VA Privacy and Information Security Awareness and Rules of Behavior

From Awareness to Action the VA Way





FY16 Text-Only Course Transcript

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

Table of Contents

Purpose of this Document

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

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

This version of the VA Privacy and Information Security Awareness and Rules of Behavior Text-Only Course Transcript is valid for fiscal year (FY) 2016 (i.e., October 1, 2015 through September 30, 2016).

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

1. Print and sign the appropriate Rules of Behavior (ROB), as well as initial each page in the space provided.
    a. Sign Appendix A: VA National Rules of Behavior if you are an employee.
    b. Sign Appendix B: Rules of Behavior for Contractors if you are a contractor.
2. Contact your supervisor or Contracting Officer Representative (COR) to submit the signed ROB and to coordinate with your local Talent Management System (TMS) Administrator to ensure you receive credit for completion.

Using Hyperlinks Within This Document

Throughout this document, you are able to access more detailed information. The INFO, knowledge checks, and applicable Rules of Behavior links in the appendices by selecting the available hyperlinks. **To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.**

Module 1: Welcome

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

Who Must Take This Course?

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

All VA employees (or users) who use VA information or VA information systems must take this training, including:

- Paid employees
- Unpaid employees
- Volunteers.

Applicable ROB

VA National: 1b, 2h(1)

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

There are some exceptions to the definition of all users who must take this training.

Contractors

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

Students or other trainees

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

VHA and VBA employees and contractors

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

INFO: Laws

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

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

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

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

You can find more information in the Privacy and Information Security Resources document in Appendix D, Resources.

Rules of Behavior (ROB)

You must take this course as well as acknowledge, accept, and comply with the VA National Rules of Behavior (ROB) every year in order to use or maintain access to VA information and information systems. There are two versions of the ROB included in this course: one for VA Users who are not contractors (defined in Handbook 6500 Appendix D) and one for contractors (defined in Handbook 6500.6 Appendix D). Both versions of the full ROB are in the Appendices. Some offices or facilities require more rules and guidelines for increased protection. Always follow the ROB and your local rules.

Applicable ROB

VA National: 1j, 2a(2), 2a(3)

VA Contractor: 2a, 3d

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

INFO: Which ROB version applies to you?

VA National ROB (Users who are not contractors)

Users who are not contractors includes multiple types of employees. Employees are all people who work for VA under Title 5 or Title 38, United States Code. This definition of employees also includes volunteers, without compensation (WOC) employees, and

students or other trainees. These users must complete this training and acknowledge and accept the ROB to use, gain, or maintain access to VA information systems or VA sensitive information.

Contractor ROB

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

From Awareness to Action the VA Way

Awareness

This course is your eyes and ears for privacy and information security awareness. Be on the lookout for examples in the course for taking action the VA way.

"I will complete mandatory periodic security and privacy awareness training within designated time frames and complete any additional role-based security training required based on my roles and responsibilities."

Understanding

Use your good judgment to make the connection between the Rules of Behavior and your work.

"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 they contain or that may be accessed through them as well as the security and protection of VA information in any form (e.g., digital, paper, verbal)."

Commitment

When you protect VA sensitive information, you are protecting Veterans and their families as well as VA and its employees.

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

Action

Commitment leads to action. Comply with the Rules of Behavior every day. Be aware. Be secure. It's the VA way.

Course Objectives

Evolving computer technologies and tools increase the speed and effectiveness of providing services to Veterans. New risks are a part of every new opportunity. You must be aware of these risks at all times and ready to move from awareness to action to protect sensitive information and systems. Awareness and action—it's the VA way!

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

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

Module 2: Privacy and Security Basics

Objectives

Protecting privacy and information security is the focus for everyone at VA. Following the rules every day is the VA way of being aware and noticing risks in everyday situations. It is also about taking action to keep those risks from turning into losses for Veterans or VA. Wise actions are stated in rules of behavior so you know what you must do.

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

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

Privacy and Information Security Requirements

You have a responsibility to protect privacy and safeguard information security. Information security is a set of principles and actions that ensures VA information systems and VA sensitive information are not accessed or changed by unauthorized people and are available when we need them.

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

- Talking with others
- Handling paper records or electronic files
- Using email and other types of electronic messaging
- Using electronic devices and VA information systems
- Using the Internet and social media.

Applicable ROB

VA National: 1a, 1f, 2b(13)

VA Contractor: 1h, 2b(14)

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

INFO: Confidentiality, Integrity, and Availability

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

Confidentiality

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

Integrity

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

Availability

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

Types of VA Sensitive Information

It is your responsibility to protect privacy. That means you do not disclose, alter, or destroy VA sensitive information unless you have permission. Veterans are counting on you.

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

Both Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) are VA sensitive information and refer to information about a specific person, such as:

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

Protected Health Information (PHI)

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

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

Regulatory or program-specific information

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

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

Knowledge Check: Types of VA Sensitive Information

Consider the following question by selecting the best answer.

Which of the following sensitive information examples represent PHI?

A. An employee's education records
B. Medical program quality assurance records
C. A patient's name and diagnosis
D. A volunteer's driver's license number
E. A framework used for servers, desktops, and networks

Answer C. is correct. A patient's name and diagnosis is an example of PHI (Protected Health Information). Other types of VA sensitive information are PII and regulatory or program-specific information. Remember, you must protect all types of VA sensitive information.

What Are Federal Records?

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

The Federal Records Act of 1950 and later regulations require federal agencies to create and maintain federal records. Federal records document the business activities of the organization/agency. They are federal property and must be managed and maintained in accordance with the prevailing law.
Each work unit within VA must create and maintain a listing of records. This list is known as a file plan. Federal records must be kept according to a Records Control

Schedule (RCS) that is approved by the National Archives and Records Administration (NARA). The RCS provides the retention and disposition rulings for all scheduled federal records listed in the RCS. A document known as the General Records Schedule contains more information about disposition rulings.

Organizational Records Officers and Records Liaison Officers manage federal records across VA administrations and facilities. Work with your local organization Records Officer or Records Liaison Officer if you are creating, transporting, storing, or disposing of records to be sure VA sensitive information is protected.

Find more information about federal records in the Privacy and Information Security document in Appendix D, Resources.

INFO: Examples of Records and Nonrecords

Records

Examples of records include:

- Materials created or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business
- Materials that are 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.

Nonrecords

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

Examples of nonrecords include:

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

Continuous Readiness in Information Security Program

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

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

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

Strong Passwords

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

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

Applicable ROB

VA National: 2c(2), 2c(3), 2c(4)

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

Some systems may reject recently used passwords. Avoid using a password that has been used within your last three password changes and change your password every 90 days as required. For more information on passwords, refer to VA Handbook 6500, Appendix F, VA System Security Controls.

INFO: Strong Passwords

Strong passwords meet VA's minimum password requirements. Examples of strong passwords include p1e@Sent and ReMeM8Er!.

Avoid weak passwords that contain any of the following:

- Your username, a real name, or a company name
- Complete dictionary words
- Words that are similar to previous passwords
- Words using increments, such as Password1, Password2.

Simple Actions, Big Impact: Preventing Lost PIV Cards

In common situations like this one, your simple actions can have a big impact.

"I protect my PIV card the same way I would protect my cash and credit cards in my wallet. I need my PIV card as proof of my identity and to access VA facilities and systems."

Your VA PIV card is vital to protecting the security, identity, and privacy of every person at VA, protecting VA as an organization, and most importantly, protecting the Veterans we serve.

Be on the lookout. It's the VA way.

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

Personal Identity Verification (PIV) Cards

A Personal Identity Verification (PIV) card is also known as a PIV badge. It is an identification (ID) card that increases protection of VA facilities, information, and information systems. The first element of two-factor authentication is something you have, such as a PIV card that provides access to VA buildings, networks, and resources. The second element is something you know, your Personal Identification Number (PIN) to access information systems. PIV cards comply with Federal Information Processing Standard (FIPS) 201 and related guidance. You must protect your PIV card from loss or theft. Always keep it with you. Be careful not to leave it in the computer when you are away, and never place it on a chair or table in a public place where you might forget it. If you lose or misplace your PIV card, you could be giving a dishonest person the opportunity to enter VA facilities or gain access to Veterans' information.

Applicable ROB

VA National: 2a(4)

If a card is lost, it must be reported to VA security and law enforcement, the Information Security Officer (ISO), and your management. A lost PIV card must be revoked in the system immediately.

Note: You can learn more about PIV cards by contacting your local PIV office or security office. See Appendix D, Resources for the policy governing PIV cards.

Knowledge Check: Personal Identity Verification (PIV) Cards

Consider the following question.

Controlling access is one way to protect information. Which of the following is an example of two-factor authentication that can be used to gain access to a VA facility or VA information system?

A. PIV card and driver's license
B. Password and Social Security card
C. Personal identification number (PIN) and PIV card
D. Passport and driver's license

Answer C. is correct. Your Personal identification number (PIN) together with your PIV card allows two-factor authentication for access to VA buildings, networks, resources, and complies with Federal Information Processing Standard (FIPS) 201 and related guidance.

Who Can Help?

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

Applicable ROB

VA National: 2a(2),2c(1),2h(2)

VA Contractor: 1h

Supervisor

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

- Ensure staff understands IT security and privacy information protection issues.
- Ensure staff complies with security and privacy regulations and policies.
- Ensure staff only has access within the scope of their duties.
- Verify staff completes all privacy and security information security training requirements.
- Ensure staff signs the VA National ROB each year.
- Help staff report identified privacy and information security incidents.

Contracting Officer (CO) or Contracting Officer Representative (COR)

Contracting Officers (CO) or Contracting Officer Representatives (COR) are responsible for:

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

Privacy Officer (PO)

Privacy Officers (POs) are required to:

- Promote privacy awareness
- Communicate privacy training requirements and deadlines
- Ensure compliance with federal privacy laws and regulations and VA directives, handbooks, and other guidance
- Respond to, investigate, and report privacy incidents
- Provide support when incidents occur
- Track privacy training completion
- Complete a Privacy Threshold Analysis (PTA) and annual Privacy Impact Assessment (PIA).

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

Information Security Officer (ISO)

Information Security Officers (ISOs) must:

- Manage local information security programs and provide training
- Monitor access to VA information systems
- Help create and maintain information system security plans and emergency plans
- Assess system risks
- Take part in security self-assessments and system audits

- Ensure information security measures are working as intended
- Respond to, investigate, and report information security incidents.

Note: See Appendix D, Resources for a link to the ISO Locator to identify the ISO for your location.

Knowledge Check: Common Mistakes

Consider the following question.

Which of the following examples are mistakes that can expose VA sensitive information wherever you are working?

A. Discussing patient information in public
B. Sharing VA sensitive information with a colleague who doesn't have a need to know
C. Leaving VA sensitive information unattended on your desk
D. All of these

Answer D is correct. All of these examples are a risk to Veterans and VA. It is your responsibility to keep VA sensitive information safe wherever you are working. Follow all information security and privacy policies and procedures and the ROB.

Summary

Here are the key points of this topic. It's important to:

- Protect VA sensitive information, which includes SPI or PII, PHI, and regulatory or program-specific information
- Comply with the ROB to protect privacy and ensure information security
- Make sure you handle records carefully and protect VA sensitive information contained in records
- Contact your supervisor or COR, PO, and ISO to help you comply with all regulations.

Module 3: How to Recognize and Report an Incident

Objectives

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

- Identify common privacy and information security incidents
- Recognize consequences and penalties that may occur if you cause an incident
- Recall how to report incidents.

Recognizing and Reporting Incidents

Incidents are defined as suspected or identified privacy and information security violations.

Applicable ROB

VA National: 1f,1g

VA Contractor: 1h

Examples of all-too-common incidents include:

- Mishandling of VA sensitive information in paper documents
- Mailing VA sensitive information to the wrong recipient
- Missing or stolen unencrypted equipment
- Accessing electronic VA sensitive information without authorization or the need to know
- Discussing patient information in inappropriate locations
- Relocating inventory (Personal Computer [PCs], computers, printers, etc.) without notifying IT.

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

Simple Actions, Big Impact: Keeping Unencrypted Equipment Safe

In common situations like this one, your simple actions can have a big impact.

"I was shocked by what I read online: Every week, more than 12,000 laptops are reported lost in airports in this country, and almost 200 mobile phones are are left in taxicabs. Every week!"

We handle our equipment with care at VA, especially when we're traveling. We keep our laptops and tablets secured with VA-issued cable locks. By encrypting laptops and other devices, VA prevents accidental access to sensitive information.

Use your good judgment. It's the VA way.

Impact

Privacy and information security incidents can affect VA, Veterans, and you. Here are some things that can happen because of an incident:

- Veterans may be harmed by making sensitive information public, including a financial loss, loss of privacy, or exposure to identity theft.
- You could face job loss, fines, and possibly prison if you are the cause of an incident.
- VA may lose the public's trust.
- VA may have to report the incident to Congress, especially if the incident is an information data breach affecting a large number of Veterans.
- VA resources that could be spent to serve Veterans must be spent instead to correct mistakes.
- Certain kinds of incidents could threaten our national security.

Consequences if You Cause an Incident

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

Applicable ROB

VA National: 1e

Serious consequences of privacy and information security violations could include:

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

Simple Actions, Big Impact: Availability of VA Sensitive Information

In common situations like this one, your simple actions can have a big impact.

“If I don’t have a need to know in order to do my job, I shouldn’t even look at sensitive information. Who knew curiosity can be a crime? Veterans can trust me to mind my own business and respect their privacy. I expect the same integrity in business practices whenever my personal information is used by my bank or my doctor’s office or any other service I purchase.”

Veterans trust that VA employees respect their private information and follow the Rules of Behavior. At the least, inappropriate access to sensitive information undermines trust. At worst, you could be prosecuted if you cause a data breach. If you do not need to know sensitive information to do your job, don’t seek it!

Commit to protecting VA sensitive information. It’s the VA way.

Severe Penalties

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

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

Also, if you:

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

Applicable ROB

VA National: 1e

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

Knowledge Check: Reporting an Incident

Consider the following question.

You overhear a coworker on a personal phone call telling someone medical details about one of the patients in your area. You believe the person on the phone is not a VA employee. What do you do?

A. Ask your coworker about it when he or she gets off the phone
B. Report your suspicions to the PO
C. Tell the patient about what you overheard
D. All of the above

Answer B is correct. Everyone at VA is responsible for reporting any suspicious activity or situation that could put VA sensitive information or information systems at risk.

The Steps to Report an Incident

Always be ready to report a privacy or security incident. If you notice an activity or situation that could put VA sensitive information or information systems at risk, here are the steps to report it:

Applicable ROB

VA National: 1f, 1g

VA Contractor: 1h

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

Step 2. Report it:

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

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

Additional contact information to report incidents may be found in the Privacy and Information Security Resources document in the course Resources. The National Service Desk now answers the NSOC telephone number, which is also located in Appendix D, Resources.

Knowledge Check: Reporting an Incident

Consider the following question.

Joe found medical records in the waste basket in a copy center next to his workstation. Should he report this as an incident?

A. No, he can easily place the medical records in the shredder bin
B. Yes, leaving PHI in a an unsecured wastebasket is a risk to Veteran's information and must be reported
C. No, he can place the documents on the copier with a note asking the person who threw them away to put them in the shredder bin
D. No, he can keep the medical records until someone asks for them

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

More Contacts

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

Applicable ROB

VA National: 1f, 1g

VA Contractor: 1h

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

Summary

Here are the key points to help you when reporting incidents:

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

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

Module 4: VA Equipment, New Tools, New Risks

Objectives

Equipment and tools used in the workplace come in all sizes and shapes. Some equipment is stationary, while other equipment is portable. As technology continues to evolve, privacy and security risks also evolve.

New tools bring new risks. Mobile devices, like smart phones and tablets, are easy to transport and are easily lost or stolen. They can provide easy access to an array of software applications (apps) and popular social media that help get work done efficiently. Be aware of risks before you begin using a new device and whenever you use social media. Always take action to protect information. When you have completed this topic, you will be able to:

- Select the correct actions to protect VA sensitive information when using mobile devices and social media tools
- Describe how to safeguard VA sensitive information when using mobile devices and other equipment
- Recognize when you may use personally owned equipment for VA business
- Identify how social media can expose VA sensitive information.

Requirements for VA Mobile Devices

You are responsible for the care, use, and protection of any VA-issued mobile devices and the information stored on them. VA supports thousands of mobile devices across the country, and these devices may store, process, or transmit VA sensitive information that needs protection.

Applicable ROB

VA National: 1a,2b(9),2b(13)

VA Contractor: 2b(14)

To protect the information on your VA mobile devices:

- Keep your security software up-to-date, following VA's guidance
- Use VA-approved encryption and passwords
- Enable VA-approved security tools
- Notify IT inventory coordinators, via your supervisor, if your location has changed
- Never open attachments from an unknown sender
- Never select a URL sent by an unknown sender directing you to a website
- Report all odd messages or suspected threats and warnings to your ISO.

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

INFO: Protecting Mobile Devices

Know the rules

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

Protect patient data and your information

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

Keep it with you

Never leave any of your mobile devices unattended.

- Smaller mobile devices that do not have the ability to use a cable lock should be kept in a secure place, such as a locked cabinet, desk, or safe, if available.
- If you are working in an uncontrolled area, use VA-issued cable locks for laptops and tablets with this capability to help keep your equipment secure, and keep your smaller mobile devices that are unable to be cable locked with you personally.

Safeguard VA data

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

Simple Actions, Big Impact: VA Mobile Devices

In common situations like this one, your simple actions can have a big impact.

"I pay really close attention to my VA mobile phone. It's either in my purse or in my hand. I am always careful—except for last week. At the end of a long workday, I backed out of my parking spot and caught a glimpse of my VA BlackBerry sliding off the back of my car. Thank goodness I didn't drive away. That was a close one."

It only takes a single lapse of attention to create a risk. Make sure that you know where your mobile devices are at all times. Use VA-approved, encrypted portable electronic devices.

Be aware. Be secure. It's the VA way

Limited Personal Use of VA Office Equipment

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

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

Applicable ROB

VA National: 1d, 2g(7)

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

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.

INFO: Prohibited Activities

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 mailing
- Supporting “for profit” activities outside of VA
- Participating in unapproved lobbying or fundraising.

Personal Electronic Devices

You must have permission to use any personal electronic devices for VA work. **Be aware**: VA does not allow you to bring your personally owned equipment into a VA facility and connect to the network. Personally owned devices may only use VA-approved remote access technologies, such as Citrix Access Gateway (CAG), to access VA resources.

Applicable ROB

VA National: 2e(2),2e(3),2g(1)

If you are approved to bring personally owned equipment into a VA facility, you must have approval from the System Owner or local Chief Information Officer (CIO) to use remote access from your personally owned equipment while in the facility. Never store VA sensitive information on any personal electronic device.

Risks of Electronic Devices

Criminals can access your electronic devices and can copy unencrypted data, email, contacts, and files. Examples of equipment or devices that can have wireless capabilities include telephone headsets, wireless keyboards, mobile telephones, tablets, and laptop computers.

Applicable ROB

VA National: 2b(14),2d(2),2g(4)

Contractor: 3a,3b

INFO: Wireless telephone headset

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

Wireless keyboards

Wireless keyboards use a Cloud service to translate the keystrokes into text, which puts VA sensitive information at risk while it is in the Cloud. Do not use a wireless keyboard while working on VA business-related activities unless it meets National Institute of Standards and Technology (NIST) certification and has been approved by your Facility CIO.

Instant Messaging

VA has implemented a secure instant message (IM) system when using VA's network. VA allows you to access and use Microsoft Lync® as a secure, encrypted way to exchange VA sensitive information. Microsoft Lync may not be available for some mobile devices. Never conduct VA business using instant message features of personally owned devices.

Applicable ROB

VA National: 2a(1),2b(4),2g(6)

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

IMs saved in Microsoft Outlook® conversation history are not encrypted, so make sure you delete IMs from your conversation history. Users can turn off the feature to save messages to your conversation history in the Lync set-up. Contact the VA National Service Desk for help, if needed. It's important to know that IMs are not part of a system of records.

Texting

You may use VA text messaging in the performance of job duties in the same manner as you utilize email. That is, if you have a VA-issued device with text message capability, you may send and receive text messages. However, text messages are not encrypted. You must not send PII or PHI to patients using text messages. Sending VA sensitive information in an unencrypted text message can put VA at risk.

Applicable ROB

VA National: 2a(1),2b(4),2g(6)

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

Text messaging is a form of electronic transmission and is subject to employee and contractor ROB guidance.

Using Apps on a VA Mobile Device

Software applications, or apps, can make some tasks faster and easier on mobile devices. Apps available in the VA App Catalog have passed extensive security reviews and have been deemed safe for use with sensitive data. If you will be receiving VA information on an app, that app must be downloaded from the VA App Catalog.

Applicable ROB

VA National: 1a,1(d),2b(9)

If the VA App Catalog does not have the apps you need for your work, you may need to download apps from a public app store. All VA ROB must be followed. VA-approved public app stores include:

- Apple App Store
- Google Play Store.

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

Mobile device users who have approval to download applications to VA devices from approved public app stores must take great care to protect VA sensitive information. VA maintains a catalog of approved apps that may be safely used with sensitive information. **Apps from public catalogs *are not approved* for use with sensitive information.** Be wary of pop-ups that might request access to your information and keep in mind that no public apps can be used to store or process PII or PHI. You must protect VA sensitive information when you use any type of electronic device or communication to store, transport, or dispose of information.

INFO: Mandatory training before using public app stores

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

Before you use and download public apps through public app stores, you must participate in a mandatory training session available through the MyVeHU Campus titled *Protecting Privacy and Security While Using Apps from the Public App Store* (session code: #14138).

Other training available on the TMS includes:

- TMS 3926744—*Mobile Training: Security of Apps on iOS Devices*
- TMS 3926743—*Mobile Training: Apple Native Email Client*

Note: The best solution is to use only VA-approved apps from the VA App catalogue if the intended use involves VA sensitive information. You should not download any public app from a public app store for work purposes to access or store VA data. However, VA is always testing third-party apps to upload to the VA App catalog. Continue to check the VA App Catalog, as new and verified apps are added often.

Privacy and Security on Mobile Apps

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

Downloading Public Apps

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

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

- Location
- Contacts
- Calendar
- Photos
- Microphone.

Public Apps and PHI/PII

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

Mobile Device Privacy Settings

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

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

Knowledge Check: Using Apps on Your VA Mobile Device

Consider the following question.

There's an app I want to use on my VA-furnished electronic tablet to keep track of follow-up items for my data mining project. The best app is only available from the Apple App Store. What should I do?

A. Download it through the Apple App Store and start using it
B. Check Yammer to find out if any of my other colleagues are using it
C. Ask my local IT department if it's okay
D. Do not download it. Submit a help desk ticket for the app to be tested and hopefully added to the VA App Catalog

Answer D is correct. The best solution is to use only VA-approved apps from the VA App Catalogue if the intended use involves VA sensitive information. You should not download any public app from a public app store for work purposes to access or store VA data. However, VA is always testing third-party apps to upload to the VA App Catalog. Continue to check the VA App Catalog, as new and verified apps are added often.

Using Social Media Securely

VA has approved some social media tools and technologies for use when doing VA business. These include blogs, Facebook, Twitter, YouTube, and VA Pulse. When you access and use these tools, be aware that they can be open to attacks, including phishing and social engineering.

Applicable ROB

VA National: 2h(3)

VA Contractor: 2b(12)

Here are some recommended practices when using the approved social media tools:

- Never comment on VA legal matters, unless you are an official spokesperson and have approval to do so.
- Never post any VA sensitive or protected information on any social media site.
- Never store VA sensitive information on a third-party file sharing site (e.g., Google Docs, Dropbox).
- Limit the details you reveal in text, which can expose VA sensitive information.
- Refrain from posting VA business or VA sensitive information in personal emails or external social media outlets, such as websites, Facebook pages, blogs, and Tweets.
- Be aware of the details you reveal in photos.

- Be professional and use good judgment when posting pictures and text; you are accountable for the content you publish.

Refer questions about these tools to VA Public Affairs, the VA organization responsible for managing VA social media channels. See VA Directive 6515, Use of Web-Based Collaboration Technologies, for more information.

Social Engineering Attacks

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

Applicable ROB

VA National: 2g(3)

Examples of social engineering attacks include:

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

Interactive Exercise: Prevent Attacks

Read the following examples and consider which are threats that could harm VA networks.

Category 1: Text message

You receive a text message from someone you do not know asking you to verify your VA username and password. Is this secure?

A. Yes, it is secure.
B. No, it is not secure.

Answer B is correct. The text message is not secure. Never share your password or verify codes. This could be a social engineering threat.

Category 2: Conversation between coworkers

It is okay to share your password with your teammates so they can cover for you in a pinch.

A. Yes, it is okay.

B. No, it is not okay.

Answer B is correct. Never share your password or other account information, even with trusted coworkers.

Category 3: Email

You receive an email from an unknown sender and it has an Internet link and an attachment. Should you open the link and attachment?

A. Yes, you can open the link.
B. No, you cannot open the link.

Answer B is correct. Do not open the link. Attackers may use links or attachments to infect VA computers. It's a tactic called phishing. If you don't know the sender, don't open the link or attachments.

Risk of Wireless Networks

Criminals can access your electronic devices through wireless networks and can copy unencrypted data, email, contacts, and files.

To protect your VA devices:

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

Identity Theft

The thought of your identity being stolen can be overwhelming. Unfortunately, in today's digital age, more people are experiencing this scenario than ever before. The more aware you are about looking for warning signs, the harder it will be for identity theft to occur.

INFO: General Identity Theft Prevention Tips

Use strong passwords. Create passwords that employ a combination of uppercase and lowercase letters, numbers, and symbols.

Lock your computer. If you are using a computer at your office or in a public place, make sure to lock it before you walk away to safeguard any personal information stored on the computer.

Double-check mailings and faxes. Always make sure that documents aren't stuck together and that the recipient's information is correct before sending any personally identifiable information. When faxing sensitive data, contact the recipient before and after the transmissions to verify that it was received by the correct person.

Use social media responsibly. Assume that anything you post online can be accessed by anyone. An identity thief can use the information he or she learns about you on social media sites to answer "challenge" questions and potentially gain access to your personal accounts. Monitor your privacy settings and consider limiting access to your page to a small number of people.

Summary

Let's sum up the key points of this topic:

- Keep your equipment with you at all times, or store your items in a secure location.
- Use VA-encrypted electronic devices that have been approved by your ISO and CIO.
- Make sure your devices are encrypted and password protected.
- Understand how public apps downloaded from public app stores are accessing other data on your VA-issued mobile device.
- Download VA-approved apps from the VA App Catalog.
- Protect yourself from identify theft.

Module 5: Using VA Systems Securely

Objectives

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

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

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

Telework Guidance

Teleworking, or telecommuting, refers to a work flexibility arrangement under which you do not commute to a central place of work every day. Instead, if you are approved to telecommute, you may work from another approved worksite, such as a home office or a telework center.

Applicable ROB

VA National: 2d(3), 2d(5)

Some software tools used when working remotely include:

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

Be sure to use all teleworking tools securely to protect VA sensitive information.

INFO: VA's Telework Policy

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

VA Form 0740 is used to establish a telework agreement. This document includes the request to telework, the employee's workplace arrangements and work schedule, and information about equipment used to telework. If you are eligible for telework, you must first complete training; this is a yearly requirement: *VA Telework Training Module for Employees* (VA TMS ID: 1367006). Then, attach your certificate of completion with the

telework agreement forms. Start by asking your supervisor for directions to complete the request.

Knowledge Check: Protecting Electronic Devices

Consider the following question.

Which of the following is a good practice to secure VA electronic devices from attack?

A. Installed full-disk encryption
B. Enable VA-approved security tools
C. Maintain positive control of the mobile device at all times
D. All of these

Answer D is correct. Protect the devices that are assigned to you. You are responsible for the care, use, and protection of these devices and the information stored on them. Never disable any antivirus or firewall protection on the device.

Remote Access

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

Applicable ROB

VA National: 2d(1), 2d(3), 2d(5), 2d(6), 2d(9)

VA Contractor: 3c

You must follow VA's national and local security policies, procedures, and configuration standards before being allowed access to any VA network. Being granted remote access capabilities means you must:

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

INFO: Remote Access

Citrix Access Gateway

Citrix Access Gateway (CAG) provides access for non-VA devices, such as personal devices or those devices used by contractors. You can also use CAG for remote access from a VA-furnished device.

Wireless Networks

You should use a hardwired connection to VA's networks whenever possible. Connecting by Wi-Fi (wireless access) can put VA at risk. If you must use a wireless connection, be sure to use VA-approved remote access and VA-approved wireless devices.

Applicable ROB

VA National: 2b(14), 2d(2), 2g(4)

VA Contractor: 3a, 3b

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.

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

INFO: Personally owned devices

Very rarely, some individuals may have approval to use personally owned devices.

Simple Actions, Big Impact: IT Inventory

In common situations like this one, your simple actions can have a big impact.

"When I moved from one VA job to another, I was surprised that I couldn't just take my VA workstation equipment, especially my monitor, with me. I guess it makes sense that IT resources stay with the department that purchased them, but I had never thought about it."

VA maintains inventory control of IT equipment. Local IT staffs conduct periodic wall-to-wall inventories. You are responsible for any equipment issued to you. Your supervisor can help you notify IT when an equipment location change is needed, whether it is due to a job change or just a move into the next cubicle.

Be on the lookout to take action. It's the VA way.

Inventory Control for Electronic Devices

Applicable ROB
VA National: 2b(16)

VA employees, contractors, and volunteers use VA electronic devices to support their work. Other examples of electronic devices include desktop computers, laptops, BlackBerry devices, Apple internet operating system (iOS) devices, Android devices, universal serial bus (USB) drives, biomedical equipment, and copy machines. Inventory control is important because it ensures VA equipment is not lost or stolen and is in the correct place.

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

- Work with your supervisor to notify your IT inventory coordinators prior to changing locations or relocating. IT equipment has to be accounted for, like all other federal property. Missing laptops, data cables, and other IT equipment means possible risk for Veterans and lost resources for VA.
- Agree to periodic electronic device inspections.
- Protect the devices that are assigned to you. You are responsible for the care, use, and protection of these devices and the information stored on them.
- Enable VA-approved security tools.

- VA-issued laptops must have full disk encryption installed and it must be operational.

Note: Some laptops that run software for biomedical devices cannot be encrypted. Since VA needs these devices to treat patients and store patient information, but placed on a separate local area network to ensure security.

INFO: Monitoring threats on medical devices

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

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

Recommendations:

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

Threats to Systems, Software, and Networks

Simple Actions, Big Impact: Safe use of Removable Media

In common situations like this one, your simple actions can have a big impact.

"Portable storage devices, like thumb drives or portable hard drives, are really convenient, but they can also cause big problems. I never, ever use a personal thumb drive at work. I never, ever use any kind of removable media to transfer data of any kind to my personal computer. It's not worth the risk to VA or Veterans."

Removable media may contain or allow access to private information. This could lead to potential loss or exposure of sensitive Veteran information. Use VA-approved portable electronic devices, which are encrypted, adding a layer of protection to your data. Never use removable media to transfer data to a personal device. VA data should only be located on VA-approved devices.

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

Applicable ROB

VA National: 2f(2)

VA Contractor: 2b(15)

Tips for protecting VA information systems:

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

INFO: Threats to Systems, Software, and Networks

Malware

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

Risks:

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

Protection Methods:

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

Phishing and Spoofing

Risks:

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

Protection Methods:

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

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

Insider Threats

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

Many people are naturally curious, but acting on your curiosity can lead to violating privacy and confidentiality. This will weaken Veterans' good faith in VA. Insiders know how a facility operates and may have access to information that they can use illegally or even sell to others. The potential for fraud increases when the opportunity is available. Avoid being caught up in an illegal scam by closely following all of the rules for handling VA sensitive information.

Help protect VA from insider threats by being aware of the ROB. Remember, if something a colleague is doing doesn't seem quite right, report it as an incident.

INFO: Insider Threats

Risks:

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

Prevention:

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

Preventing Attacks

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

Applicable ROB

VA National: 1f, 2f(1), 2f(3), 2g(5)

VA Contractor: 2b(5)

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

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

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

Knowledge Check: Identify Threats to VA Networks

Consider the following question.

Which of the following is an example of a security risk that might allow others to access and harm VA systems, software, and networks?

A. Using only VA-approved security software
B. Typing the website address instead of selecting provided links
C. Downloading a program or software from the Internet onto your VA-issued computer
D. All of these

Answer C is correct. Downloading a program or software from the Internet onto your VA-issued computer can allow others to access and expose VA sensitive information. The VA NSOC monitors all network traffic for unusual or unapproved activities.

Summary

Let's sum up the key points of this topic:

- Use VA-approved remote access tools when you access VA's network remotely.
- Use a hardwired connection to VA's network whenever possible.
- Be aware of possible threats and how to prevent them.
- Report any strange activity on your computer system to your ISO.

Module 6: Conversations and Electronic Messaging

Objectives

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

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

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

Routine Conversations

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

Conversations on the phone or in person are so common that we hardly think about them. When we're talking about a medical diagnosis or other PII or PHI, though, we need to be more aware and extra careful. Discussing patient information where you can be overheard by others is an all-too-common security incident. You must never share information with anyone whose job does not require him or her to know.

INFO: Conversations

Public areas

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

Gossip

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

Simple Actions, Big Impact: Conversations

In common situations like this one, your simple actions can have a big impact.

"It's not okay to discuss a patient's information in a public place even if a patient's name is not used."

Have you ever ridden in an elevator in a VA medical facility and overheard anyone conversing together discussing patients? They never mention names but continue to talk in great detail about the specifics of the patient's diagnosis?

Any discussion of sensitive information in a public place creates a risk. At the least, it creates a feeling that we don't care about confidentiality. A combination of facts could reveal a person's identity even if you never say a name.

Private Conversations

When you have a business reason to exchange sensitive information with coworkers, remember to speak carefully.

When having face-to-face conversations, be sure to:

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

Applicable ROB

VA National: 2b(9)

When having conversations over the phone, be sure that you:

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

Email Encryption

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

Applicable ROB

VA National: 2b(a)(11)

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

PKI works for both external and internal messaging (if the recipient also has PKI). RMS only works internally. VA-issued computers encrypt email through Microsoft Outlook. Mobile devices, such as BlackBerry phones, must have an encryption certificate or an RMS client installed, which allows the device to send and receive encrypted emails.

INFO: Encryption

PKI

You may also hear PKI referred to as S/MIME encryption. This form of encryption prevents information in email messages and email attachments from being read by people who are not authorized. It also provides authentication of the sender if the message is signed.

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

RMS

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

PKI or RMS

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

Digital signature

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

Encryption

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

- PKI S/MIME Encryption—Refer to the TMS course 1256927, *Getting Started with Public Key Infrastructure*, to learn more about PKI encryption.
- RMS Encryption—Refer to the TMS course 336914*, An Introduction to Rights Management Service—RMS*, to learn more about how to use RMS.

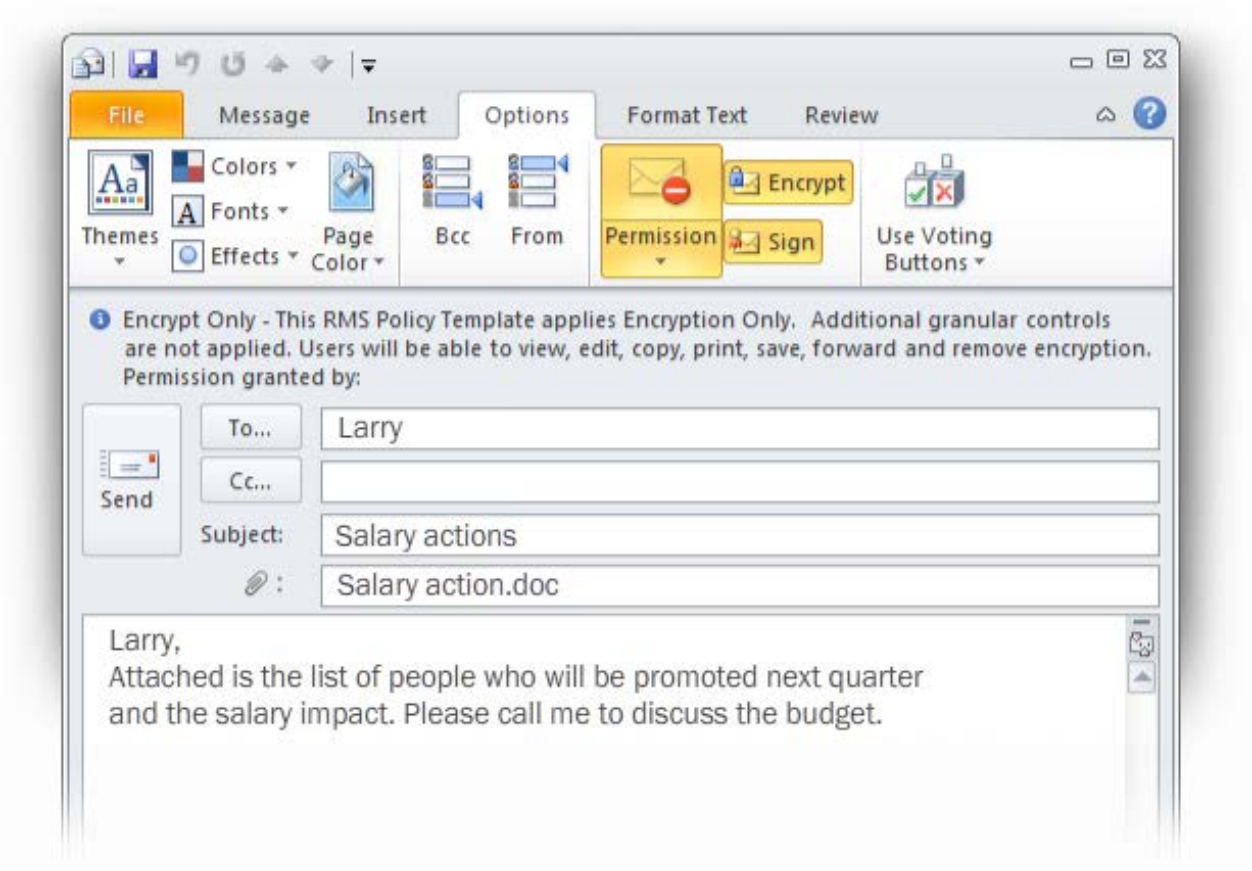
Interactive Exercise: Unencrypted Email

Electronic messages may include email, instant messages, or even calendar information and may be sent from a variety of devices.

For each email message example, determine whether the email content is secure and can be sent or if the email content is at risk and should not be sent.

Scenario 1

You're sending an encrypted email with an attachment that consists of a list of promotions and salaries to a colleague who has a need to know.



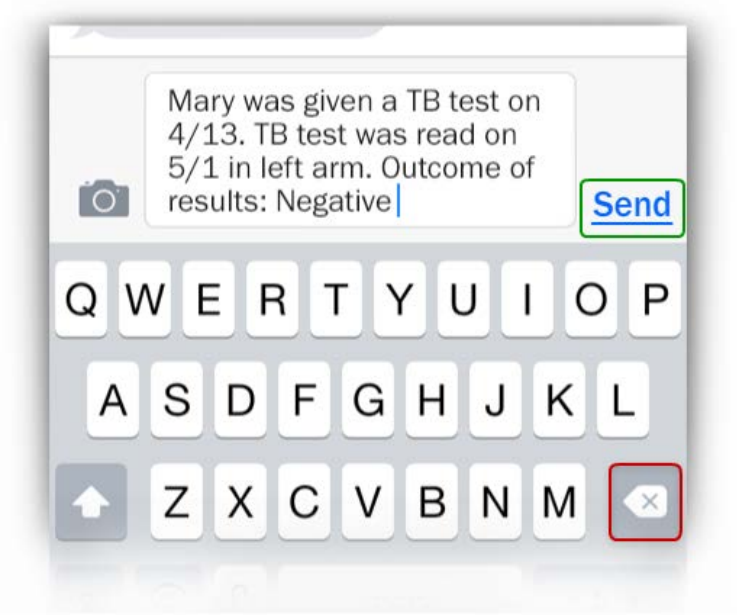
A. Send email
B. Do not send email

Answer A is correct. The information is secure; you may send this message. Because the message is encrypted, the sensitive information in the attachment is also secure. Always encrypt emails containing sensitive information.

Scenario 2

You are about to send a patient her test results in a text message from your VA mobile phone.

The text message reads:



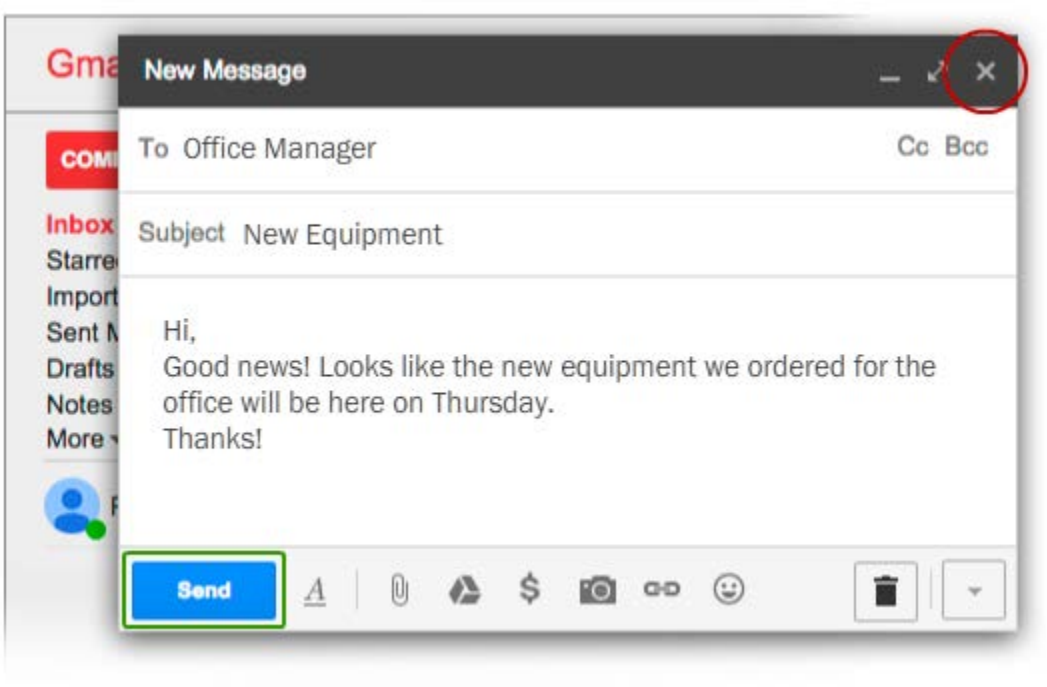
A. Send text message

B. Do not send text message

Answer B is correct. Never send VA sensitive information through text messages, as those are not protected by encryption.

Scenario 3

You have written an email using your personal email address to communicate VA business. No sensitive information is involved.



A. Send email
B. Do not send email

Answer B is correct. Do not send the email. Never send an email using your personal email address to communicate VA business. It is a violation of VA policy memorandum VAIQ 7581492, Use of Personal Email.

Secure Email Practices

Always follow these guidelines when sending emails containing VA sensitive information:

Applicable ROB

VA National: 2b(a)(10)

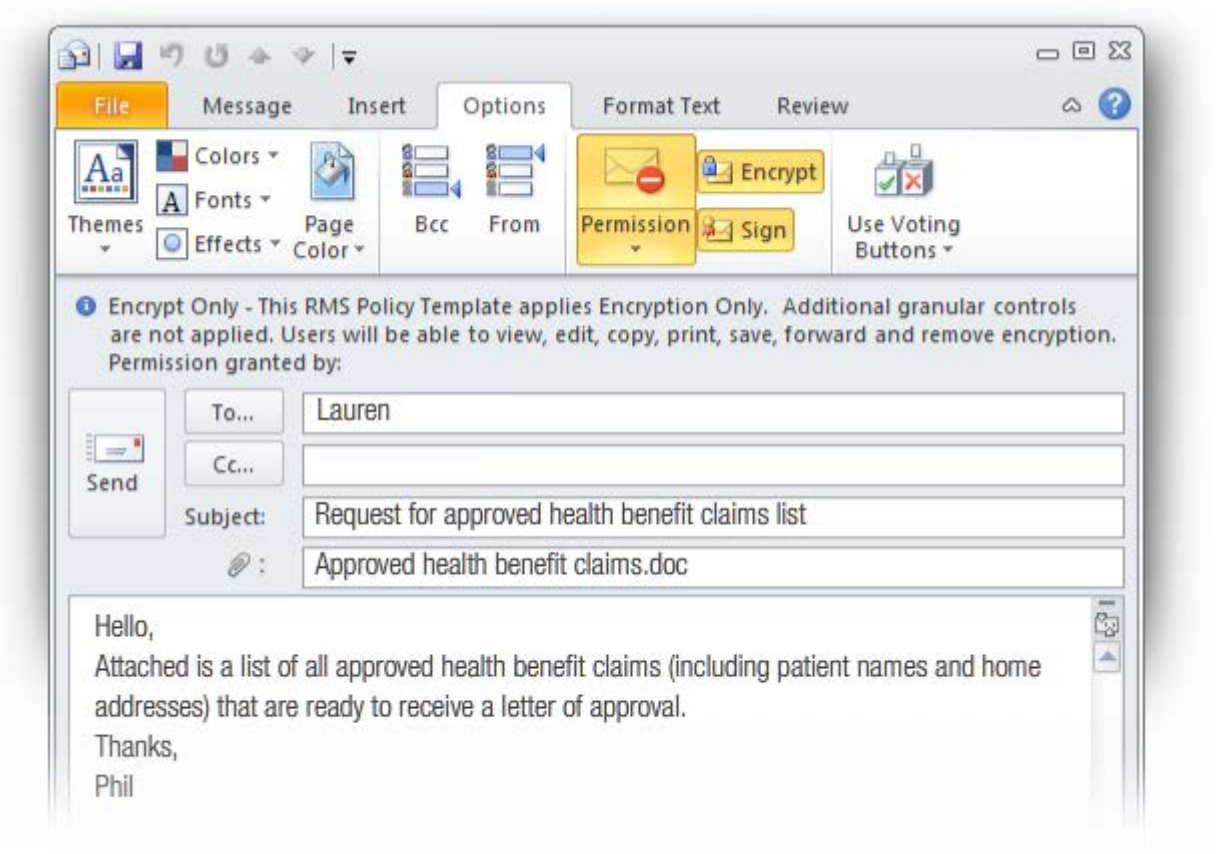
Contractor: 2b(12)

- Use encryption.
- Use RMS or PKI to make sure emails are encrypted.
- Do not include VA sensitive information in the subject line.
- Include your name and phone number on encrypted emails.
- Confirm all individuals on the distribution list are approved to receive the information.
- Consider the audience carefully before using Reply All for an email.
- Delete unnecessary emails and attachments containing VA sensitive information as soon as possible. (However, be sure to check with your supervisor before deleting or destroying emails or attachments that might be records).
- Be sure the feature to Auto Forward messages to addresses outside of VA's network is turned off.
- Do not use your personal email address to communicate about VA business. When you use VA email, a copy is kept of all emails and makes it possible for VA to keep track of business actions. Using personal email puts VA at risk of losing information or failing to keep required records.

Knowledge Check: Protecting information in Email

Review each of the three scenarios and determine if the sensitive information in each email is protected or not protected.

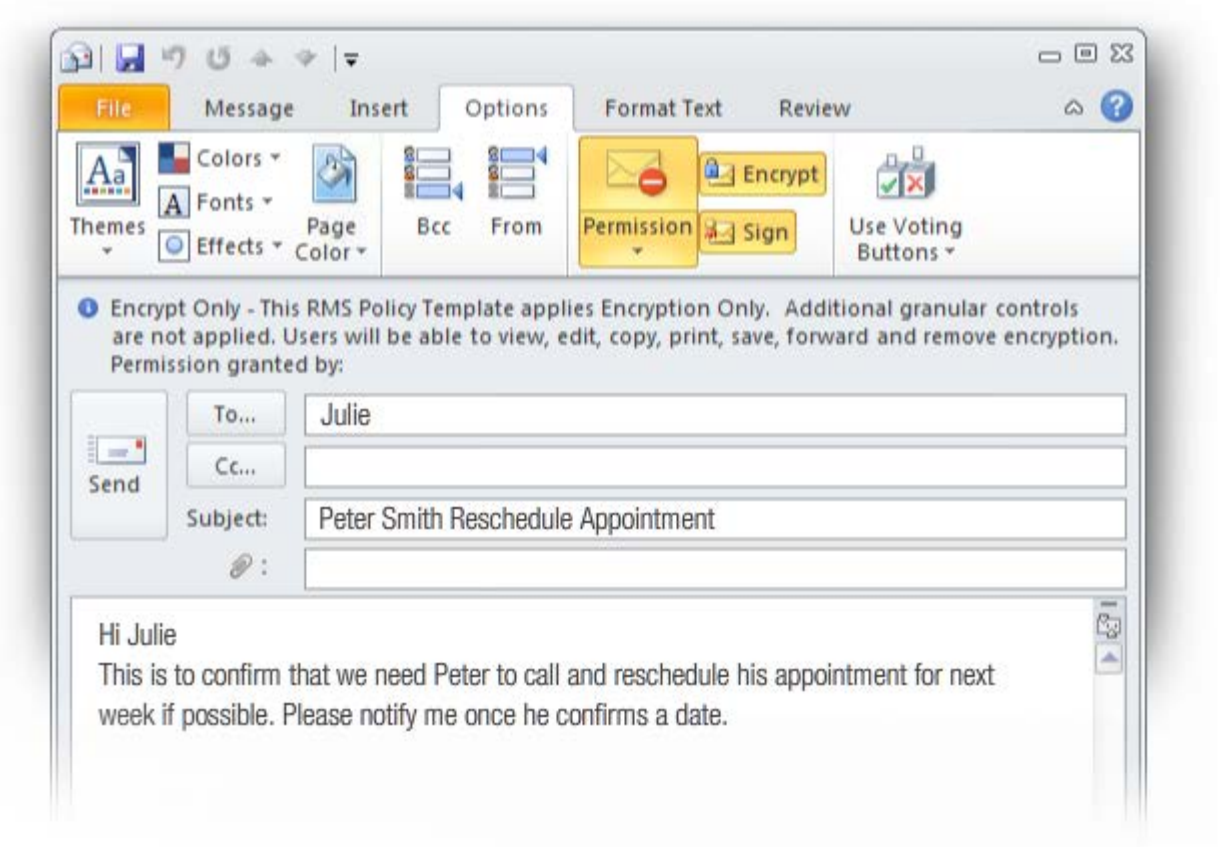
Scenario 1:



Protected or Not Protected?

The correct answer is Protected. The sensitive information in the attachment to this message is protected by encryption. When sensitive information is included in the body of an email or attached to the email, use RMS or PKI encryption to protect it.

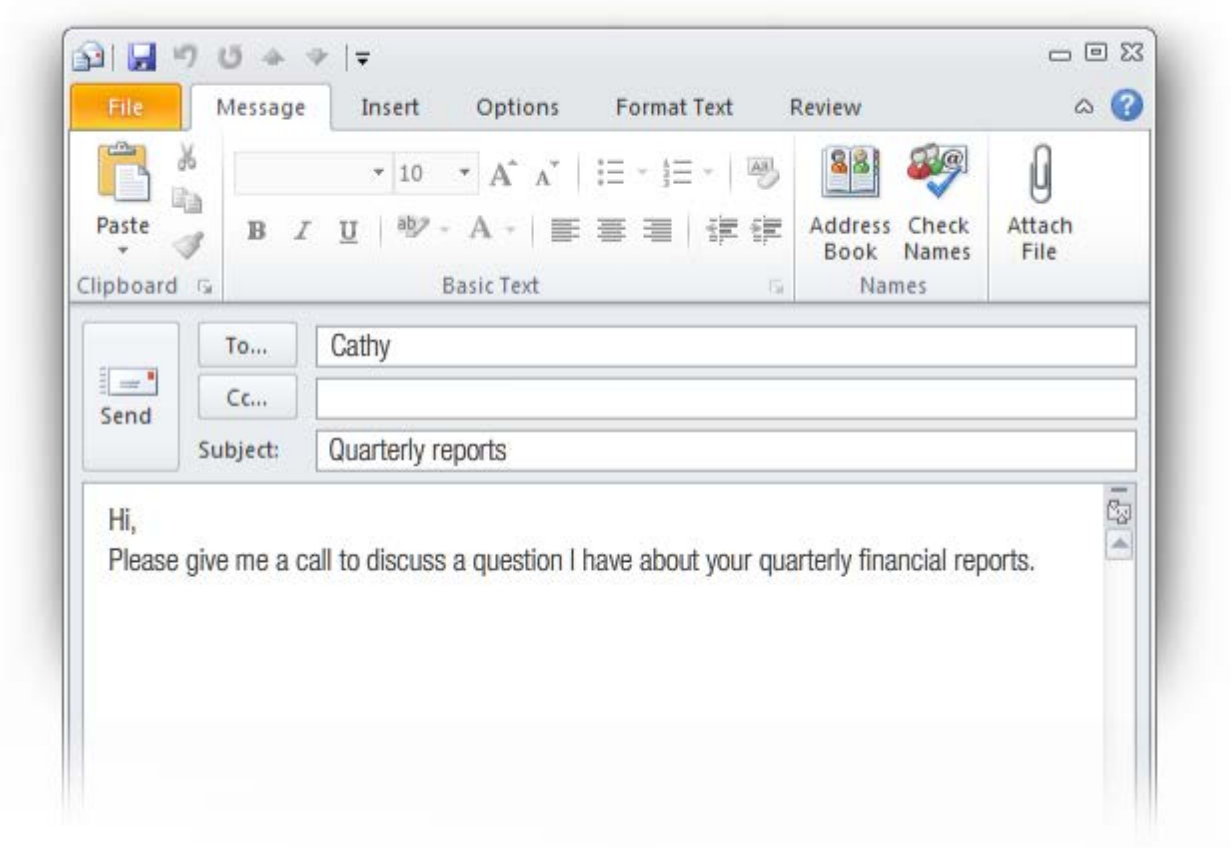
Scenario 2:



Protected or Not Protected?

The correct answer is Not Protected. In this example, even though the email is encrypted, the sensitive information that appears in the subject line is not protected. Never place a patient name or any sensitive information in the subject line of an email, because the subject line cannot be encrypted.

Scenario 3:



The correct answer is Protected. In this example, because the email does not contain sensitive information, it is already protected. Do not encrypt emails that do not contain VA sensitive information.

Electronic Calendar

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

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

Simple Actions, Big Impact: Mailing VA Sensitive Information

In common situations like this one, your simple actions can have a big impact.

"I practice due diligence to protect messages that I send whether by postal mail or email. I make sure letters are sealed before I put them in the mailbox. Email is a bigger challenge. I always encrypt emails to protect sensitive information in the content."

Unencrypted email messages can expose private information. Emailed information is more secure if it is encrypted. You must encrypt all emails that contain VA sensitive information. If encryption is not available or not supported by the recipient, find another way to communicate more securely.

Take Action. Be aware. Be secure. It's the VA way.

Summary

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

- Protect your conversations and electronic messages.
- Never include VA sensitive information in the subject line of any email.
- Never post VA sensitive information on Outlook Calendars.

Module 7: Handling Paper and Electronic Documents Safely

Objectives

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

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

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

Requirements for Documents, Files, and Federal Records in Paper Format

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

Applicable ROB

VA National: 2a(5), 2b(2), 2b(12)

Paper documents are familiar to most of us. Some examples of paper documents include printouts of letters, reports, or other content that was first created on a computer; copies made on a copy machine; handwritten notes; drawings; magazines; or photos.

A few other specialty items must also be handled as if they are paper documents, such as faxed information, x-rays, labels, or microfiche. Take some time to explore the information link to be sure you know how to handle paper items securely and prevent unauthorized disclosure.

Every facility has designated individuals who administer or oversee the VA Federal Records Program in their respective area. This role goes by many names across VA administrations. We refer to Records Liaisons in this course to describe those who have local and oversight responsibilities to insure that file plans are maintained. The Records Liaison coordinates the storage and disposition of records and provides assistance to the Organizational Records Officer with the local records program.

INFO: Best Practices

Paper documents and files

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

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

Paper records

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

Using and storing paper records

- Place a cover sheet indicating sensitive information on top of any federal records, before sending paper records to anyone. Refer to VA Directive 6609 for instructions on mailing documents or federal records containing SPI.
- Clearly mark any folders in storage boxes if they contain VA sensitive information. If you need to move federal records to off-site storage, first contact your Records Liaison. Be sure to clearly mark transfer forms (SF-135 or VA Form 0244) when moving records that contain VA sensitive information.
- Be sure federal records that are stored off-site are listed on the work center's file inventory. As long as federal records are in the legal custody of VA, Records

Officers must maintain access control and security for records with VA sensitive information in them. Coordinate with your facility Records Liaison and Privacy Officer if you are storing or handling federal records.

Destroying or disposing of paper records

- Ask your supervisor, facility Records Manager, or work center Records Liaison for guidance before you dispose of or destroy any material that may be a federal record. You can also consult VA Directive 6300 and VA Handbook 6300.1 for guidance.

Simple Actions, Big Impact: Handling Faxes

In common situations like this one, your simple actions can have a big impact.

“Faxes aren’t as common as they used to be. The best practice for VA facilities is to only use a fax to transmit VA sensitive information when a secure electronic transmission is not available. It’s too easy to mistype a fax number and send a document containing sensitive information to the wrong person.”

Before sending any fax, double-check the fax number and the content of the fax to ensure accuracy. Also, contact the recipient prior to sending the fax and after sending to verify the receipt of the fax.

Be on the lookout to take action. It's the VA way.

Faxing Paper Documents

The best practice for VA facilities is to only use a fax to transmit VA sensitive information when a secure electronic transmission is not available. If you do use fax technology, be sure to send faxes from a location that is not public, and be sure your recipient also has a secure location or someone is by the receiving machine to collect the information.

Applicable ROB

VA National: 2b(12)

Fill out a cover sheet with these four items:

- Recipient's name
- Your name and contact information
- Instructions for the recipient to verify fax receipt
- The following confidentiality statement should be used on fax cover sheets:
    - This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above. Source: VA Handbook 6500, Appendix F

Requirements for Using Mail and Delivery Services

VA sends thousands of pieces of mail to individuals and thousands of batches of form letters every week. It is a big challenge to get it right every time. Many VA facilities also have a locally approved mail system to transfer paper files among staff at the facility. Each piece of internal mail or U.S. mail must be handled with a commitment to protect sensitive information.

Applicable ROB

VA National: 2b(2)

INFO: Using mail

Here is what you can do to make sure any mail you send meets privacy and security standards.

Internal office mail services

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

Regular mail or delivery services

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

- Pack envelopes, parcels, packages, and boxes in a way that will prevent loss, tampering, or unauthorized access.
- Verify the person's name on the envelope matches the person's name on the documents inside the envelope.
- Confirm envelopes are securely sealed.
- Make sure mass-produced letters and mail merges that contain VA sensitive information are sealed prior to delivery to the approved shipping service.
- Check the recipient name and mailing address.
- Confirm that mailing labels and window envelopes show only the recipient's name and address and no other information.
- Send original documents and all media that contain VA sensitive information through a shipping service with tracking capabilities, such as USPS, UPS, or FedEx (Copies of documents containing VA sensitive information may be sent through the untracked U.S. Postal Service).

Interactive Exercise: Handling Paper and Electronic Documents

For each of the following scenarios, consider whether information is secure or at risk as you are handling paper and electronic documents.

Scenario 1 of 3:

You arrive early to a meeting and enter the conference room. You notice that someone has left several reports that look like they contain sensitive information on the table.

Secure or at risk?

The information is at risk. Do not leave sensitive information unattended in areas such as public spaces, private offices, conference rooms, copy or fax machines, mailboxes, or wall trays.

Scenario 2 of 3:

I need to get rid of these paper records today. I'll make sure I throw them away properly when I get home.

Secure or at risk?

The information is at risk. Ask your supervisor, facility Records Manager, or work center Records Liaison for guidance before you dispose of or destroy any material that may be a federal record. Never remove VA records from a VA facility without your supervisor's approval.

Scenario 3 of 3:

I need to leave early. I'll take care of these letters to three patients tomorrow. I'll leave them on my desk so that I don't forget where I stopped. Nobody ever bothers my cubicle.

Secure or at risk?

The information is at risk. Maintain a clean desk policy where you ensure you do not leave VA sensitive information unattended on your desk during the day or when you leave for the day.

Paper Logbooks

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

Applicable ROB

VA National: 2b(6), 2b(15)

VA Contractor: 2b(14)

Keep this guidance in mind:

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

Electronic Media and Electronic Storage

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

Applicable ROB

VA National: 2b(8), 2b(15)

VA Contractor: 2b(11)

Be sure to also consult your Records Officer before disposing of any electronic media, media storage, or electronic information systems that may be records. Records may not be destroyed before the date noted in the RCS. Never destroy records without permission. All types of electronic media, storage, or systems that may contain VA sensitive information must be sanitized or destroyed when no longer in use. Ask your ISO for help with the sanitization and disposal or redistribution of electronic media. Here are some examples of these items:

- Electronic media: Emails; Excel and Access spreadsheets; JPEG, TIF, and HTML files; flat files; Word documents; PDF documents
- Electronic media storage: Magnetic tapes, floppy disks, CDs/DVDs, and external hard drives
- Electronic information systems: VistA/CPRS, Concur Government Edition (CGE)

Transporting VA Sensitive Information

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

Applicable ROB

VA National: 2b(3), 2d(7), 2d(8)

VA Contractor: 2b(10)

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

Knowledge Check: Transporting VA Sensitive Information

Consider the following question.

You must get written permission from your supervisor, CIO, and ISO before you can ____ any VA sensitive information from a VA facility or office.

A. Use
B. Remove
C. All of these

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

Microsoft SharePoint®

VA has approved Microsoft SharePoint® for you to use for online data storage and collaboration. SharePoint is found on the VA Intranet. Your ISO, CIO, and PO can help you determine which types of information can be shared on specific SharePoint sites.

Applicable ROB

VA National: 2b(7), 2b(13), 2c(5), 2g(2)

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

- Share VA sensitive information only on sites where access is limited to individuals approved to access the information.
- Get access to only the sites you need to do your job.
- Share only the information your work unit needs to share to do its job.
- Protect records stored on SharePoint in these ways:
    - List the SharePoint sites in the work unit's file inventory.
    - Ask your facility Records Officer to schedule the disposition of these records, if they are unscheduled.
    - Consult with the facility Records Officer prior to destroying any record in SharePoint.

Summary

Let's sum up the key points of this topic:

- Protect paper files and prevent unauthorized disclosure when sending faxes, interoffice mail, and regular mail.
- Do not keep unauthorized paper logbooks.
- Store, transport, or dispose of records according to VA-approved methods and according to your unit's RCS.

Module 8: Course Summary and Rules of Behavior

Course Summary

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

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

Acknowledge, Accept, and Comply with the ROB

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

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

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

Instructions for Signing the Rules of Behavior

Before you complete the signature step, first identify whether you are a user or a contractor, then print the appropriate ROB document (Appendix A: VA National Rules of Behavior for VA Employees [Users who are not contractors] or Appendix B: Rules of Behavior for VA Contractors).

To acknowledge and accept the ROB:

- Initial each printed page with your initials where indicated
- Sign the last page of the document where indicated.

VA Employee (User who is not a contractor)

See Appendix A to print, review, initial, and accept the VA National Rules of Behavior.

Before you complete the signature step, make sure you are selecting the correct ROB. Remember, these rules are for you if you are a user who is NOT a contractor, such as any of the following: a VA employee who works for VA under Title 5 or Title 38, United States Code; a volunteer; a without compensation (WOC) employee; a student or other trainee.

Contractor ROB

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

Applicable ROB

VA National: 1a, 1i, 1j, 3a, 3b

VA Contractor: 5

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

Submitting Your Signed ROB

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

- If you are a VA employee (User who is not a contractor) and signed the VA National Rules of Behavior, provide the signed copy to your supervisor.
- If you are a VA contractor and signed the Contractor Rules of Behavior, provide the signed copy to your COR.

Course Completion

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

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

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

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

I. APPENDIX A: Department of Veteran Affairs National Rules of Behavior

Department of Veteran 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 U.S. Department of Veterans Affairs (VA) information or information systems.

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 they contain or that may be accessed through them, as well as the security and protection of VA information in any form (e.g., digital, paper, verbal).

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 Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (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, and suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

Initials _____

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 Privacy Officer (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; Information System Owner, local Chief Information Officer (CIO), or designee; 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 Rules of Behavior (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 in 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 provides 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 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, POs, 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 information.

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

Initials _____

(5) I understand VA's system of records may contain Confidential Medical Information that relates to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or sickle cell anemia. I will not disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority as outlined in applicable federal laws and regulations, including 38 U.S.C. § 7332. I understand my responsibilities as outlined in 38 U.S.C. § 7332, and I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals.

b. Data Protection

(1) I will safeguard electronic VA sensitive information at work and remotely. I understand that all VA owned mobile devices and portable storage devices must be encrypted using Federal Information Processing Standards (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 Deputy Assistant Secretary for Information Security (DAS for OIS). This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)).

(2) I understand that per VA Directive 6609, Mailing of Sensitive Personal Information (SPI), the following types of SPI 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 his or her personal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization contact person). 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 when sent to a person or entity that does not have the capability of decrypting the data, provided that the mailing is approved in advance and in writing by my supervisor or ISO.

Initials _____

(3) I understand that I must have approval from my supervisor to use, process, transport, transmit, download, or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or regional offices)).
(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. VA owned and approved storage devices/media must use VA's approved configuration and security control requirements. The Information System Owner, local CIO, or designee, and ISO and PO must review and authorize the mechanisms for using, processing, transporting, transmitting, downloading, or storing VA sensitive data outside of VA owned or managed facilities.
(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, whether regional-level 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 record retention requirements. Two secure options that can be used are to utilize a cross-cut shredder that meets VA and National Institute of Standards and Technology (NIST) 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 devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)).

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

(11) I will not auto-forward email 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 secure location.

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use encryption products approved and provided by VA to protect sensitive data. I will 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, ISO, and/or Information System Owner, local CIO, or designee before providing any access.

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

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

(16) I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized Office of Information and Technology (OI&T) employee.

c. Logical Access Controls

Initials _____

(1) I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor, ISO, and/or Information System Owner, local CIO, or designee when the access is no longer needed.
(2) I will only use 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 not share my password or verify codes. 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 by my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee.
(4) I am responsible for the security of VA property and information, regardless of my work location. VA security policies are the same and will be enforced at the same rigorous level when I telework as when I am in the office. I will keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information.

Initials _____

(5) I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information are adequately secured in remote locations (e.g., at home and during travel). I agree that if I work from a remote location, pursuant to an approved telework agreement with VA sensitive information, authorized OI&T personnel may periodically inspect the remote location for compliance with security requirements.
(6) I will protect information about remote access mechanisms from unauthorized use and disclosure.
(7) I will notify my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee 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.
(9) I understand that VA prohibits access to VA's internal network from countries that pose a significant security risk. I will therefore not access VA's internal network from any foreign country designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner. This prohibition does not affect access to VA external web applications.

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 authorized in advance by my VA supervisor, ISO, and Information System Owner, local CIO, or designee. 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. I will follow VA Handbook 6500 requirements for connecting any non-VA equipment to VA's network.
(3) I will not use personally-owned information systems (capable of storing data) on-site at a VA facility to directly connect to VA's network. I will not use personally-owned information systems on-site to perform assigned official duties unless approved by the Information System Owner, local CIO, or designee. I will obtain my Information System Owner, local CIO, or designee's approval prior to using remote access capabilities to connect personally-owned equipment to VA's network while 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 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 OI&T 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 by my Information System Owner, local CIO, or designee and approved by my ISO. I will ensure that all such activity is in compliance with Federal and VA policies.
(5) I will not attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data.
(6) I will only use my access to VA computer systems and/or records for officially authorized and assigned duties. The use must not violate any VA policy regarding jurisdiction, restrictions, limitations or areas of responsibility.
(7) I will use my access under VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology, understanding that this Directive does not pertain to accessing VA applications or records. I will not engage in any activity that is prohibited by the Directive.
(8) I will prevent unauthorized access by another user by ensuring that I log off or lock any VA computer or console before walking away or initiate a comparable application feature that will keep others from accessing the information and resources available in my computing session.

Initials _____

h. Miscellaneous

(1) I will complete mandatory periodic security and privacy awareness training within designated time frames, 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 OI&T 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.

(5) If as an Other Federal Government Agency employee, I cause any level of data breach, I understand it may result in disciplinary or other adverse action, as well as criminal or civil penalties; and I recognize that I will be required to complete VA's security and privacy awareness training as part of incident remediation measures.

3. ACKNOWLEDGEMENT AND ACCEPTANCE

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

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

_____ _____

Print or type your full name Signature Date

_____ _____

Office Phone Position Title

II. APPENDIX B. Rules of Behavior for Contractor

CONTRACTOR RULES OF BEHAVIOR

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

1. **GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS and ACTIVITIES UNDER THE CONTRACT:**
    a. I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.
    b. I consent to reviews and actions by the Office of Information & Technology (OI&T) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.
    c. I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OI&T, VA, and law enforcement personnel.
    d. I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal government systems; deny access to Federal government systems; accrue resources for unauthorized use on Federal government systems; or otherwise misuse Federal government systems or resources are prohibited.
    e. I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

Initials _____

f. I agree that OI&T staff, in the course of obtaining access to information or systems on my behalf for performance under the contract, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers (ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.
g. I understand I must comply with VA's security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer's Technical Representative (COTR). If the contractor believes the policies and guidance provided by the COTR is a material unilateral change to the contract, the contractor must elevate such concerns to the Contracting Officer for resolution.
h. I will report suspected or identified information security/privacy incidents to the COTR and to the local ISO or Privacy Officer as appropriate.

2. GENERAL RULES OF BEHAVIOR

a. Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job.
b. The following rules apply to all VA contractors. I agree to:
    1. Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the contract.
    2. Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.
    3. I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the contract. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.
    4. Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the contract.

Initials _____

5. Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the contract or at the direction of the COTR or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not confer me unrestricted access or use, nor the authority to bypass security or other controls except as expressly permitted by the VA CIO or CIO's designee.
6. Contractors' use of systems, information, or sites is strictly limited to fulfill the terms of the contract. I understand no personal use is authorized. I will only use other Federal government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal law still apply.
7. Grant access to systems and information only to those who have an official need to know.
8. Protect passwords from access by other individuals.
9. Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.
10. (Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA.
11. Follow VA Handbook 6500.1, Electronic Media Sanitization to protect VA information. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders.
12. Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.
13. Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.

Initials _____

14. Not host, set up, administer, or run an Internet server related to my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA unless explicitly authorized under the contract or in writing by the COTR.
15. Protect government property from theft, destruction, or misuse. I will follow VA directives and handbooks on handling Federal government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the COTR.
16. Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with VA.
17. Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated with my performance of services under the contract terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the COTR.
18. Understand that restoration of service of any VA system is a concern of all users of the system.
19. Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

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

a. When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.
b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.
c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.
d. I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given contract or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same. Initials_____

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

4. STATEMENT ON LITIGATION

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

5. ACKNOWLEDGEMENT AND ACCEPTANCE

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

_____

[Print or type your full name] Signature

_____

Last 4 digits of SSN Date

_____

Office Phone Position Title

_____

Contractor's Company Name

Please complete and return the <u>original</u> signed document to the COTR within the timeframe stated in the terms of the contract.

III. APPENDIX C: Glossary

A

Application (App)—A software program hosted by an information system. Source: NIST SP 800-137

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

B

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

C

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Contractors—See User. Individual or (system) process acting on behalf of an individual, and authorized to access an information system. SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009
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 information or VA information systems, these individuals must complete VA-approved security and privacy awareness training, sign the VA National ROB or Contractor ROB, and complete appropriate background screening before such access may be granted. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

D

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

b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at same facility.

c. Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person. SOURCE: 45 C.F.R. § 164.402

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Disclosure—The act of making VA knowledge or facts known. Disclosure is to reveal or share information. At VA, the Principle of Disclosure requires that "VA personnel will zealously guard all personal data to ensure that all disclosures are made with written permission or in strict accordance with privacy laws." Source: VA Directive 6502

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

E

Employees—See User. Individual or (system) process acting on behalf of an individual, and authorized to access an information system. SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009
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 information or VA information systems, these individuals must complete VA-approved security and privacy awareness training, sign the VA National ROB or Contractor ROB, and complete appropriate background screening before such access may be granted. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Encryption—The process of changing plaintext into ciphertext for the purpose of security or privacy. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

F

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Federal Information Security Management Act (FISMA)—A law that requires VA to have an information security program. Title III of the E-Government Act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Source: NIST SP 800-63

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Federal Records Act—A law that requires VA to maintain a system of records. The Federal Records Act requires federal agencies to make and preserve records that have adequate and proper documentation of their organizations, functions, policies, decisions, procedures, and essential transactions. These records are public property.

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

G

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

H

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

These broad new requirements will necessitate compliance by covered entities, business associates, and related vendors in the health care industry. Source: http://www.nixonpeabody.com/publications_detail3.asp?ID=2621

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

I

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Information security—A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

J—N/A

K—N/A

L—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

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.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

N

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

O—N/A

P

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

PKI complies with all federal and VA security policies and is the accepted Global Business Standard for Internet Security. As an added benefit, PKI can provide the functionality for digital signatures to ensure document authenticity. Source: http://www.va.gov/pivproject/

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Personally Identifiable Information (PII)—Any information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security number, biometric records, etc., alone or when combined with other personal or identifying information, 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 PII. (See Sensitive Personal Information, below). Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Phishing—Efforts to steal personal data. Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means. Source: NIST SP 800-83

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Privacy Impact Assessment (PIA)—An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

copyrighted, or trademarked property beyond fair use, proprietary data, or export-controlled software or data. Source: VA Directive 6001

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Protected Health Information (PHI)—Individually identifiable health information held by a covered entity or by a business associate acting on its behalf. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. §§ 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer. Within VA, VHA is the only covered entity. Certain other VA components, such as OI&T, are business associates of VHA. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Public Key Infrastructure (PKI) encryption—An architecture that is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

R

Records—Records are defined by 44 U.S.C. as all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them (see 44 U.S.C. Ch. 33, Sec. 3301).

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Records Control Schedule (RCS)—A 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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Remote access—Access by users (or information systems) communicating externally to an information system security perimeter. SOURCE: NIST SP 800-18
Remote access uses telecommunications to enable authorized access to non-public VA computing services that would otherwise be inaccessible from work locations outside a VA local area network (LAN) or VA-controlled wide area network (WAN) computing environment. Remote access includes access to non-public VA Information Systems and data that are exposed to the public Internet (e.g., web access to electronic mail [email] by the home user or business traveler) as well as modem, dial-up, and/or Virtual Private Network (VPN) access to internal VA IT servers and desktop workstations. Source: VA Handbook 6500

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

S

Sensitive Personal Information (SPI)—The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i)

education, financial transactions, medical history, and criminal or employment history; (ii) information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records. NOTE: The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information."

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

T

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

TITUS toolbar—TITUS Classification for Microsoft Office is a security and governance solution that enables organizations to ensure consistent and proper handling of their Microsoft Office documents. With a wide range of customizable functionality, this solution can force users to easily identify the sensitivity of every document, warn users of policy violations, and scan message content for PII and other sensitive information.

The user's classification selection is stored with the Office document as persistent metadata, which organizations can use to increase the accuracy and effectiveness of data loss prevention (DLP), archiving, and perimeter security solutions. Source: http://www.titus.com/software/document-classification/index.php

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

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

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

U

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

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.

V

VA Pulse—VA Pulse is a collaboration platform that connects people and ideas across VA. It is open to anyone with a VA.gov email address. Use it to, find the information you need, connect with colleagues to solve problems, share best practices, streamline your

workflow. Sort of a combination of Facebook and LinkedIn specifically built for and fully supported by VA. Note: VA Pulse new social media tool replaces Yammer. Source: VAPulse.net To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

VA sensitive information/data—All Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions. SOURCE: 38 USC § 5727. NOTE: The term “Personally Identifiable Information” is synonymous and interchangeable with “Sensitive Personal Information.”

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

W—N/A

X—N/A

Y

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

Source: PCMag.com Encyclopedia

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

YouTube—The name of a website on which users can post, view, or share videos. Source: Youtube. (n.d.). Dictionary.com Unabridged. Retrieved May 26, 2015, from Dictionary.com

To return to your place in the main document after selecting a hyperlink to an item in the appendix, select Alt + <left arrow> on your keyboard.

Z—N/A

IV. APPENDIX D. Privacy and Information Security Resources

Table 1: VA Phone Numbers
Office of Inspector General (OIG) 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
FSS HISD SharePoint site for MDPP guidance* https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/HISD.aspx
Information Security Portal* https://vaww.portal2.va.gov/sites/infosecurity/index.aspx

Table 2: VA Web Links
ITWD's Role-based Training* http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Pages/default.aspx
Locator to identify ISOs* https://vaww.portal2.va.gov/sites/infosecurity/ISO-PO-Locator/default.aspx
Locator to identify POs* https://vaww.portal2.va.gov/sites/infosecurity/ISO-PO-Locator/Privacy%20Officers/Forms/AllItems.aspx
PIV cards http://www.va.gov/PIVPROJECT/index.asp
Remote access solutions* https://vpnportal.vansoc.va.gov/Default.aspx?strSource=u+ICXXnt3TlrIVosSsqAABgrAfO5euqrcalEYQjZ0d7TQ+n8hKoNYUEUKNucaA2wE7Cdxa4vj6MmCL1waoAFIw
Rights Management Service (RMS)* http://go.va.gov/o2ip
Role Definitions PDF document* http://vaww.infoshare.va.gov/sites/ittrainingacademy/rbt/Shared%20Documents/Role%20Definitions.pdf

*These links are only accessible on the VA Intranet

Table 3. VA TMS Courses
Available at: https://www.tms.va.gov
TMS ID 10203, Privacy and HIPAA Training
TMS ID 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
TMS ID 3858544, Social Engineering—Hacking Human Nature
TMS ID 3926743, Mobile Training: Apple Native Email Client
TMS ID 3926744, Mobile Training: Security of Apps on iOS Devices

Table 4. Privacy Laws and Regulations
Available at: http://www.privacy.va.gov/privacy_resources.asp
Freedom of Information Act (FOIA) 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 Statues/ 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.

Table 5. Information Security Laws, Regulations, and Related Statues/ Specifications
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-2010-title38/pdf/USCODE-2010-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-2011-title38/pdf/USCODE-2011-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

Table 6. Selected VA Privacy Handbooks and Directives
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 Security and Privacy Incidents
VA Handbook 6502, VA Enterprise Privacy Program
VA Handbook 6502.4, Privacy Act Review
VA Handbook 6512, Secure Wireless Technology
VA Handbook 6609, Mailing of Personally Identifiable and VA Sensitive Information
VHA Directive 1605, VHA Privacy Program
VHA Handbook 1605.1, Privacy and Release of Information
VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information

Table 7. Additional Selected VA Handbooks and Directives
Available at: 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

Table 7. Additional Selected VA Handbooks and Directives
VA Handbook 5021.3, Employee/Management Relations
VA Handbook 5021.6, Employee/Management Relations, Appendix A
VA Handbook 6300.1, Records Management Procedures
VA Handbook 6500, Appendix F, VA Password Management
VA Handbook 6500.6, Contract Security and Appendix D, Contractor Rules of Behavior

Table 8. Forms and Memorandum
Available at: http://www1.va.gov/vapubs/index.cfm
VA Form 0244, Records Transmittal and Receipt
VA Form 0740 New Telework Request Agreement, Aug 2013
VA Form 7468, Request for Disposition of Records
VAIQ 7581492, Use of Personal Email
VAIQ 7633050, Mandatory Use of PIV Card Authentication for VA Information System Access