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

**System of Records**—A file of personal data documented by VA. A system of records is a file, database, or program from which personal information is retrieved by name or other personal identifier. The Privacy Act provides a number of protections for your personal information. These typically include how information is collected, used, disclosed, stored, and disposed. Source:  
[http://www.rms.oit.va.gov/system\\_of\\_records.asp](http://www.rms.oit.va.gov/system_of_records.asp)

T

**Tweets**—Brief messages sent through Twitter. Tweets are small bursts of information called Tweets. Each Tweet is 140 characters long, but don't let the small size fool you—you can discover a lot in a little space. You can 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 you to the latest stories, ideas, opinions and news about what you find interesting. Simply find the accounts you find most compelling and follow the conversations. Source: Twitter

U

N/A

V

**VA Confidentiality Statutes (Title 38 U.S.C. 5701, 5705, and 7332)**—Statutes requiring VA to keep medical claims, information, and health records private.

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

**VA Sensitive Information**—VA sensitive information is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions, such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Source: VA Handbook 6500



**Virtual Private Network (VPN)**—A private “tunnel” through a public network (i.e., the Internet). A VPN is a logical network that is established, at the application layer of the OSI model, over an existing physical network and typically does not include every node present on the physical network. Authorized users are granted access to the logical network. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. Source: VA Handbook 6500

## W

**Wireless Network**—A network of computers that are not connected by cables. Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber optic cabling between network devices. Source: <http://compnetworking.about.com/cs/wireless/f/whatiswireless.htm>

## 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

## APPENDIX D: Privacy and Information Security Resources

Table 1. VA Phone Numbers

Table 2. VA Web Links

Table 3. VA TMS Courses

Table 4. Privacy Laws and Regulations

Table 5. Information Security Laws, Regulations, and Related Statutes/Specifications

Table 6. Selected VA Privacy Handbooks and Directives

Table 7. Additional Selected VA Handbooks and Directives

### Table 1. VA Phone Numbers

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

(800) 488-8244

**VA IT Helpdesk** (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\***

<http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/default.aspx>

**Locator to Identify ISOs and POs\***

<https://vaww.infoprotection.va.gov/index.aspx>

**PIV Cards**

<http://www.va.gov/PIVPROJECT/index.asp>

**Role Definitions PDF Document\***

<http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Shared%20Documents/Role%20Definitions.pdf>

\*These links are only accessible on the VA Intranet

**Table 3. VA TMS Courses**

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

TMS ID 10203, Privacy and HIPAA Training

TMS ID 1049914, Role Based Records Management Training for VA Personnel

TMS ID 1256927, Getting Started with Public Key Infrastructure

TMS ID 2626967, Social Networking and Security Awareness

**Table 4. Privacy Laws and Regulations**

Available at: [http://www.privacy.va.gov/privacy\\_resources.asp](http://www.privacy.va.gov/privacy_resources.asp)

**Freedom of Information Act (FOIA)**

Requires federal agencies to disclose records requested in writing by any person subject to certain exemptions and exclusions.

**Health Information Technology for Economic and Clinical Health Act (HITECH)**

Describes when and how hospitals and 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 5. Information Security Laws, Regulations, and Related Statutes/Specifications

#### Federal Information Security Management Act (FISMA)

[http://www.dhs.gov/files/programs/gc\\_1281971047761.shtm](http://www.dhs.gov/files/programs/gc_1281971047761.shtm)

Requires federal agencies to have a program to assess risk and protect information and information security assets that support agency operations.

#### Federal Records Act

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

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.

#### Internal Revenue Code (IRC) Specifications

**IRC at 26 U.S.C.A. § 6103 (p)(4).**

[http://www.patentofficelawsuit.info/irs\\_6103.htm](http://www.patentofficelawsuit.info/irs_6103.htm)

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.

**IRC at 26 U.S.C.A. §§ 7213, 7431.**

[http://www.patentofficelawsuit.info/irs\\_7431.htm](http://www.patentofficelawsuit.info/irs_7431.htm)

Describes penalties for disclosing tax return information without permission from the individual.

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

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

<http://us-code.vlex.com/vid/sec-confidential-nature-claims-19233871>

Information about any claims processed by VA must be kept confidential

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

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

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

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

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

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

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

Available at: <http://www1.va.gov/vapubs/index.cfm>

VA Directive 6066, Protected Health Information (PHI)

VA Directive 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

VA Handbook 6300.6/1, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses

VA Handbook 6500, Information Security Program and Appendix D, VA National Rules of Behavior



VA Handbook 6500.1, Electronic Media Sanitization
VA Handbook 6500.2, Management of Security and Privacy Incidents
VA Handbook 6502, VA Enterprise Privacy Program
VA Handbook 6502.4, Privacy Act Review
VA Handbook 6512, Secure Wireless Technology
VA Handbook 6609, Mailing of Personally Identifiable and VA Sensitive Information
VHA Directive 1605, VHA Privacy Program
VHA Handbook 1605.1, Privacy and Release of Information
VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information

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

Available at: <a href="http://www1.va.gov/vapubs/index.cfm">http://www1.va.gov/vapubs/index.cfm</a>
VA Directive 0701, Office of Inspector General Hotline Complaint Referrals
VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program
VA Directive 6515, Use of Web-Based Collaboration Technologies
VA Handbook 5011/5, Hours of Duty and Leave
VA Handbook 5021.3, Employee/Management Relations
VA Handbook 5021.6, Employee/Management Relations, Appendix A
VA Handbook 6300.1, Records Management Procedures
VA Handbook 6500, Appendix F, VA Password Management
VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior