It's in Your Hands

VA Privacy and Information Security Awareness and Rules of Behavior

FY14 Text-Only Course Transcript

Table of Contents

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) 2014 (i.e., October 1, 2013 through September 30, 2014).

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

Module 1: Welcome and Introduction

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

Why Am I Taking this Course?

Many laws require VA staff to take privacy and information security training. If you use and have access to VA information systems or VA sensitive information, VA requires you to take this course so you know what to do to keep information safe and help VA comply with these laws.

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

Note: Veterans Health Administration (VHA) and Veterans Benefit Administration (VBA) employees and contractors who have access to Protected Health Information (PHI) are also required to complete Privacy and Health Insurance Portability and Accountability (HIPAA) Training (VA TMS ID: 10203)

Who Must Take this Course?

All VA employees must take this training, including:

- Paid employees
- Volunteers
- Unpaid employees
- Students or other trainees.

Note: If you are a medical trainee (i.e., student, intern, resident, or fellow), VA does not require you to complete this course, but you must complete the course VHA Mandatory Training for Trainees (VA TMS ID: 3185966).

Contractors working for VA must also take this training if their contract states that it requires the training.

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

- 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).

Applicable ROB

Employee: 1b, 2h(1)

Contractor: 1a, 1g, 2b(18)

You can find more information about these items in Appendix D: Privacy and Information Security Resources.

Rules of Behavior (ROB)

The VA National Rules of Behavior (ROB)[1] describe what everyone MUST do to protect privacy and keep information safe. Some offices or facilities require even more . protection. Always follow the ROB and your local rules.

Applicable ROB

Employee: 1j, 2a(2), 2a(3)

Contractor: 2a, 3d

In order to use and have access to VA information systems or VA sensitive information you must take this course and acknowledge and accept the ROB every year. There are two versions of the ROB—one for VA employees and one for contractors.

Employee ROB:

Employees must complete this training and acknowledge and accept the ROB to gain or maintain access to VA information systems or VA sensitive information. You may find the full version of the VA Employee Rules of Behavior in Appendix A. When you finish

[1] Sources: VA Handbook 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program and Appendix D, VA National Rules of Behavior; VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior.

reviewing this text-only course document, you should sign and submit the hard copy of the Employee ROB document to your supervisor.

Contractor ROB:

Contractors must complete this training if their contract language requires it and must acknowledge and accept the ROB to gain or maintain access to VA information systems or VA sensitive information. You may find the full version of the VA Contractor Rules of Behavior in Appendix B. When you finish reviewing this text-only course document, you should sign and submit the hard copy of the Employee ROB document to your COR.

Course Objectives

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

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

Module 2: Overview of Privacy and Information Security

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

Module Objectives

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

- Describe your legal responsibilities to protect privacy and ensure information security
- Recall the types of information that are considered sensitive
- Explain basic ways to protect sensitive information.

Protecting Privacy and Information Security

You have a responsibility to protect privacy and ensure information security. Remember, whether the information you work with is stored on paper or in digital form, keep it safe! You must protect all types of VA sensitive information when you:

- Talk with others
- Handle paper records or electronic files
- Use email and other types of electronic communication
- Use electronic devices
- Store, transport, and dispose of information in all formats.

Applicable ROB

Employee: 1a, 2b(13)

Contractor: 2b(14)

You are legally required to uphold these responsibilities and follow the law. You are also required to report any incidents whenever you see these requirements not being followed. If you do not, you may lose your job, have to pay fines, or face prison. Complying with the ROB will make sure you are following the law.

It's in Your Hands Scenario: Privacy and Information Security at VA

At VA, we need everyone to take privacy and information security incidents seriously. Everyday situations may seem harmless, but ordinary mistakes can put VA sensitive information—and Veterans—at great risk.

Watch for "It's in Your Hands" scenarios throughout the course to read stories about VA's most commonly reported incidents. These are ordinary situations that could happen to anyone and could cause you and others great harm if you make the wrong choice. The "Best Choices" tips in these stories remind you what to do to meet the challenge and prevent these all-too-common incidents.

Protecting VA and Veterans—every day—is in **your** hands.

Privacy: What to Protect

To protect privacy, you must protect VA sensitive information that belongs to Veterans, their families, VA employees, and VA. Privacy may be violated on purpose or by accident. To protect privacy, do not disclose, alter, or destroy VA sensitive information unless you have permission.

VA sensitive information includes:

- Personally Identifiable Information (PII), also sometimes called Sensitive Personal Information (SPI)
    - PII or SPI refers to private information about a specific person that can identify a person, such as:
        - Name, address, and phone number
        - Social Security number (including the last four digits)
        - Date of birth
        - Credit card numbers
        - Education records
        - Financial records
        - Criminal and employment histories

- Protected Health Information (PHI)
    - Protected Health Information (PHI) is a type of PII that includes health records or payment information linked to a specific person that may disclose a person's medical condition or history, such as:
        - Patient medical record
        - Patient diagnosis
        - Patient test results
        - Patient payment history
- Internal Business Information (IBI)
    - Sensitive information that VA uses internally that is not meant to be communicated outside of VA is called Internal Business Information, or IBI. You may also hear this referred to as proprietary information. IBI is not public knowledge, and enables VA to meet its mission. Some examples include:
        - Pricing information submitted to VA by vendors during bid processes
        - Facility or computer room diagrams
        - Documentation of IT systems
        - Operational business and information reports.

Knowledge Check: Types of VA Sensitive Information

It's important to know what information is considered sensitive. Review each type of specific information, and determine what kind of VA sensitive information it is.

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

- Blueprints of Hospital Floor Plans (The correct answer is IBI)
- Name (The correct answer is PII)
- Medical Diagnosis (The correct answer is PHI)
- Medical Records (The correct answer is PHI)
- Social Security Number (The correct answer is PII)
- Pricing Information Submitted to VA by Vendors (The correct answer is IBI)
- Birth Date (The correct answer is PII)
- Documentation of IT Systems (e.g., IP Addresses) (The correct answer is IBI)

Information Security: How to Protect It

Information security includes ways of safeguarding VA's information systems and VA sensitive information from unauthorized access or modification to ensure its confidentiality, integrity, and availability. Be sure you know how to maintain confidentiality, integrity, and availability to keep VA sensitive information safe.

Applicable ROB

Employee: 1c

Contractor: 2b(7), 2b(13), 2b(17)

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

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

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

Protecting VA Sensitive Information

When you see VA sensitive information, do you know what to do to protect it? Be sure you understand VA's information security and privacy policies and procedures, and always follow the Rules of Behavior—wherever you are working.

Keep these tips in mind:

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

Knowledge Check: Protecting Privacy and Information Security

It's important for you to know where to find all the information you need to keep VA sensitive information safe. Answer the question by selecting the correct document.

Answer the following question by selecting the best answer.

It is your responsibility to keep VA sensitive information safe. What document provides all the information you must follow to protect VA sensitive information?

A. VA Employee Handbook
B. VA National Rules of Behavior
C. OPM Values and Ethics Guidebook
D. NIST Information Security Handbook

Answer B is correct. VA National Rules of Behavior and the Contractor Rules of Behavior provide all the rules you must follow to protect VA sensitive information.

Who Can Provide Support?

You can always reach out for help with your questions or concerns about privacy and security.

Your supervisor or CO/COR, Privacy Officer (PO), and ISO can help you comply with all regulations.

Supervisor

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

- Ensuring staff understand IT security and information protection issues
- Ensuring staff comply with security regulations and policies
- Ensuring staff only have access within their scope of duties
- Verifying staff complete all privacy and information security training requirements
- Ensuring staff sign the ROB each year
- Helping staff report suspected incidents.

CO/COR

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

- Ensuring contractors sign the Contractor ROB each year

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

PO

PO responsibilities include, but are not limited to:

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

See Appendix D: Privacy and Information Security Resources to learn more about how to identify your PO.

ISO

ISO responsibilities include, but are not limited to:

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

Applicable ROB

Employee: 2a(2), 2c(1), 2h(2)

Contractor: 1h

See Appendix D: Privacy and Information Security Resources to learn more about how to identify your ISO.

The Continuous Readiness in Information Security Program

VA's Continuous Readiness in Information Security Program (CRISP) highlights what each of us can do to protect VA sensitive information. CRISP is a program that incorporates security and privacy into everyone's everyday functions and provides ongoing security and privacy practices for VA's environment.

To learn more about CRISP, refer to Appendix D: Privacy and Information Security Resources.

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

Protecting all types of VA sensitive information is important. Read each scenario and determine if the sensitive information being described is secure or at risk.

Select "secure" or "at risk" for each of these three scenarios.

Scenario 1 of 3:

"I wonder if I should shred these records—some of these are really old. If nobody has wanted them in the past year, I may as well shred them." *Secure or at risk?*

The correct answer is "at risk." Some paper files may be records, which may not be destroyed until the legally assigned disposition has been reached. Be sure to check with the Records Management Officer. Follow all information security and privacy policies and procedures and the ROB when handling VA sensitive information—both paper and electronic.

Scenario 2 of 3:

"I need to get this patient payment spreadsheet to Lisa right away, but the file is acting so funny. It keeps putting odd characters into the spreadsheet. I wonder if I have a virus, but I just don't have time to deal with that right now. I'm sure it's fine." *Secure or at risk?*

The correct answer is "at risk." Any time you suspect you have a virus, report it. If you don't, the integrity of your information could be at risk.

Scenario 3 of 3:

"Janet, my father is a patient here and I have some questions about his upcoming surgery. Can you help me with that?"

"Since I'm not involved with your father's care, I'm not allowed to access his information, but I'll see if his nurse is available to talk with you." *Secure or at risk?*

The correct answer is "secure." Confidentiality of information is preserved when you view, access, and collect only the information you need to do your job.

It's in Your Hands – Module Summary

Now that you've finished this module, you are aware of your role in protecting VA sensitive information.

Let's recap the key points of this module:

- Always follow privacy and information security policies and procedures
- Always view, access, and collect only the minimal information you need to do your job
- Share VA sensitive information with only those persons who have a need to know in the performance of their official government duties
- Protect VA sensitive information in all forms and all environments.

Module 3: Private Conversations and Paper Records and Files

Module Objectives

Privacy and information security are in your hands on a daily basis, whether the information is shared in conversation or in writing. 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 finished this module, you will be able to:

- Explain how to protect VA sensitive information during private conversations and when handling paper records and files
- Recognize common mistakes when communicating VA sensitive information
- Choose the correct actions to protect privacy and ensure information security during private conversations and when handling paper records and files.

Private Conversations

We all have conversations at work about sensitive information. It is important that you take care to protect your conversations just as you do private records. When having conversations about sensitive information, follow these guidelines:

- Discuss VA sensitive information in private, such as in a private office
- Close office doors or leave areas where others can overhear
- Lower your voice when others are around
- Avoid talking in public places, such as lobbies or elevators
- Never give VA sensitive information over the phone to someone you do not know and who may not have the legal authority to receive it
- Never leave VA sensitive information on voicemail.

Applicable ROB

Employee: 2b(9)

Contractor: 1g, 2b(10)

It's in Your Hands Scenario: Private Conversations

Situation:
Tom, a local business man, receives treatment at a small VA outpatient clinic. The checkout desk is next to a busy waiting room. As Tom checks out, the receptionist gives him his prescription and says, "Mr. Daniels, here is your prescription for your oral chemotherapy. The radiologist will be calling you later this week to schedule your first radiation treatment."

Impact:
By saying the patient's name and identifying his specific treatments, the receptionist has exposed sensitive information to anyone nearby. The patient may be embarrassed by the disclosure of his treatment information. Even more important, as a business owner in a small community, this disclosure and gossip in the community could affect Tom's personal relationships or his business, and cause him significant financial hardship.

Best Choices—It's in Your Hands:

- Avoid discussing private information when possible.
- Talk with people in private when discussing sensitive information.
- Make sure to keep your voice down if you must be in a public place when discussing sensitive information.

What Are Records?

Records are a special kind of information that require additional care. This information can be paper or electronic. It can include images, audio, video, and other media. The Federal Records Act of 1950 requires federal agencies to make and preserve records. These records document their business activities. These records are public property and must be managed according to the law.

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 kept according to a Records Control Schedule (RCS). The RCS is required by the National Archives and Records Administration (NARA). The RCS is a list of records that have been scheduled by NARA and given a retention and disposition ruling. These rulings are listed in the NARA document known as the General Records Schedule.

Records

Examples of records include:

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

Non-records are those items that usually are not included within the scope of official records, as well as documents not required or included on a records retention schedule.

For more information about records management, refer to the following links found in Table 7 of Appendix D: Privacy and Information Security Resources.

- VA Directive 6300, Records and Information Management
- VA Handbook 6300.1, Records Management Procedures

Applicable ROB

Employee: 2b(8)

Contractor: 2b(14)

Protecting Paper Documents, Records, and Files

Paper documents, records, and files refer to all non-electronic forms of information (e.g., hard copies of workpapers, x-rays, labels, microfiche). To prevent unauthorized disclosure, each type of document must be handled in a certain way. Select each type of document to learn what to do to protect VA sensitive information.

Paper Files

Follow these best practices to protect paper files:

- Do not leave files out in areas such as public spaces, private offices, conference rooms, copy or fax machines, mailboxes, or wall trays.
- Lock files and documents when you are not in your work area.

- Always get written permission from your supervisor before you remove sensitive information from VA locations.
- Get approval from your supervisor before transporting sensitive documents.
- Always transport sensitive documents in secure containers or briefcases.

Paper Records

Some paper files may include records identified in the RCS. Always follow procedures whenever transporting paper records that contain sensitive information. Records must be kept according to the RCS and must be retained or disposed of properly. Ask your supervisor or refer to VA Directive and Handbook series 6300 for more information about proper handling of paper records.

- Always ask your supervisor or office records administrator for guidance before you dispose of or destroy any material that may be a record.
- When moving paper records to temporary or permanent storage, sort items into sensitive information records and non-sensitive information records.
- Before sending paper records to anyone, place a cover sheet indicating sensitive information on top of any sensitive records. Refer to VA Directive 6609 for instructions on mailing SPI.

Applicable ROB

Employee: 2a(2), 2b(12)

Faxes

Fill out a cover sheet and list the following four items:

- Recipient's name
- Your name and contact information
- Instructions for the recipient to verify fax receipt
- The confidentiality statement identified in VA Handbook 6500, Information Security Program Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program (the link to this document may be found in the Privacy and Information Security Resources document on the Resources page).

Inter-Office Mail

- Place documents in closed inter-office envelopes. For added safety, put VA documents with sensitive information 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.
- Distribute inter-office mail to the correct addresses right away.
- Transport sensitive documents in secure containers or briefcases.

Regular 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 sealed securely.
- Make sure mass-produced letters and mail merges that contain VA sensitive information are sealed prior to delivery to the approved shipping service.
- Check the recipient name and mailing address.
- Confirm that mailing labels and window envelopes only show the recipient's name and address and no other information.
- Send original documents and all media that contain VA sensitive information through a shipping service with tracking capabilities, such as UPS or FedEx.
- Send copies of documents containing VA sensitive information through the United States Postal Service.

It's in Your Hands Scenario: Paper Documents

Situation:
Patricia is a physician at a VA medical center and has printed some patient files to review while she's eating lunch in the cafeteria. When her friend Hank joins her, she moves the papers to the chair next to her and forgets them. Later, she returns to the cafeteria to collect them and learns a cafeteria worker found them and threw them in the garbage.

Impact:
Nearly 80% of incidents reported to VA's Incident Response team are paper-related. The most common incident is mishandled paper—leaving it where it doesn't belong. Whether the patient information in this story ends up in the wrong hands, or simply a landfill, the privacy of several Veterans has been compromised. The information included personally-identifiable information (PII) and protected health information (PHI), which will require VA to provide one year of credit monitoring for the affected patients.

Best Choices—It's in Your Hands:

- Always be very careful not to leave papers with sensitive information in public spaces. If you must transport them, transport them in secure containers or briefcases.
- If you find papers that contain sensitive information, be sure to report it as an incident.

Knowledge Check: Mailing PHI or PII Correctly

It's important for you to know which documents must be tracked when they are mailed. Answer the following question by selecting True or False.

Original documents and media that contain VA sensitive information must be mailed through a shipping service with tracking capabilities, such as UPS or FedEx.

A. True
B. False

The correct answer is True. Original or hard-to-replace documents and media that contain VA sensitive information must be mailed through a shipping service with tracking capabilities. Copies containing sensitive information may be mailed through the US Mail.

Log Books

Log books are helpful in conducting VA business. However, they must be used safely. Keep log books with VA sensitive information in electronic files on authorized VA systems. If your job requires you to maintain a log book, use an electronic log book if at all possible.

Paper log books create a high risk of violating privacy because they can be lost or stolen. VA does not allow the use of paper log books for personal use. This includes the use of paper log books in clinics and medical centers.

To maintain a paper log book, you must have an important business need. In this case, you must have it approved by the Facility or Program Director.

If there is a business need or legal requirement for the use of a paper log book, you **must** get approval. Physical (paper) log books must be approved by the Facility Director as required by local policy and approval processes. Supervisors, Service Chiefs, or other responsible parties must confirm the business requirement, location, and content.

Note: Log books have the potential to be records. If your log book is considered a record, and has been reviewed by NARA, you must follow NARA's applicable retention and disposition rulings.

It's in Your Hands Scenario: Paper Log Books

Situation:
James is a medical resident. He keeps a paper log book to track his patients' data, including names, Social Security numbers, and diagnoses. He believes it's easier and safer than carrying a laptop everywhere. He keeps it with him at all times wherever he goes. One day, James takes the log book with him when he goes to the gym and locks it in the locker inside his duffel bag. After getting out of the pool, James notices his towel with the key he attached to it is gone. He finds someone has stolen his duffel bag containing the log book.

Impact:
Loss and misuse of paper log books represents one of the ten most frequently reported incidents across VA and has the potential to expose Veterans to public disclosure of their private information. Because this log book contained dozens of Veterans' sensitive information, all of the Veterans will have to be offered credit protection for one year.

Best Choices—It's in Your Hands:

- Track patient data in an electronic format that can be encrypted, if at all possible.
- If you have permission to use a paper log book, shred the information in an approved shredder at the end of each day.

Data Security

- Make sure the information kept in the log is the least amount of sensitive information required.

Physical Security

- Make sure the log is properly protected.
- Make sure the log book is locked up when not in use.

Records Management

- Follow NARA's guidance for retention and disposition if your log book is considered a record.
- Destroy the physical pages according to VA Records Management guidelines.

Disposal

- Keep sign-in rosters in your sight and in their assigned area of use, and shred them using a VA-approved shredder at the end of each business day.

Applicable ROB

Employee: 2b(6)

Additional Guidance

- Follow your organization's specific guidance regarding written log books.

Decision Exercise: Paper Log Books

Paper log books are a significant risk for VA because they can hold large amounts of VA sensitive information and are easily lost or stolen. Paper log books are prohibited from personal use, but sometimes there is a compelling business need. If you do need to keep information in a log book, there are certain rules you must follow. See the process below to gain authorization for use of paper log books and to see the rules you must follow when working with them.

Do you have a compelling business need to use a paper log book?		
Yes	▪ Have your supervisor, Service Chief, or other responsible party confirm need, location, and content ▪ Get authorization from Facility Director or Program Director ▪ Ensure there are authorizations in place	Are authorizations in place? • **If Yes**, you must follow these rules: ▪ Make sure the information kept in the log is the least amount of sensitive information required ▪ Properly protect the log by placing in a locked drawer when not in use ▪ Destroy physical pages according to VA Records Management guidelines ▪ Keep sign-in rosters in your sight, in their assigned area ▪ Shred sign-in rosters using a VA-approved shredder at the end of each business day ▪ Follow your organization's specific guidance regarding paper log books • **If No**, get authorization from the Facility Director or Program Director
No	▪ Use an electronic alternative instead	

It's in Your Hands – Module Summary

Now that you have finished this module, you know some ways to protect VA sensitive information in paper records and files. You also know how to protect your conversations when discussing VA sensitive information when talking to other people.

Let's recap the key points of this module:

- Be aware of your surroundings and keep conversations private.
- Never discuss VA sensitive information in public places in person or by phone.
- Protect paper files and prevent unauthorized disclosure when sending faxes, inter-office mail, and regular mail.
- Do not keep unauthorized paper log books.

Module 4: Privacy in Electronic Communications

Module Objectives

Privacy and information security must be maintained in every electronic communications format you use on a daily basis. Making sure VA's sensitive information in electronic formats is safe is in your hands. In this module, you'll learn how to protect VA sensitive information in electronic communications.

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

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

Email Encryption

Email messages can expose private information. Emailed information is safer if it is encrypted. VA uses public key infrastructure (PKI) encryption and Rights Management Service (RMS) encryption to keep email with sensitive information safe. You must use PKI or RMS to encrypt all emails that contain sensitive information. While VA-issued workstations have the capability to encrypt email through Microsoft Outlook, mobile devices, such as Blackberries, must have an encryption certificate installed, which allows the device to encrypt emails. Contact the VA National Service Desk for any PKI or RMS questions.

Applicable ROB

Employee: 2b(10), 2b(11)

Contractor: 2b(12)

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

- **PKI S/MIME Encryption**—Refer to TMS course 1256927, Getting Started with Public Key Infrastructure to learn more about PKI encryption.
- **RMS Encryption**—Refer to TMS course 336914, An Introduction to Rights Management Service – RMS, to learn more about how to use RMS.
- **Digital Signature**—A digital signature helps you add another level of security to your email messages. This helps the email recipient verify the authenticity and integrity of messages that you send.

PKI

S/MIME (PKI) encryption prevents information in email messages and email attachments from being read by people who are not authorized. S/MIME (PKI) also provides authentication of the sender if the message is signed.

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

RMS

RMS protects the content of email messages and other Microsoft Office documents. RMS provides additional controls that PKI does not. RMS can prevent forwarding, copying, and Microsoft-provided screen captures of RMS-protected content. RMS can only be used for encrypting messages and documents sent within VA until the next version of RMS is enabled in VA.

To determine whether you need to use PKI or RMS encryption, ask yourself if the information you are sending contains sensitive information. If it does, you must use PKI or RMS encryption. If you want that protection to persistently protect the information along with other controls, then use RMS instead of PKI. If you have questions about how to use PKI or RMS, you can search for additional training in TMS or contact your supervisor.

It's in Your Hands Scenario: Email Encryption

Situation:
A busy Veterans Benefits Administration (VBA) human resources supervisor sends an unencrypted email containing a spreadsheet with the full names and benefits information for 165 Veterans to her coworker. When she types in the recipient name, it auto-populates the "To" field with the wrong name and the file goes to an outside industry colleague. Because the file is unencrypted, this information is exposed to someone who should not see it.

Impact:
Because the information was disclosed to someone outside of VA who had no need to access this information, the result is that all 165 Veterans listed in the spreadsheet must be notified and credit monitoring offers must be sent to them—a very big deal for a seemingly small mistake. In addition to the loss of Veterans' and the public's trust, VA could possibly pay much more in legal fees and damages if the incident results in a lawsuit.

Best Choices—It's in Your Hands:

- Always double check email addresses when sending sensitive information.
- Always encrypt emails when sensitive information is included in the email or as an attachment.

Secure Email Practices

Email provides a quick and easy way to transmit information. However, you must be careful to protect privacy when using email. Always follow these guidelines when sending emails that contain sensitive information:

- Use RMS or PKI to make sure emails are encrypted.
- Ensure there is no sensitive information in the subject line of an email.
- Include your name and phone number in the email.
- Confirm all individuals on the distribution list are approved to receive the information.
- Consider the audience carefully before replying all to an email.
- Delete unnecessary emails and attachments containing VA sensitive information as soon as possible.
- Save emails and attachments that may be official records.
- Ensure the auto forward feature to addresses outside VA's network is turned off.

Applicable ROB

Contractor: 2b(12)

Knowledge Check: Sending Emails with VA Sensitive Information

Review the three emails and determine if each email should be encrypted. Select encrypt or don't encrypt for each email.

Email 1 of 3

To: Joe
Subject: Phone System

Hey Joe,
I have a quick question for you on the new phone system. Can you tell me how to take three separate phone lines and conference them together? I couldn't find it in the manual (PDF attached). Give me a call if you want to talk me through it.
Tom

Tom Howell, CISSP
Office Hours: 7:00AM–4:30PM Eastern Time

Don't encrypt is the correct answer for email 1. This email does not have VA sensitive information. You do not need to encrypt this email.

Email 2 of 3

To: Janie
Subject: Patient endoscopy

Janie,
George Walland needs to schedule an endoscopy for next week if possible. Below is his information to make the appointment. Please confirm the appointment with me upon scheduling.

George Walland
DOB: 09-08-1948

Thank you.
Theresa Fannelli, R.N.

Encrypt is the correct answer for email 2. This email has VA sensitive information. You should encrypt this email.

Email 3 of 3

To: Amy
Subject: Request Claim
Attached: robert_berenson_claim.doc

Amy,
Attached is the 12/2/2012 benefits claim for Robert Berenson, as requested. If you have any questions, please let me know.

Jan Cooper
Department of Veterans Affairs
Email: janet.cooper@va.gov

Encrypt is the correct answer for email 3. This email has VA sensitive information. You should encrypt this email.

Instant Messaging and Texting

Instant messaging and texting are easy ways to share information quickly, but you must be careful! Follow VA rules when sending these types of messages to minimize risk.

Instant Messages

VA recently implemented a secure instant message (IM) system within VA's network. VA allows you to access and use Microsoft Lync as a secure, encrypted way to exchange VA sensitive information.

Note that Microsoft Lync may not be available for many of the mobile devices that are coming online.

Note: IMs saved in Microsoft Outlook are not encrypted, so make sure that Microsoft Outlook does not save these IMs in your conversation history. Contact the VA National Service Desk for assistance if needed.

Text Messages

Never use your mobile phone's text messaging feature to send VA sensitive information. All VA sensitive information must be encrypted during transmissions. Because text messaging does not guarantee proper encryption, do not use text messaging to transmit VA sensitive information. Sending VA sensitive information in an unencrypted text message can put VA at risk.

Applicable ROB

Employee: 2a(1), 2b(4), 2g(6)

Contractor: 2b(1), 2b(2)

Electronic Calendars

Never include VA sensitive information when using electronic calendars.

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

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

Microsoft SharePoint

VA has approved Microsoft SharePoint for you to access and use for online data storage and collaboration. SharePoint is found on VA's intranet.

Your ISO, Chief Information Officer (CIO), and PO can help you determine which types of information can be shared on specific SharePoint sites. Here are some tips to protect VA information on SharePoint:

- Share VA information only on sites where access is limited to individuals approved to access the information.
- Get access to only the sites you need to do your job.
- Share only the information your work unit needs to share to do its job.

Applicable ROB

Employee: 2b(7) 2b(13), 2g(2)

Knowledge Check: Posting Files on SharePoint

It's important for you to know how to protect information when posting it on SharePoint. Select the best answer to protect VA information.

Answer the following question by selecting the best answer.

What should you do to protect information on SharePoint?

A. Share VA information only on sites where access is limited to individuals approved to access the information
B. Get access to only the sites you need to do your job
C. Share only the information your department needs to share to do its job
D. All of the above

Answer D is correct. When using SharePoint, you should share VA information only on sites where access is limited to individuals approved to access the information, get access to only the sites you need to do your job, and share only the information your department needs to share to do its job.

Using Social Media

VA supports the access and use of approved 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 access and use these tools, be aware that they can be open to attacks, including phishing and social engineering.

Follow these tips:

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

Applicable ROB
Employee: 2h(3)

Knowledge Check: Calendars

It's important for you to understand how to protect VA sensitive information when using electronic communication tools. Answer the following question by selecting the best answer.

When scheduling appointments on your electronic calendars, which statement is true?

A. Never enter VA sensitive information on your electronic calendar
B. Encrypt your calendar information to ensure VA sensitive information stays safe
C. Use Google's calendar to schedule appointments if you are using a VA-issued iPad

Answer A is correct. Never enter VA sensitive information on your electronic calendar.

It's in Your Hands – Module Summary

Now that you've finished this module, you know the actions you can take to protect VA sensitive information in electronic communications.

Let’s recap the key points of this module:

- Use VA-issued devices that are encrypted and password protected.
- Be aware of the risks and guidelines for using social networking and collaboration tools.
- Be aware of common threats to VA-issued mobile devices.
- Never send VA sensitive information in the subject line of any email.
- Never post VA sensitive information on unsecured shared or Outlook calendars or on social networking sites.

Module 5: Protecting Electronic Devices

Module Objectives

Electronic devices that are used for VA business must be protected, and it's up to you to protect them—it's in your hands.

In this module, you'll learn how to protect VA electronic devices. You'll also learn about VA's policy for teleworking, remote access, and use of personal equipment.

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

- Recall VA policy regarding the use of personal equipment
- Explain how to protect VA electronic devices from attacks that can damage equipment, systems, software, and networks
- Recall procedures for accessing VA networks when working remotely
- Recognize common mistakes when using VA electronic devices
- Choose the correct actions to protect privacy and ensure information security when using VA electronic devices.

VA Electronic Devices

Protect your VA electronic devices from loss, theft, and misuse.

VA employees, contractors, and volunteers use VA electronic devices to support their work. Some of these devices include desktop computers, laptops, Blackberry devices, USB drives, biomedical equipment, and copy machines. Note that VA issued laptops must have full disk encryption installed and it must be operational.

Applicable ROB

Employee: 2b(16), 2f(4), 2f(5), 2h(4)

Contractor: 2b(14), 2b(16)

Here is what you need to remember to do to keep these devices secure:

- Take care of the devices that are assigned to you—you are responsible for the care, use, and protection of these devices and the information stored on them.
- Keep your devices secured—protect them from loss, theft, damage, and misuse.
- Agree to periodic electronic device inspections.
- Do not disable VA-approved security tools.

It's in Your Hands Scenario: Protecting VA Electronic Devices

Situation:
Some laptops that run software for medical devices cannot be encrypted. VA needs these devices to treat patients and store patient information. An unencrypted laptop of this type was lost from a VA medical center and compromised the privacy of more than 7,500 Veterans. The loss exposed Veteran names, addresses, ages, medical information, and last four digits of their Social Security numbers.

Impact:
In the case of the lost, unencrypted laptop, a class-action lawsuit was filed by the Veterans. No settlement has yet been made, but a previous class-action lawsuit for a lost laptop cost VA millions of dollars, plus associated legal fees.

Best Choices – It's in Your Hands:

- Use a locking laptop security cable to secure laptop computers wherever they are being used.
- Place electronic devices in locked and secure locations when they are not in use.

Protecting VA Mobile Devices

Criminals can target vulnerable mobile devices. Be sure the mobile devices you use for VA business are secure and that you follow the rules to protect VA sensitive information.

VA supports more than 48,000 mobile devices across the country, and each device can store, process, and transmit information that needs protection at all times. These devices are easy to transport, which adds challenges to ensuring device security. To protect your VA mobile device, always follow VA instructions to keep your security software up-to-date. Use VA-approved encryption and passwords to protect VA mobile devices. For more information about encryption for your VA device, contact your Information Security Officer or the VA National Service Desk.

- **Know the Rules** – Approval is needed from your supervisor before you transport, transmit, access, or use VA sensitive information remotely.
- **Protect Your Information** – Make sure that your mobile device does not contain the only copy of any VA information. That way, if your mobile device is lost, broken, or stolen, your information can be restored.
- **Keep It With You** – Never leave any of your mobile devices unattended. If you are working in an uncontrolled area, use VA-issued cable locks to help keep your computer secure.

Applicable ROB

Employee: 1a, 2b(9), 2b(13)

Contractor: 2b(14)

Be aware, hackers may try to gain full remote access to your devices. Do not click on website links or open attachments sent by unknown senders.

Wireless Devices and Networks

Using wireless devices and networks in public places may put VA sensitive information at risk. It's more difficult to protect VA sensitive information accessed using wireless networks 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. If you must use a wireless connection, be sure to use VA-approved remote access and wireless devices. Never set up unapproved wireless networks in VA facilities.

Wireless Internet Access or Wi-Fi

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

Applicable ROB

Employee: 2b(14), 2d(2), 2g(4)

Contractor: 3a, 3b

To protect your VA device:

- Turn off your device's Wi-Fi capability unless you are working from a secure, password protected network
- Only connect to websites on the Internet using VA's virtual private network (VPN) when you are in airports or other public places (e.g., the library or a coffee shop).

Wireless Telephone Headsets

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

Knowledge Check—Using Mobile Devices

It's important to understand the best practices while you are working remotely with your mobile devices. Read the following scenario and select the correct answer for each of the questions based on the information provided.

Scenario: Today you are working remotely. Unfortunately, there is noisy construction work going on nearby. You decide to go to a coffee shop to work. You take along all of your necessary mobile devices and you are all set to work—or are you?

What are some best practices while you are working remotely with your mobile devices?

- **Device 1**
  Coffee shop Wi-Fi
  The coffee shop says it has a secure, password protected Internet connection. Go ahead and connect to the coffee shop's Wi-Fi, but make sure you are using VA's VPN to connect to any VA websites. *True or False?*

  The correct answer is true. You are allowed to use a secure, password protected public Internet connection. Just make sure to use VA's VPN to access any VA websites. This keeps VA information and systems safe.
- **Device 2**
  VA-issued encrypted Blackberry
  You have your VA-issued encrypted Blackberry with you to take business-related calls and send quick emails to colleagues. However, you should not use your VA-issued encrypted Blackberry to email VA sensitive information. *True or False?*

  The correct answer is false. You are allowed to email VA sensitive information through your VA-issued Blackberry if you have requested and received encryption of your Blackberry.
- **Device 3**
  Personal smart phone
  You have your personal smart phone with you to make personal calls, emails, and texts. You cannot use your personal phone to send text or email messages with VA sensitive information. *True or False?*

  The correct answer is true. You are not allowed to use your phone's texting or email features to send VA sensitive information because VA cannot ensure that appropriate security controls are in place.

Limited Personal Access and Use of VA-Issued Devices

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

- Does not interfere with work
- Does not affect productivity

- Does not violate standards of ethical conduct.

Contractors may not access or use VA-issued devices for personal use unless it is stated in the terms of the contract. No one may access or use VA-issued devices for prohibited activities.

Applicable ROB

Employee: 1d, 2g(7)

Contractor: 1c, 2b(4), 2b(6)

Prohibited activities include, but are not limited to:

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

Personal Identity Verification (PIV) and Identity Cards

VA employees and contractors who have access to VA buildings, networks, and resources are required to carry a Personal Identity Verification (PIV) card. PIV cards are required to increase protection of VA information and information systems. If an employee or contractor departs VA, his or her PIV card must be revoked in the system right away. Make sure to tell your local security office immediately of any staff changes.

Applicable ROB

Employee: 2a(4)

PIV Cards

- A PIV card, which is also known as a PIV badge, is an identification card that complies with Federal Information Processing Standard (FIPS) 201 and related guidance.
- A PIV card contains a photograph and stored identity information so that the identity of the cardholder can be verified.
- PIV cards are issued to those requiring routine access to VA facilities or information systems.
- PIV cards may be used for encrypting email.
- You can learn more about PIV cards by contacting your local PIV office or security office.

Strong Passwords

Strong passwords are difficult to guess. They help to protect VA sensitive information from unauthorized access. In addition to PIV cards, VA uses strong passwords to protect VA information and information systems. To protect your VA-issued devices and your access to VA sensitive information, you must meet VA's password requirements. Your password must have at least eight characters and have three of the following:

- Uppercase letters
- Lowercase letters
- Numbers (0–9)
- Special characters (such as #, %, @).

Applicable ROB

Employee: 2c(2), 2c(3), 2c(4)

Contractor: 2b(8), 2b(9)

Note: VA's computer systems will not let you set a password that does not comply with these policies.

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

Strong passwords meet VA's minimum password requirements. Examples of strong passwords include SSEufu6&* and TeLrk#@23g. Avoid weak passwords that contain any of the following:

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

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

For more information on passwords, the link to the VA Handbook 6500, Appendix F, VA System Security Controls, can be found in Appendix D: Privacy and Information Security Resources.

Knowledge Check: Strong Passwords

In creating a strong password, you are helping to protect VA sensitive information from unauthorized access. Select the password from the list that is considered a strong and secure password.

A. Password 1
B. Gti456!*
C. 12345678
D. James121068

Answer B is correct. By creating a strong password, you help protect VA sensitive information from unauthorized access.

Social Engineering Attacks

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

Social engineering is when someone takes advantage of your trust by asking you questions that can help them gain unauthorized access to VA systems. They may approach you in person, call you, or email you. Examples of social engineering attacks include:

- Someone asking for your username and password (e.g., in-person, over the phone, or by IM)
- Emails that contain harmful content:
  - Attachments with malicious code
  - Embedded links to malicious websites
- Internet sites with pop-up windows that ask you to re-enter your username and password.

Applicable ROB

Employee: 2g(3)

Threats to Systems, Software, and Networks

Watch out for threats to VA sensitive information stored on VA systems, software, and networks.

VA's information security is in your hands—it is up to you to protect VA information systems from threats such as malware, phishing, and spoofing. These threats can allow others to access and expose VA sensitive information. The VA Network Security

Operations Center (NSOC) monitors all network traffic for unusual or unapproved activities.

- Never download a program or software from the Internet onto your computer. Check with your supervisor, ISO, and your local OIT representative to request any software.
- Never give your password to anyone.

Applicable ROB

Employee: 2f(2)

Contractor: 2b(15)

Malware

Examples of malware include viruses, worms, Trojan horses, and spyware.

Risks:

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

Protection Methods:

- Access and use only VA-approved security software
- Do not open suspicious email attachments or websites
- Do not select links inside pop-ups
- Do not download unapproved software, free trials, etc.

Phishing

Risks:

- Collects VA sensitive information by pretending to be an honest source. For example, you receive a free offer that requires you to select a link, enter your username and password, and answer "a few simple questions."

Protection Methods:

- Right click the suspicious link to display the URL

Note: Phishing links often have one or two characters that are different from the real website. [e.g., www.ebay.webs.com (phishing URL) vs. www.ebay.com (real URL)]

Spoofing

Risks:

- Appears as a link to a real website and takes user to a fake site (e.g., you receive an email that appears as if it came from a known sender, but it is from a spoofer)

Protection Methods:

- Ensure you have VA-approved encryption on your devices.
- Type in the website address instead of selecting links provided.

Note: OIT staff combat spoofing by using filters on all network traffic.

Preventing Attacks

You can help prevent attacks or limit the amount of damage these attacks can cause by following these guidelines:

- Follow any instructions to update your VA-approved security software.
- Avoid strange websites.
- Avoid opening strange emails or attachments.
- Never go around system controls to access VA sensitive information, unless specifically authorized by your local CIO.
- Report anything odd on your computer system to your ISO, such as:
    - Odd characters in documents or email
    - Missing data
    - Sudden increases in spam or unsolicited email
    - Emails with strange attachments.

Applicable ROB

Employee: 1f, 2f(1), 2f(3)

Contractor: 2b(5)

It's in Your Hands Scenario: Protecting Electronic Devices from Malware

Situation:
Bill has a major deadline for an important report, and his computer's virus checker is causing the computer to slow down. He decides to disable the virus checker and run it manually until his schedule eases. After all, it's important to VA that he meets these deadlines.

Impact:
While virus attacks may be relatively rare, sometimes a virus can invade a network automatically through a vulnerability and bring down the entire network. No deadline is worth the potential damage caused by disabling virus protection. A virus can infect millions of computers very quickly and cause extensive damage. In 2009, the estimated total cost of damages due to the Conficker virus was several billion dollars, and the virus continues to mutate and circulate through business and personal computers.

Best Choices—It's in Your Hands:

- Make sure you always keep your virus software enabled.
- Always allow VA automated security updates to run on your computer.

Knowledge Check: Threat Prevention

It's important for you to know how to protect your electronic devices from common threats. Electronic devices can come under attack from several types of threats. Match these types of threats with methods used to prevent them.

Type of Threat:

A. Malware

B. Phishing

C. Spoofing

Threat Prevention Methods

___Right click on the link to display the URL (The correct answer is B: to protect against phishing, right click on the link to display the URL.)

___Do not open suspicious email attachments or visit suspicious websites (The correct answer is A: to protect against malware attacks, do not open suspicious email attachments or visit suspicious websites.)

___Type in the website instead of selecting links provided (The correct answer is C: to protect against spoofing, type in the website instead of selecting links provided.)

Remote Access

If you use any remote, mobile, or personal device to access VA's network, you must connect through VA's VPN. Contact your ISO for information on how to get a VPN account. You must have written permission from your supervisor or COR and local CIO in order to access VA sensitive information remotely. Before you can work from home, you must have an approved and signed telework agreement in place.

Remote, mobile, or personal devices include any portable devices that can store information (e.g., laptop computers, cell phones, digital cameras, audio recorders.) You must follow VA's national and local security policies, procedures, and configuration standards before being allowed access to any VA network.

Applicable ROB

Employee: 2d(1), 2d(3), 2d(5), 2d(6)

Contractor: 3c

When accessing VA's network remotely, always:

- Connect via VA's VPN
- Follow remote access procedures
- Let your supervisor and ISO know when you no longer need remote access.

RESCUE

Remote Enterprise Security Compliance Update Environment (RESCUE) provides VA VPN access on VA-furnished devices. If VA issued you a laptop computer, you would use RESCUE to access VA's network if you are not connected directly in a VA facility.

Citrix Access Gateway

Citrix Access Gateway (CAG) provides VA VPN access for non-VA devices or those devices used by contractors. If you are a VA contractor working on your company's computer equipment at your company's facility, you would access VA's network using CAG.

Personal Electronic Devices

VA, along with other federal agencies, is working on a Bring Your Own Device policy. Until this policy is published, a personal electronic device can only be connected to VA's network at a VA facility with permission from your supervisor, CIO, and ISO.

- Always use VA's VPN to access VA networks from personal electronic devices.
- Never store VA sensitive information on any personal electronic device.
- Never store VA sensitive information on a third party file sharing site (e.g., Google Docs).

Applicable ROB

Employee: 2e(2), 2e(3), 2g(1)

Knowledge Check: Remote Access

It's important for you to know what you need to do to protect VA sensitive information prior to working from home. Answer the following question by selecting the best answer.

You have just had a discussion with your supervisor about working remotely from home every other Friday. What must you do before you can begin to work from home?

A. Have an approved telework agreement
B. Get written permission from your local CIO
C. Request a VA Virtual Private Network account from your ISO
D. All of the above

Answer D is correct. To work remotely, always have an approved telework agreement, get written permission from your supervisor and local CIO, and request a VA Virtual Private Network account from your ISO.

It's in Your Hands – Module Summary

Now that you've completed this module, you know some ways to protect VA-issued devices from attack. You should also be aware of VA's policy for accessing VA's network using remote access.

Let's recap the key points of this module:

- Make sure your devices are encrypted and password protected.
- Create a strong password.
- Never share your passwords with anyone.
- Use VA's VPN when you access VA's network remotely.
- Be aware of possible threats.
- Report any strange activity on your computer system to your ISO.

Module 6: Storage, Transportation, and Disposition of Information

Module Objectives

VA sensitive information must be stored, transported, and disposed of using proper procedures. It's in your hands to protect this information. In this module, you will learn how to store, transport, and dispose of paper and electronic files containing VA sensitive information.

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

- Explain how to protect 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 correct 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 access and use. You must protect information stored on electronic devices. Electronic devices may be lost or stolen, and, without protection, VA sensitive information may be compromised. Sensitive information may also be viewed by others while you are working.

Desktops/Laptops

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

Applicable ROB

Employee: 2g(8)

Contractor: 2b(3), 2b(14)

Mobile Devices (e.g., Blackberry, iPad)

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

Removable Storage Devices

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

Other Devices with Internal Memory

- Store your device in a safe place, if possible.
- Ask Office of Information and Technology (OIT) staff to remove the memory before equipment is replaced or removed from VA's protected environment.

Guidelines for Protecting VA Sensitive Information on VA Devices

Keep VA-issued devices safe from loss or theft. Here are a few ways to protect VA sensitive information stored on your devices:

Applicable ROB

Employee: 2b(1), 2b(5), 2e(1)

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

It's in Your Hands Scenario: Loss or Theft of Sensitive Information

Situation:
Joe is a physician assistant who works between two offices. He carries a VA digital camera to record patient symptoms that are outwardly visible. Each photo is labeled by the patient's last name and Social Security number. While commuting, Joe runs into a local sandwich shop to grab lunch and leaves the camera in the back seat. When he returns, his window has been broken and the camera is gone.

Impact:
Since the camera could not be encrypted, the names and Social Security numbers will be easily accessible by the thief. In addition to the damage to VA's reputation, all Veterans impacted by the loss or theft of their sensitive information must be offered free credit monitoring for one year, which could cost VA a substantial amount.

Best Choices – It's in Your Hands:

- Never leave any VA mobile devices or electronic equipment unattended when traveling between locations.
- Use VA-approved encryption and passwords to protect VA mobile devices and electronic equipment when possible.
- Lock and secure equipment when it's not in use.

Knowledge Check: Protecting Information on VA Devices

Protecting information stored on VA electronic devices is important. Let’s reinforce what you’ve learned. Every VA office must protect VA sensitive information following VA rules and best practices. Can you recall how to protect each of your devices when storing sensitive information?

Computer:

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

Mobile Devices (e.g., Blackberry, iPad):

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

Removable Storage Devices:

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

Applicable ROB
Employee: 2b(3), 2d(5), 2d(7), 2d(8)
Contractor: 2b(10)

Other Devices with Internal Memory:

- Store your device in a safe place, if possible.
- Ask OIT staff to remove the memory before equipment is replaced or removed from VA's protected environment.

Guidelines for Transporting VA Sensitive Information

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

Be careful in airport security lines. The airport security conveyor belt is a common place for laptop theft. Place your computer on the belt only when you are the next in line, and always keep your eyes on it.

Storage and Disposal of Records

Some documents are records. Be sure to store or transport them safely. Every VA facility must inventory its records and have an approved RCS. The RCS states how long records must be kept. A local file plan states the location of records.

- It is illegal to destroy or dispose of records before the disposition date stated in the RCS.
- When records have been kept as long as required, they must be destroyed by one of the approved methods.
- You can be fined or penalized if you do not follow procedures for keeping or destroying records. If the records have VA sensitive information, consequences can be even more severe.

Applicable ROB
Employee: 2b(15)
Contractor: 2b(11), 2b(14)

Consult your Records Management Officer before destroying or moving records to storage.

Guidelines for Disposing of Paper and Electronic Media

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

Paper Files

- Printed forms of VA sensitive information must be destroyed using a VA-approved shredder.
- Documents must be placed in locked shredding bins or containers so the contents may not be removed until ready to be shredded.

Paper Records

- Printed forms or paper copies of VA sensitive information must be destroyed using a VA-approved shredder.
- 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 Management Officer.
- Paper records must not be thrown out in wastebaskets or dumpsters.
- Paper records must be destroyed by shredding, burning, or macerating.

Electronic Media

- All electronic media that contain VA sensitive information must be sanitized or destroyed when it is no longer being used.
- You should ask your ISO for help with the sanitization and disposal or redistribution of media.

Applicable ROB

Employee: 2b(8), 2b(15)

Contractor: 2b(11) 2b(14)

Knowledge Check: Storage and Disposal of Paper Records

It's important for you to know how to dispose of documents that may be considered records. Answer the following question by selecting the best answer.

You are cleaning out your desk and determining what to do with several old documents you have stored. You suspect that some may be considered official records. What should you do?

A. Ask a colleague if he thinks the documents are records
B. Move the documents to official records storage, just to be safe
C. Dispose of them by shredding them with a VA-approved shredder
D. Contact your Records Management Officer before destroying the documents or moving them to storage

Answer D is correct. Always check with your Records Management Officer before destroying or moving any documents that may be records.

It's in Your Hands – Module 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.

Let's recap the key points of this module:

- Protect all VA sensitive information, including paper or electronic media.
- Get written permission from your supervisor to take any VA sensitive information outside of a VA facility.
- Use VA-encrypted electronic devices that have been approved by your ISO and CIO to transport VA sensitive information.
- Keep your items with you at all times, or store your items in a secure location.
- Store, transport, or dispose of records according to VA-approved methods.

Module 7: Reporting Incidents

Module Objectives

When incidents do happen, it's up to you to report them so that the damage can be minimized. It's in your hands. In this module, you'll learn the steps to report incidents. You'll 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 correct 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:

- Improper access of files and records
- Lost or missing paper documents
- Changing or deleting of data without permission
- Unencrypted email with VA sensitive information
- Loss, theft, or destruction of equipment.

Applicable ROB

Employee: 1f, 1g

Contractor: 1h

Remember: Any time you hear or see something that is of concern, report it! All possible incidents should be reported to your supervisor, PO, or ISO immediately.

It's in Your Hands Scenario: Most Frequent Incidents

Situation:
Thousands of privacy and information security incidents are reported each year at VA. It's important for you to report any incidents, regardless of how small they may seem.

VA can track and respond to incidents if they are reported. The most common or greatest impact incidents reported in 2012 included:

- Lost or stolen paper log books
- Malware, viruses, phishing
- Misdirected mail containing VA sensitive information
- Lost or stolen equipment
- Unauthorized disclosure of VA sensitive information
- Unencrypted email containing VA sensitive information
- Unauthorized access to information
- Unattended documents containing VA sensitive information
- Missing or stolen information

You should always report anything you think may be an incident. Protecting VA and Veterans is in **your** hands.

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.

- VA may lose the public's trust and have to notify Veterans that their personal information has been improperly disclosed.
- Breaches involving large numbers of Veterans require reports to Congress.
- Veterans may be harmed by their sensitive information being made public, may experience financial loss, or may become victims of identity theft.
- You could face job loss, fines, and possibly prison if you are the cause of an incident.

Consequences

It makes a difference whether an incident is accidental or intentional. The consequences for intentional acts are more severe than the consequences for accidents. Serious consequences of privacy and information security violations may include:

Applicable ROB

Employee: 1e

- 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.

Penalties

Unfortunately, some people try to access and 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 three years in prison
- Violate the Privacy Act, you can face up to $5,000 and a year in jail per occurrence
- Violate laws protecting PHI, additional penalties may apply.

Violation of federal privacy regulations can incur from $100 up to $1.5 million in fines with potential jail time.

Applicable ROB

Employee: 1e

Contractor: 1d, 1e

Refer to the link to VA Handbook 5021, Employee/Management Relations found in Appendix D: Privacy and Information Security Resources, or contact your Human Resources or Employee Relations representative for more information.

Knowledge Check: Consequences of Privacy or Information Security Violations

Incidents involving VA sensitive information can have serious consequences for VA and Veterans, and for you. Review the list below and select the ones you think are reportable incidents. Then check your selections by reading the feedback.

A. Misdirected mail containing PII/PHI
B. Lost or stolen equipment
C. Unattended documents in a locked office
D. Shredding papers that are not considered records
E. Unencrypted email containing PII/PHI
F. Missing or stolen information

Feedback: The incidents to report are A, B, E, and F: misdirected mail containing PII/PHI, lost or stolen equipment, unencrypted email containing PII/PHI, and missing or stolen information. Items C and D are not incidents: unattended documents in a locked office and shredding papers that are not considered records.

The Steps to Report an Incident

If you see or hear something that is of concern, report it to your supervisor, ISO, and PO. If you work in VHA, you can also report it to your Administrator of the Day (AOD). All incidents should be reported.

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

Additional contact information to report incidents may be found in Appendix D: Privacy and Information Security Resources. These questions will help you provide clear information when you report an incident.

Who?

Contact your supervisor, your ISO, and PO right away. You should also contact your Administrator of the Day (AOD) if you work for VHA. Report all actual and potential incidents. If you are a contractor, you should also report every incident to your COR and Project Manager.

Applicable ROB

Employee: 1f, 1g

Contractor: 1h

What?

What happened (e.g., what information was shared)?

Why?

Why did it happen? (if known)

When?

When did it happen?

How?

How did it happen?

Additional or Alternate Contacts

In situations where you cannot report an incident to your supervisor, ISO, PO, and AOD, you can reach out to other points of contact.

- If your supervisor, ISO, PO, and AOD are not available, contact the VA National Service Desk to report the incident directly to VA NSOC.
- If an incident occurs after hours or on a weekend, contact the VA National Service Desk and follow your work unit's procedures to notify your supervisor and VA NSOC.
- If you suspect an unethical or criminal action, contact local VA police and the Office of Inspector General (IG) as well as your supervisor (or COR) and ISO and PO.
- If you suspect fraud, waste, or mismanagement of resources, then contact the IG.
- If you suspect your supervisor is involved in the incident, report the incident to your ISO and PO.

Applicable ROB

Employee: 1f, 1g

Contractor: 1h

Knowledge Check: Reporting an Incident

It's important for you to know how to report an incident properly. What should you do first when reporting an incident? Select the best answer to the following question.

You come into the office early to get some work done and are the first person in the office. As you walk to your desk, you notice some papers on the printer in the open area by the Medical Center visitor waiting room. There are several medical billing claims that have been printed with PII and PHI on them, including names and Social Security numbers, which have been left unattended since the day before. You decide to report it as an incident.

What's your first step?

A. Contact the VA NSOC
B. Contact your supervisor, ISO, and PO
C. Email the VA National Service Desk
D. Email the VA Office of the Inspector General

Answer B is correct. You should first contact your supervisor, ISO, and PO. Your ISO or PO will report it to the VA NSOC within one hour of the incident being reported.

It's in Your Hands – Module Summary

Let's recap the key points of this module:

- Report incidents or suspected incidents right away.
- Report incidents to your supervisor (or COR), ISO, and PO.
- If your supervisor (or COR), ISO, and PO are not available, report the incident directly to NSOC by contacting the VA National Service Desk.
- Remember, never be afraid to report an incident. Any time you hear or see something of concern, report it!

Module 8: Course Summary and Rules of Behavior

Course Summary

Privacy and information security are in your hands every day. These policies, guidelines, and best practices are here to help protect you, VA, and our nation's Veterans. When it comes to making good choices to protect privacy and information security, it's in your hands!

To protect privacy and ensure information security:

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

Acknowledge, Accept, and Comply with the ROB

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

If you access and use VA information systems or VA sensitive information, you must accept responsibility for protecting privacy and ensuring information security by accepting, signing, and complying with the ROB. The ROB are the minimum compliance standards for all VA locations. You must review and sign the ROB to receive and retain access to VA information or information systems.

Instructions

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

If you are reviewing the Text-Only Version of the Annual Privacy and Information Security Awareness and Rules of Behavior training, print and sign either the Employee Rules of Behavior document or the Contractor Rules of Behavior document. To complete this training, identify your role, print the appropriate document (Appendix A: Rules of Behavior for VA Employees or Appendix B: Rules of Behavior for VA Contractors), and then acknowledge and accept the appropriate ROB. To acknowledge

and accept the ROB, initial each printed page with your initials where indicated, and sign the last page of the document where indicated.

VA Employee

See Appendix A to review and accept Employee Rules of Behavior.

Before you complete the signature step: Are you selecting the correct ROB? These rules are for you if you are a VA employee who works for VA under Title 5 or Title 38, United States Code. This also includes volunteers, without compensation (WOC) employees, and students* or other trainees. **Note:** By selecting "I Acknowledge and Accept" on the following page you are fulfilling the requirement in VA Handbook, 6500, Appendix D, Introduction, part 2 (e and f).

*Reminder: If you are a medical trainee (i.e., student, intern, extern, resident, or fellow), VA does not require you to complete this course, but you must complete the course VHA Mandatory Training for Trainees (VA TMS ID: 3185966).

VA Contractor

See Appendix B to review and accept Contractor Rules of Behavior.

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

Applicable ROB

Employee: 1a, 1i, 1j, 3a, 3b

Contractor: 5

Signed ROB Submission

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

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

Course Completion

Congratulations! 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.

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

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

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.

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

Initials _____

PO, immediately upon suspicion.

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

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

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

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

2. SPECIFIC RULES OF BEHAVIOR

a. Basic

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

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

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

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

Initials _____

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;

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.

Initials _____

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

(4) If approved to use, process, store, or transmit electronic VA sensitive information remotely, I must ensure any device I utilize is encrypted using FIPS 140-2 (or its successor) validated encryption. Information systems must use VA's approved

configuration and security control requirements. The local CIO and ISO must review and approve (in writing) the mechanisms used to transport and store the VA sensitive data before it can be removed from the VA facility.

(5) I will ensure that all printouts of VA sensitive information that I work with, as part of my official duties, are physically secured when not in use (e.g., locked cabinet, locked door).

(6) I acknowledge that particular care should be taken to protect SPI aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function.

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

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

Initials _____

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

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

(11) I will not auto-forward e-mail messages to addresses outside the VA network.

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

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by VA to protect sensitive data. I will only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. For questions regarding need-to-know and safeguards, I will obtain guidance from my VA supervisor, local CIO, and/or ISO before providing any access.

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

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

(16) I will never swap or surrender VA hard drives or other storage devices to

Initials _____

anyone other than an authorized OIT employee.

c. Logical Access Controls

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

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

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

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

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

d. Remote Access/Teleworking

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

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

(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

Initials _____

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

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

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

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

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

e. Non-VA Owned Systems

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

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

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

f. System Security Controls

Initials _____

(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	

Initials _____

APPENDIX C: Glossary

A

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

B

Blog – An online journal. A blog (shortened from "Web log") is an online journal that may be personal or topical, 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

Citrix Access Gateway (CAG) – A secure application and data access solution that provides users with remote access from anywhere. Source: www.citrix.com

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

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

Contractors – People who agree to supply VA with goods or services at a certain price. Contractors are all non-VA users who have 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: W3C Glossary Dictionary

F

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

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

Federal Information Security Management Act (FISMA) – A law that requires VA to have an information security program. Title III of the E-Government Act requires each

federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Source: NIST SP 800-63

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

Flickr – A web-based photo and video host service. Flickr allows users to store, sort, search, and share photos and videos online through social networking sites. Source: http://www.flickr.com/help/general/

Freedom of Information Act (FOIA) – A law that gives people the right to see federal government records. FOIA provides that any person has a right of access to federal agency records, except to the extent that such records are protected from release by a FOIA exemption or a special law enforcement record exclusion. It is VA's policy to release information to the fullest extent under the law. Source: http://www.foia.va.gov/

G

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

H

Health Information Technology for Economic and Clinical Health Act (HITECH) – A law that describes when and how VA hospitals and doctors can exchange a person's health information. The HITECH Act of the American Recovery and Reinvestment Act imposes more stringent regulatory requirements under the security and privacy rules of HIPAA, increases civil penalties for a violation of HIPAA, provides funding for hospitals

and physicians for the adoption of health information technology, and requires notification to patients of a security breach. These broad new requirements will necessitate compliance by covered entities, business associates, and related vendors in the health care industry. Source: http://www.nixonpeabody.com/publications_detail3.asp?ID=2621

Health Insurance Portability and Accountability Act (HIPAA) and HIPAA Privacy Rule (1996) – A law that requires VA to keep a person's health information private. HIPAA establishes requirements for protecting privacy of personal health information. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system. Source: http://www.hipaa.com/

I

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

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

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

Integrity – To make sure VA information is correct. Integrity is the guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. Source: VA Handbook 6500

Internal Business Information (IBI) – Knowledge or facts owned by an organization, including assets such as future product designs, customer/price lists, and internal policies not intended for public consumption. Sometimes also referred to as Proprietary Information. Source: Carnegie Mellon Software Engineering Institute

J – N/A

K – N/A

L – N/A

M

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

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

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

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

Microsoft SharePoint – Software used to store documents on an Intranet site. It can be used to set up collaborative sites to share information with others, manage documents from start to finish, and publish reports to help make decisions. Source: Microsoft

N

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

O – N/A

P

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

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

Personal Identity Verification (PIV) Cards – An ID card that receives, stores, recalls, and sends data securely. The PIV card is an ID card issued by a federal agency that contains a computer chip, which allows it to receive, store, recall, and send information in a secure method. The main function of the card is to encrypt or code data to strengthen the security of both employees' and Veterans' information and physical access to secured areas, while using a common technical and administrative process. The method used to achieve this is called Public Key Infrastructure (PKI) technology. PKI complies with all federal and VA security policies, and is the accepted Global

Business Standard for Internet Security. As an added benefit, PKI can provide the functionality for digital signatures to ensure document authenticity.
Source: http://www.va.gov/pivproject/

Personally Identifiable Information (PII) – Any information 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 which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information. Source: Office of Management and Budget (OMB) Memorandum 07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information (May 22, 2007). NOTE: The term Personally Identifiable Information is synonymous and interchangeable with Sensitive Personal Information. 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: Partners Healthcare Glossary of Common Terms, Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Privacy Act of 1974 – Legislation that states how federal agencies can use personal data. The Privacy Act of 1974 establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements. Source: http://www.justice.gov/opcl/privacyact1974.htm

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

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

Protected Health Information (PHI) – The HIPAA Privacy Rule defines PHI as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as VHA. NOTE: VHA uses the term protected health information to define information that is covered by HIPAA but, unlike individually-identifiable health information, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer. Source: VA Handbook 6500.2

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

Q – N/A

R

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

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

Records Management Officer – A person who is responsible for managing VA records. A Records Management Officer, who is also known as a Records Custodian, 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

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

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

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

S

Sanitize – A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, Damage, and Destruct are actions that can be taken to sanitize media. Source: NIST SP 800-88

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

Social Engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Source: NIST SP 800-82

Social Media – Web and mobile-based tools that allow persons and groups to exchange ideas. Social Media is specifically designed for social interaction that uses highly accessible and scalable publishing techniques using web-based technologies. Social media uses web-based collaboration technologies to blend technology and social interaction in order to transform and broadcast media monologues into social dialogue, thereby transforming people from content consumers to content producers. This form of media does not include email. Source: VA Directive 6515

Spoofing – Spoofing refers to sending a network packet that appears to come from a source other than its actual source. Source: NIST SP 800-48

T

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

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

Twitter – Allows people to stay connected through the exchange of short messages. Twitter is a real-time information network that connects users to the latest stories, ideas, opinions, and news about what they find interesting. Users can find the accounts they find most compelling and follow the conversations. Source: Twitter

U

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

V

VA Confidentiality Statutes (Title 38 U.S.C. 5701, 5705, 7332) – Statutes requiring VA to keep medical claims, information, and health records private. (1) Title 38 U.S.C. 5701: VA Claims Confidentiality Statute is a statute that states VA must keep claims private. VA Confidentiality Statute 38 U.S.C. 5701 provides for the confidentiality of all VHA patient claimant and dependent information with special protection for names and home addresses. (2) Title 38 U.S.C. 5705: Confidentiality of Medical Quality Assurance Records is a statute that states VA shouldn't disclose medical quality-assurance program information without permission. VA Confidentiality Statute 38 U.S.C. 5705 provides for the confidentiality of Healthcare Quality Assurance (QA) records. Records created by VHA as part of a designated medical quality assurance program are confidential and privileged. VHA may only disclose this data in a few limited situations. (3) Title 38 U.S.C. § 7332: Confidentiality of Certain Medical Records is a statute that states VA must keep health records containing drug abuse, alcohol abuse, HIV, and Sickle Cell Anemia private. VA Confidentiality Statute 38 U.S.C. § 7332 provides for the confidentiality of VHA-created, individually-identifiable drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or Sickle Cell Anemia medical records and health information. 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

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

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

W

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

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
Office of Inspector General (IG) Hotline (to report fraud, waste, or mismanagement of resources) (800) 488-8244
VA National Service Desk (to request computer, network, or access support; or to report security incidents to the Network Security Operations Center [NSOC]) (800) 877-4328

Table 2. VA Web Links
CRISP Information* http://vaww.sde.portal.va.gov/oitauditprep/SitePages/Home.aspx
Information Security Portal* https://vaww.infoprotection.va.gov/
ITWD's Role-based Training* 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 VA's Intranet

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

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

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-subchapI-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, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program and Appendix D, VA National Rules of Behavior
VA Handbook 6500.1, Electronic Media Sanitization
VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information
VA Handbook 6502, VA Enterprise Privacy Program
VA Handbook 6502.4, Privacy Act Review
VA Handbook 6512, Secure Wireless Technology
VA Handbook 6609, Mailing of Personally Identifiable and VA Sensitive Information
VHA Directive 1605, VHA Privacy Program
VHA Handbook 1605.1, Privacy and Release of Information
VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information

Table 7. Additional Selected VA Handbooks and Directives
Available at: http://www1.va.gov/vapubs/index.cfm
VA Directive 0701, Office of Inspector General Hotline Complaint Referrals
VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program
VA Directive 6515, Use of Web-based Collaboration Technologies
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 System Security Controls
VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior