VA Privacy and Information Security Awareness and Rules of Behavior

Text-Only Course Transcript

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

Contents

Course Background

Privacy and information security laws require annual training for federal employees and others who use federal information systems. This course satisfies the annual training requirements of the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA).

The course provides an overview of:

- Privacy and security legal requirements and penalties
- Common situations where privacy and security are at risk
- How to report an information security or privacy incident.

At the end of this course, you must review and sign the National Rules of Behavior.

Purpose of This Document

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

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

You should take the online version of this course if possible. If you complete the course using this text-only document, you will need to coordinate with your supervisor and local Talent Management System (TMS) Administrator to ensure you receive credit for completion.

Welcome

A Social Network Nightmare (Fictional Scenario)

A young medical receptionist, Melanie, is talking to a Veteran patient, Trevor. Trevor is being discharged.

> *Melanie:* Hey, it was good to see you again. And I know that you'll get better soon. I'll come and visit you when I'm off my weekend shift.
>
> Trevor avoids making eye contact and walks away.
>
> Melanie takes out her smart phone and begins to craft a message for her Social Network post.
>
> *The war doesn't end when our Vets come home. Just found out about a friend recovering from a service-related injury. My heart is with you, Trevor. #Honor Vets*
>
> Melanie posts the message to her Valley High Class of 2003 group. Messages from Melanie's friends begin to appear.
>
> *Ronnie posts: Hey Trevor, just read Mel's post. I had no idea. Give me a call.*
>
> *Jennifer posts: Are you doing alright, Trev?*
>
> *Mike posts: My Army buddy dealt with service-related injury when he returned too. Be strong.*
>
> *Trevor reviews his Social Network site and notices the posts from Ronnie, Jennifer, and Mike. Trevor is embarrassed and upset. He begins to wonder…"I knew that coming here for treatment was a bad idea…now everyone knows."*

Melanie violated one of VA's privacy and information security rules: Protected Health Information (PHI) must never be shared on any social networking site.

The Stories You're About to Read

Welcome to the Annual Privacy and Information Security Awareness and Rules of Behavior Training. This course is required for all employees, students, volunteers, and contractors who access VA information and information systems.

The story you've just read and the stories you are about to read are fictional examples of situations you face every day at VA, situations in which information and information systems are at risk.

The heroes in our stories prevent mistakes in these common situations. You might call them Everyday Heroes.

If you look around at your co-workers, you'll see many people doing the right thing, and you'll discover situations where you can help each other do better. Every time you do the right thing, you're somebody's hero, every day. This course will help you remember *what* information must be protected at VA and *how* you protect information and information systems. Please note, VHA personnel are also required to complete a more detailed privacy course.

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

- Recall your five privacy and information security responsibilities
- Recognize privacy and information security legal requirements, consequences, and penalties
- Recognize actions required in common situations to protect sensitive information; protect computers and IT equipment; and protect systems, software, and networks
- Recognize how to report privacy and information security incidents
- Sign and comply with National Rules of Behavior.

Your Five Responsibilities

Everyday Hero to the Rescue: Part 1 (Fictional Scenario)

It's Monday around lunchtime, and Harold and Maria are sitting in their desks at a VA Field Office. Harold is on his lunch break reading about the latest superhero film on the Internet. Maria is working at her desk in front of a computer on the opposite side of the office. Harold wheels his chair over to Maria to have a conversation.

> *Harold:* Maria, only a few more days before the movie comes out. Aren't you excited?
>
> *Maria laughs:* Sure, whatever.
>
> *Harold:* So you're going though, right?
>
> *Maria:* No, I have more exciting things to work on.
>
> *Harold:* What?
>
> *Maria:* I just received the patient data that I've been expecting for my research.
>
> *Harold:* OK, that's exciting.
>
> *Maria:* It is! I just can't wait to get started. I've been waiting for this data for months. In fact, I was just about to send some files to my home email account so that I can get started tonight…
>
> *Harold looks a bit concerned. He begins to wonder…"I know she means well…but should Maria really be sending this information to her home email account?"*

Harold knows that Maria's excitement may lead to a security incident. VA policy prohibits sending sensitive information to a personal email account.

We'll check back with Harold and Maria later.

Objectives

At VA, you review privacy and information security requirements every year because it's important to protect Veterans and employees by following the rules. And most of you are doing a great job—most of the time. But let's face it—there are a lot of rules!

In this topic, you will review privacy and information security requirements, along with a few tips and tools to help you recall the information. You will also practice choosing the right action in different situations.

In this topic, you will learn how to:

- Identify five types of requirements
- Recognize the legal requirements of privacy and information security
- Define privacy
- Define information security
- Define sensitive information and related special terms.

Five Heroic Requirements
With so many Rules of Behavior, how can you remember them all? Remember privacy and information security requirements by thinking of them as five types of responsibilities—or a hero's five requirements.

- Protect sensitive information
- Protect computers and other IT equipment
- Protect IT systems, software, and networks
- Report incidents
- Sign and comply with the Rules of Behavior

What the Law Requires
Working for VA means you must understand and meet a variety of strict legal requirements. It comes with the territory. This course meets annual training requirements of several laws. Some laws address data privacy and information security in general and others address specific types of data, the way data is stored, or the way data is transmitted. You should have a general understanding of how to comply with them while performing your job. Complying with these laws will help you prevent harm to Veterans, VA employees, or VA and help you to avoid consequences or penalties for failing to comply.

This course satisfies annual training requirements and focuses on the responsibilities required by:

- The Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA)

- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Federal Information Security Management Act (FISMA)
- Federal Records Act
- Freedom of Information Act (FOIA)
- VA Confidentiality Statutes (38 U.S.C. 5701, 5705, 7332)
- Internal Revenue Code (IRC).

Review the Resources and Glossary sections in the Appendix of this document for more information on these laws and regulations.

The Privacy Act of 1974
The Privacy Act requires the Federal Government to say why information is being collected about people and how it is being used. The Act also defines when information about an individual can be disclosed without the person's consent and when the person's consent is required. By law, federal agencies must keep sensitive information confidential. For more information about technical requirements, contact your Privacy Office. Get to know the special meaning of the terms used by these laws, so you can do what's required.

VA sensitive information (as defined in VA Handbook 6500) is an important term describing several types of protected information, including: personally identifiable information (PII), protected health information (PHI), and other regulatory or program-specific information that is used by VA to do business. These terms will be discussed in more detail later in the course.

The Health Insurance Portability and Accountability Act (HIPAA) establishes requirements for protecting privacy of personal health information. The privacy rule under HIPAA concerns health plans, health care providers, and health care clearinghouses that may use or disclose individually identifiable health information. The HIPAA privacy rule applies only to covered entities as defined by the act. VHA is the only covered entity within VA.

Title 38 U.S.C. statutes state requirements for protecting confidentiality of PII and PHI in certain situations:

- For all VA claims information (5701)
- For information generated during VA medical quality assurance efforts (5705)

- For VA records of the identity, diagnosis, prognosis, or treatment of any VA patient relating to drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or Sickle Cell Anemia (7332)

The Internal Revenue Code (IRC) requires protection of individuals' income tax returns provided to VA electronically under agreements with other federal agencies. Be aware that disclosing tax return information without the permission of the individual carries severe penalties (IRC Sections 7213 and 7431, regarding unauthorized disclosure of returns and other information).

Federal Information Security Management Act of 2002
FISMA requires everyone to be careful with information you use or come in contact with on your job. Federal agencies must protect information and information systems because they are assets used to do the work of the Federal Government. Remember that the information you work with every day in your job is a resource that belongs to VA. Use information resources responsibly to support Veterans.

Agencies must protect the confidentiality, integrity, and availability of sensitive information. You can remember these requirements by the familiar letters CIA:

- C = Confidentiality. Protect information about individuals that is PII and do not disclose VA's confidential regulatory or program-specific information.
- I = Integrity. Ensure VA sensitive information or data isn't damaged and don't make changes to data unless that is a responsibility of your job.
- A = Availability. Prevent situations that would cause VA sensitive information or VA information systems to become unavailable (e.g., disposing of records improperly or causing a network to crash).

Records Management Laws
Records management laws require you to be careful how you collect and store information in records. The laws mandate what you must do with records after they are no longer needed in your daily work.

The Federal Records Act, the Government Paperwork Reduction Act, and the Freedom of Information Act (FOIA) support the right of individuals to have access to their information. These laws also permit individuals in specified circumstances to access other information collected and maintained in records by federal agencies.

The word “records” has a special meaning. In general, the Records Act describes records as the various kinds of official evidence—sometimes called artifacts—that federal agencies must maintain to document their policies, decisions, procedures, operations, and other activities. Records may be in any format (e.g., paper, digital or electronic data, audio recording, and video recording). The Privacy Act describes records as “any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”

FOIA states the circumstances in which individuals can request copies or view federal records and circumstances under which personal information can be withheld from release to others. Follow procedures for FOIA and Privacy Act information requests.

As a VA employee, you may receive a written request for records or other information. If the request originates from outside of VA, report it to your supervisor and alert the local or regional FOIA officer or Privacy officer. Find your FOIA Officer at this link: www.FOIA.va.gov/FOIA_Contacts

Protecting Sensitive Information in Records

Records must be handled in a way that protects any sensitive information that may be included. Ask your supervisor to clarify how records are handled in your office to protect sensitive information. Here are some examples of handling records:

Records management is an administrative process for creating, using, storing, retrieving, and disposing of records.

Every office in VA is required to identify which documents are considered official records. Each office must also have an approved Records Control Schedule identifying where records are located and when and how to dispose of them.

Records may be disposed of in only three ways: temporary storage within the work unit or at a regional facility, permanent storage (coordinated through the National Archives for items of historic significance), and destruction.

Documents containing PII must be handled confidentially and securely when transported to storage or when being destroyed. Always ask your supervisor or office

records administrator for guidance before you dispose of or destroy any material that may be a record.

Mistakes and Consequences
Even if you never look at any documents or sensitive information as part of your job, you can make big mistakes. Think about how you could harm VA and Veterans if you don't uphold these laws. Whenever privacy or information security policies or laws are violated, there can be extremely unfortunate consequences for Veterans, VA, and you.

- **For Veterans.** Harm can range from embarrassment to substantial financial loss or even identity theft. Veterans and their dependents may lose confidence in VA services, which could prevent them from seeking essential medical treatment or other benefits, resulting in a decrease in their quality of life.
- **For VA.** Harm can mean the intangible loss of public trust or millions of dollars spent to notify individuals and control potential damage to them.
- **For You.** If you cause an incident, you could face disciplinary action, lose your job, pay steep fines, or even face criminal charges and imprisonment.

Legal Penalties
Protecting information is so important that there are substantial penalties for violating these laws. If you disclose sensitive information, or attempt to access or successfully access sensitive information without authorization, you can face severe consequences: from disciplinary or other adverse personnel action to criminal, civil, and administrative penalties.

Disciplinary or adverse action consequences may include:

- Suspension of access privileges
- Reprimand
- Suspension from work
- Demotion
- Removal.

Theft, conversion, or unauthorized disposal or destruction of federal property or information may also result in criminal sanctions.

Penalties may include civil or criminal fines for individuals of up to **$250,000**, and imprisonment for up to 10 years. Entities failing to protect health information could be

fined up to **$1.5 million** per year under the Health Information Technology for Economic and Clinical Health (HITECH) Act. Civil or criminal penalties for destroying or removing records without authorization may include fines up to **$2,000** or imprisonment up to three years. Penalties for Privacy Act violations may include fines up to **$5,000** and up to one year in jail per occurrence.

Do the Right Thing for Veterans
Here's the point: small choices you make, every day, create or destroy public confidence in VA and help or harm Veterans and VA's mission. At the end of this course, you will sign the National Rules of Behavior that govern the choices you make in your daily work.

While the VA National Rules of Behavior are based on federal laws, regulations, and VA directives, written guidance cannot cover every possible situation. You must go beyond the stated rules, using due diligence and highest ethical standards to guide your actions.

Ethics is a broad term that in plain words means using your ability to distinguish right from wrong as the basis to choose to do the right thing. Holding yourself to high ethical standards means putting Veterans first and never compromising their well-being for your personal convenience or for personal gain.

Everyday Hero to the Rescue: Part 2
Let's check back in with Harold and Maria.

> *Harold*: Hey Maria, I don't mean to stick my nose into your business or anything, but clinical data could contain sensitive information. You know, policy states that you're prohibited from sending it to your personal email account.
>
> *Maria:* Ah, I was so caught up in my work I didn't even think about it that way. I have a VA laptop that I can take home if I want to work on this. Thanks for the good catch, Harold.
>
> *Harold:* No problem.
>
> *Maria:* You're like my own personal superhero!

Harold grins sheepishly; he knows he saved the day by stopping Maria from creating a security incident.

Summary

Our everyday hero in this story, Harold, prevented a common security mistake that could have disclosed sensitive information. By just asking a question, he protected Veterans and helped Maria stay within the law and within VA policy. Being a hero is about doing small things that make a big difference.

Harold reminds us to do the right thing. Sometimes small choices make a big difference.

You've completed this lesson. Did you meet these objectives?

- Identify your five responsibilities
- Recognize privacy and information security legal requirements
- Define privacy
- Define information security
- Define sensitive information and related special terms.

Protect Sensitive Information

Carla Gets the Fax Facts: Part 1 (Fictional Scenario)

It's Tuesday at a VA community-based outpatient clinic, and Carla is faxing some paperwork while talking on her cell phone.

> *Carla:* Yeah, I'm leaving in just a bit. I just have to fax these last few patient records to one of our insurance providers.
>
> Natalie walks in and uses the copy machine next to Carla. Carla waves at her coworker, Natalie. Carla is distracted and not paying attention to the papers that she is faxing.
>
> *Carla (still talking on phone):* Sure, I'll get that report to you first thing in the morning. OK. Talk to you later.
>
> Carla gathers some papers and walks hurriedly out of the copy room. She leaves one sheet on the fax machine.
>
> Natalie notices the fax paper and picks it up. It is an insurance form, and it looks like it contains sensitive information. Natalie is concerned and wonders…"I don't think Carla meant to leave this here. It contains this patient's address and social security number."

Natalie knows sensitive information should never be left in a common area like a copy room or lobby.

We'll check in with Carla and Natalie again later.

Objectives

Before you can protect sensitive information, you have to know it when you see it—or hear it. That's right. Whether information is written down, spoken to you, overheard, played as an audio or video file, or stored electronically, the rule of thumb at work is to keep private information private.

In this topic, you will review requirements for protecting personally identifiable information (PII) and other sensitive information. You will also practice choosing actions to protect sensitive information in many situations.

You will learn to:

- Define different types of sensitive information
- Identify how to protect sensitive information contained in any format, when you are using it or when you have finished using it
- Recognize risks in common situations
- Choose appropriate action.

Privacy Dos and Don'ts
Here are some dos and don'ts that will help you protect Veterans' privacy.

Do:

- Maintain the confidentiality of individuals' personal information (i.e., PII) and especially personal health information
- View or access PII only if you need the information to do your job
- Collect and maintain only data that is necessary to perform VA's official functions
- Use VA email services with public key infrastructure (PKI) encryption software when sending PII or PHI electronically
- Follow local policy and procedures for disposition of records.

Don't:

- Throw any type of sensitive information in the trash
- Access PII or other sensitive information on public computers such as library or university kiosks
- Discuss PII or PHI or other sensitive information in public
- Disclose information related to drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or Sickle Cell Anemia (38 U.S.C. 7332) without written authorization by the patient.

Information May Be Sensitive If…
It's important for you to know the difference between information that's sensitive and other information that is not considered sensitive. Here are a few examples.

Examples of sensitive information include:

- Veteran medical insurance claim for alcohol treatment
- Patient name and social security number

- Pricing information disclosed to VA by vendors during bid processes
- Diagram of facility computer rooms
- Veteran loan application.

Examples of non-sensitive information include:

- VA press release
- Address of your VA facility.

Records Management and Sensitive Information
Correctly managing VA records is necessary to earn and maintain public trust. And if records contain PII or PHI, you have to be especially careful.

VA records must be carefully managed in order to:

- Conduct business efficiently and effectively
- Ensure Veterans receive the benefits and services to which they are entitled
- Protect Veterans' personal information from unauthorized access and disclosure
- Protect all records from unauthorized access, removal, or destruction
- Preserve documentation of U.S. national heritage
- Respond to FOIA requests
- Avoid civil or criminal penalties.

Remember: Do not disclose sensitive information of any kind unless it is an official responsibility of your job and only if you clearly understand when disclosure is allowed.

How to Protect Sensitive Information
Here are some things you can do to keep sensitive information confidential.

Always:

- Access only the information that is needed for you to do your job
- Remove paper documents containing sensitive information from printers or fax machines immediately after use and store securely
- Protect electronic data by saving and backing up data periodically using VA-approved storage, such as a mapped network drive; VA-approved thumb drives can be used if no mapped network drive is available

- Place documents to be discarded into locked shredder bins if they contain PII, PHI, or other sensitive information. (NOTE: For items that may be records, consult your supervisor or records administrator before disposing of them.)

Never:

- Discuss PII or other sensitive information with anyone who does not need to know that information in order to perform his or her job
- Discuss information about individuals in a public place
- Take VA sensitive information home unless you have prior written permission from your supervisor and ISO
- Throw documents containing PII, PHI, or other sensitive information into a wastebasket.

Everyday Choices–1
Now it's your turn to make choices to protect sensitive information in two common situations. Here's the first situation.

At a medical center, Dr. Carter and a medical student, Amir, are conducting rounds. They are discussing their patient, Mr. Smith, in the hallway next to the patient's room. Which of these actions potentially discloses sensitive information?

A. Amir asks if Dr. Carter has known the patient very long.

B. Amir states: "This patient, David Smith, has a history of alcoholism which has compounded his other medical issues and slowed his recovery."

C. Dr. Carter asks Amir when the patient first complained of headaches.

The correct answer is B. Section 38 U.S.C. 7332 prohibits disclosure of information about drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or Sickle Cell Anemia. This hallway discussion discloses Mr. Smith's name connected with his history of alcoholism to anyone nearby.

Everyday Choices–2
Here is another situation. See what you think. Rick is a records clerk and a history buff. One day, he finds a box of paper records for World War II Veterans at the back of a seldom-used storage area. He discovers a copy of actor Jimmy Stewart's medical

record and sends it to a friend who works for a supermarket tabloid. What is the likely outcome of Rick's action?

A. Rick is given a promotion for finding the misfiled box of paper records.

B. Rick becomes rich from the money he receives from the supermarket tabloid.

C. Rick's employment could be terminated and he could face criminal charges because he intentionally disclosed PII and used a Veteran's record for personal gain.

The correct answer is C. It is always a violation of law and VA policy to disclose any kind of sensitive information; it is a crime to do so for personal gain. Penalties for this type of violation include disciplinary action or dismissal, and possible criminal prosecution, fines, even imprisonment.

Carla Gets the Fax Facts: Part 2
Let's check back in with Carla and Natalie.

Natalie rushes down the hall to catch her coworker, Carla, and return the misplaced fax page.

Natalie: Hey Carla, wait a second. I think you just left one of your papers on the copy machine.

Carla: Oh, thanks Natalie. It's been such a crazy day. I'm just trying to get out of here.

Natalie: I know that feeling. But I just saw an email from our privacy officer about protecting Veteran personal information especially in a common area, like our copy room.

Carla: Yeah, that's right. I guess I need to slow down and focus more. Hey, thanks for having my back.

Natalie: Any time.

Carla: Bye.

Natalie was able to help prevent a security incident because she knew that private information should remain private.

Summary

Our everyday hero in this story, Natalie, helped Carla protect Veterans' personally identifiable information by taking quick action. Like Natalie, you can make a heroic difference by knowing what information is sensitive and taking care to protect it—even when you're in a hurry. A hero knows you always keep private information private.

You've completed this lesson. Did you meet these objectives?

- Define different types of sensitive information
- Identify how to protect sensitive information contained in any format, when you are using it or when you have finished using it
- Recognize risks in common situations
- Choose appropriate action

Protect Computers and Other IT Equipment

Lock it Up or Lose it: Part 1 (Fictional Scenario)

It's Wednesday around lunch time at a VA data center. A few colleagues are wrapping up a conversation before heading to lunch.

> *Bruce:* That's what I think we should do on this project. Uh, alright. Let's break for lunch, and we'll meet back at one.
>
> *Laura:* Alright, thanks. You guys want to grab something together?
>
> *Adam:* Definitely.
>
> *Bruce:* Sounds good.
>
> The meeting attendees take their personal belongings but leave their laptops behind in the empty meeting room with the door open. A moment later, Anaya and her coworker Jen walk by the office door.
>
> *Anaya*: I think that meeting went really well.
>
> *Jen*: Yeah, I agree.
>
> Anaya sees the laptops and stops. She looks concerned… "Shouldn't those laptops be secured?"

Anaya knows that all computer equipment must be secured at all times, even within a VA facility.

We'll check in with Anaya again later.

Objectives

Protecting computers and other IT equipment means understanding when these items are most vulnerable and taking precautions. It also means knowing how to implement available tools, like encryption, to protect data in case equipment is lost or stolen.

In this topic, you will review requirements and practice choosing actions to protect computers and other IT equipment. Protecting equipment will help protect the confidentiality of sensitive information and maintain integrity and availability of the information.

You will learn how to:

- Define key terms including types of IT equipment
- Identify how to protect IT equipment
- Recognize risks in common situations using laptops, universal serial bus (USB) drives, and other equipment
- Choose appropriate action.

Equipment at Risk

What equipment do you need to protect? You may be surprised. Here are some examples:

Equipment	Threat	Protection
Biomedical equipment, copy machines, and other devices with internal memory	• PII may be stored in machine memory and could be disclosed inappropriately	• Be sure IT staff is contacted to remove memory of these machines before they are replaced or removed from VA
Desktop computers	• Unauthorized access • Information visible on screen	• Log off or lock the computer screen (control/alt/delete) before leaving the area • Use screen protectors in public areas • Position screens to face away from those passing by
Laptop computers	• Loss or theft • Disclosure of sensitive information	• Lock up with locking cable • Use (do not disable) VA-installed encryption • Keep your laptop with you or locked in a secure location
Removable storage devices (USB drives, thumb drives, portable hard drives)	• Loss or theft • Disclosure of sensitive information	• Use only VA-issued devices with encryption • Keep in a secure place

Limited Use of Personal Equipment
VA employees are allowed limited personal use of government equipment. The key word is "limited." Limited personal use of government computers and other IT equipment is permitted as long as it:

- Involves minimal additional expense to the government
- Is performed on the employee's non-work time
- Does not interfere with VA's mission or operations
- Does not violate standards of ethical conduct for Executive branch employees.

Note: Some facilities may have more restrictive policies. Check with your supervisor to confirm policies at your location.

For more information, refer to VA Directive 6001, Limited Personal Use of Government Equipment Including Information Technology.

Take Action
Here are some examples of ways you can protect sensitive information by protecting computers and IT equipment.

- Lock your workstation computer when you walk away from it. (Press Control, Alt, and Delete at the same time, then select Lock Computer.) This will prevent an unauthorized user from accessing or altering information using your account.
- Get written permission to use an **encrypted** laptop computer for your work and use only a VA-approved, encrypted laptop computer and VA-issued and encrypted USB drives (also called thumb drives or portable storage).
- Follow physical security procedures, such as locking offices and conference rooms containing computer equipment, whenever the area is unoccupied. Do not leave facility doors or windows open or unlocked.

Everyday Choices–1
Here's an opportunity for you to make a choice to protect computers and other IT equipment in some common, everyday situations.

Jason's ground-floor office is very hot, so he opens an outside door to let some fresh air in. When he returns from lunch, his computer hard drive and screen are missing. What would have been a better solution to Jason's problem?

A. Jason could have closed and locked the outside door and locked his office.

B. Jason could have called his facilities management to have the thermostat adjusted instead of opening the exit door.

C. Jason could have purchased floor fans and placed them in the hallway to help hold the secure door open more easily.

D. Both A and B

Choice D is the correct answer. Make choices that put privacy and information security ahead of personal convenience or comfort. Always take basic physical security precautions to protect computers and other IT equipment. Never leave doors or windows open. Never disable security alarms on exit doors. Always lock work areas when they will be unattended.

Everyday Choices–2
Here's another common situation. Samira travels to several VA locations while conducting a study using claims data. Her study includes over 10,000 individuals' claims information stored on her laptop computer. What security measures are necessary to travel with her VA laptop?

A. The laptop hard drive must be encrypted to protect sensitive information.

B. The laptop must be secured with locking cables if it is left in a hotel room to ensure it cannot be stolen.

C. Both A and B

The correct answer is C. Here's more background: Permission must be granted by your supervisor, the facility ISO, and facility CIO before you are issued a VA laptop computer. The computer hard drive will be encrypted. To keep sensitive information safe, never remove or disable encryption. Keep the laptop with you when traveling. If you must leave it in a hotel room, use locking cables to secure it.

Everyday Choices–3
Some outdated medical equipment is being replaced. The old device has a computer memory that stores patient names and addresses along with their diagnostic information. Is there any action needed in this situation to protect sensitive information?

A. Yes. Patient names along with addresses are PHI. Equipment such as fax machines, copying machines, and medical testing devices that store this data

must have the computer memory erased before VA may dispose of the equipment.

B. No. Most people don't know how to access the machine's computer memory so there's no reason to worry about selling the machine or tossing it into the dumpster.

The correct answer is yes. Most people do not realize biomedical equipment, copy machines, fax machines, and other devices may contain sensitive information. Any stored PII or PHI must be removed and the memory must be erased by an IT technician before disposing of this equipment.

Lock it Up or Lose it: Part 2
Let's check in with Anaya.

Anaya (talking to her coworker): Will you excuse me for a moment? I need to make a quick call to our ISO.

Anaya (talking on phone): Hey Morgan, I'm by the ninth floor meeting room, and it looks like some laptops were left unattended. What should I do? OK. OK, thanks.

Anaya closes and locks the office door. Anaya left a note for the laptop owners: "I called Morgan. Locked door, didn't want your laptops to walk away. – Anaya"

Summary
Our everyday hero in this story, Anaya, quickly asked her Information Security Officer for help when she spotted computer equipment at risk. You can help protect VA and Veterans—and prevent lost or stolen equipment—by being aware of risks and taking action. To be a hero, every day, do the right thing—protect IT equipment.

You've completed this lesson. Did you meet the objectives?

- Define key terms including types of IT equipment
- Identify how to protect IT equipment
- Recognize risks in common situations using laptops, USB drives, and other equipment
- Choose appropriate action

Protect IT Systems, Software, and Networks

Watch out for Invisible Invaders: Part 1 (Fictional Scenario)

It's Thursday in a VBA Regional office. Darien stops by Will's office to ask a question.

> *Will:* Hi, Darien, what's up?
>
> *Darien:* Hey, Will. Quick question. Did you receive an email from Microsoft asking you to download a security patch?
>
> *Will*: I did. I haven't downloaded it yet. I've been hearing a lot about it around the office. Seems pretty urgent.
>
> Darien is a bit concerned with the email…"Something about this email message just doesn't seem right."

Darien knows that suspicious emails should always be reported to your ISO. When in doubt, report it!

We'll check in with Will and Darien again later.

Objectives

Systems, software, and networks are vulnerable to intentional attacks by a variety of malicious intruders. Some of these intruders are people; some of them are computer programming codes designed by people to damage or bring down VA's networks. Beware!

In this topic, you will review requirements and practice choosing actions to protect systems, software, and networks. Protecting these IT resources will help protect the confidentiality of sensitive information and maintain the integrity and availability of the information.

You will learn how to:

- Recognize a variety of attacks that can damage systems, software, and networks
- Identify risks and responsibilities for using social media or Web 2.0
- Recall how to use remote access to VA systems and networks
- Recognize risks in common situations
- Choose appropriate action.

Social Engineering
Social engineering is a broad term that means getting information by exploiting a relationship or exploiting the natural tendency of people to be friendly and trust others. Online social engineers try to get information from you through conversations or emails or instant messages, or by seeing what you post on your social networking site.

Like hackers who seek to invade networks and systems using technology, social engineers may want to get VA's information in order to commit fraud or identity theft, or just disrupt or vandalize the system or network. Here are some examples:

- Pop-up windows can be installed by hackers to look like part of the network and request that you reenter your username and password to fix some sort of problem. **NEVER** provide your password to anyone.
- Someone you don't know contacts you about a legitimate business issue. After you resolve the issue, he starts a friendly conversation and casually mentions he just got a new car and is selling his old one at a bargain price. You're curious, so he sends you an email attachment with the subject line: "Picture of the car." When you open the attachment, an embedded code enables a connection through the VA firewall. **NEVER** open attachments from sources you don't trust.

Attacks that Can Damage Systems, Software, and Networks
As computers become more and more sophisticated, the array of attackers and the types of attacks also become more sophisticated. Here are some examples and information regarding how to spot and stop these villains.

Villain	Example	How to Spot and Stop
Malware	• Computer viruses • Worms • Trojan horses • Spyware	VA installs anti-virus and host intrusion software on all systems. The VA Network Security Operations Center (NSOC) also monitors all inbound and outbound communications for unusual or unauthorized activities. Report any unusual activity on your computer system, such as unusual characters in documents or email, missing data, a sudden increase in spam or unsolicited email, or email with suspicious attachments. Do not open email and/or attachments from any unknown or untrusted source.

Villain	Example	How to Spot and Stop
Peer-to-Peer (P2P) File Sharing	• BitTorrent • Kazza	P2P file sharing is prohibited on VA equipment or networks; network scans can detect P2P programs that have been downloaded.
Phishing	You are offered a free newsletter subscription for clicking a link, entering your user name and password, and answering "a few simple questions."	To check a suspicious link, right click on the embedded link to display the URL. It will usually have one or two characters that are slightly different from the real URL: For example, www.amazon4u.com (phony) v. www.amazon.com (real). Never divulge your email password, sign-on password, or other passwords to anyone.
Spoofing	Links to known websites that take the user to a "dummy" site that looks similar to the real one, or email that appears as if it came from a known sender but, in fact, is from a spoofer.	Spoofing can be controlled by using encryption. VA technical staff combats spoofing by implementing filters of inbound and outbound traffic. If in doubt, type in the website address instead of selecting the link provided.

Social Media and Other Collaborative Tools

Use of social media and other collaborative tools has brought a new dimension of effectiveness into the VA workplace. Along with these advantages, there are new challenges to use these media safely, without disclosing PII or opening doors for Internet attacks.

Early Internet technologies enabled email, websites, and search engines to rapidly gather or send out information. Sensitive information was protected by editorial processes with approvals and checkpoints before content was published or posted to websites.

You have probably heard of social media or Web 2.0, sometimes referred to as the next generation of web technologies. These tools allow an even more rapid exchange of information by permitting people to share information and collaborate across the organization at every level. This open sharing can help VA develop new expertise and

adapt quickly to changing circumstances. It also means you must be careful to protect sensitive information when using social media.

There are many social networking tools. Facebook, Twitter, Flickr, and SharePoint are a few examples approved for VA use.

Consult VA Directive 6515, Use of Web-Based Collaboration Technologies, for VA policies for using social media.

Social Media Examples
Take a closer look at these social media tools in use at VA.

Social Media Tool	Risk	Tips for Safe Use
Microsoft SharePoint	Even though SharePoint is most often used internally (through the VA intranet), sensitive information can be disclosed to those who do not have a need to know.	• Use login and passwords to access SharePoint • Request access or use only if you need it for your work • Use SharePoint only through the VA intranet
Facebook	• Information posted on a personal Facebook site about something that was seen or heard at work could result in an incident of disclosing PII about Veterans • Once posted and shared, information is nearly impossible to “erase” • Like email, Facebook content is discoverable in court cases	• Do not discuss VA business on a personal Facebook page • Never post sensitive information on Facebook • Remember that information can become sensitive if facts posted at different times can be combined to disclose identity • Set up and keep security settings at a level where only your chosen friends can see your information • Do not post anything that you would not want to see in the headlines of the newspaper tomorrow • Consult VA Directive 6515 for social media policy guidance

Social Media Tool	Risk	Tips for Safe Use
Twitter	People you do not know will have access to information that you share. This may be a risk to VA if you share sensitive information or facts that can be analyzed to reveal sensitive information.	• Be careful about the type and amount of information that you reveal in a tweet • Do not share information about Veterans, your colleagues, yourself, your family, or your work • Never share VA sensitive information via tweets • Consult VA Directive 6515 for social media policy guidance
Flickr	• Photos can reveal personal information, such as where you live or work, what belongings you own, or places you visit regularly • Depending upon the device used to take the picture, the information stored in code about the picture may contain your exact location through coordinates gathered via a global positioning program. This could expose you to personal injury or crimes, such as burglary or identity theft.	• Remember you may need a person's consent to post photos of him or her • Never share PII or other sensitive information via Flickr • Be careful about the details revealed in any photos you post • Avoid clearly identifiable information, such as claim number, street names, or license plates • Disable the global tracking feature of any device you are using to take the pictures, such as cellular telephones, if disclosing the photo location would disclose sensitive information • Consult the VA Office of New Media for guidance before using Flickr

Network Safety Strategies

Using laptop computers, portable USB data storage (also known as thumb drives), wireless networks, and virtual private networks or VPNs can expand the possibilities for working remotely or telecommuting. Using these tools can also expose VA networks to intruders. Here's more information to help you use these tools safely.

Network	VA Requirements
Remote Access	Remote access means having access to VA networks and data from locations outside secure VA facilities. If you have a job-related need for remote access, you must apply for permission from your ISO, and: • Receive the written permission of your supervisor, facility CIO, and ISO to access, use, or send VA sensitive information while offsite • Have written permission to remove VA sensitive information from VA's facilities using either an encrypted laptop computer or an encrypted USB drive (thumb drive) • Use only encrypted, VA-issued computers to access VA networks remotely. For non-VA equipment, you must have a written waiver from the VA CIO to access sensitive VA information
Password Protection	Protect your password to protect system and network access. • Create by combining characters, letters, and numbers • Never share your password • Never use automatic password-saving features found on websites • Never store your password electronically or on paper near your computer
Virtual Private Networks (VPN)	VA provides and controls remote access through the VA VPN. You must have a VA VPN account to access the system from any location outside the firewall. • If you use Government Furnished Equipment (GFE), then you should use the RESCUE VPN; if you use other equipment or operating systems not supported by RESCUE, then you should use the VA Citrix Access Gateway (CAG) • All requests for VA VPN accounts must be approved by the immediate supervisor, the facility IT Chief/CIO, and the ISO • You must not be connected to any other VPN when you are connected to the VA VPN

Network	VA Requirements
Remote Access	Remote access means having access to VA networks and data from locations outside secure VA facilities. If you have a job-related need for remote access, you must apply for permission from your ISO, and: • Receive the written permission of your supervisor, facility CIO, and ISO to access, use, or send VA sensitive information while offsite • Have written permission to remove VA sensitive information from VA's facilities using either an encrypted laptop computer or an encrypted USB drive (thumb drive) • Use only encrypted, VA-issued computers to access VA networks remotely. For non-VA equipment, you must have a written waiver from the VA CIO to access sensitive VA information
Wireless Networks	Wireless devices can pose a significant security risk to VA because they are located outside of the physical confines of the controlled area. All sensitive information entrusted to VA must be in a VA protected environment at all times or it must be encrypted.

Required Practices

Remember these ways to protect systems, software, and network connections.

ALWAYS

- Get permission before using remote access or wireless devices
- Watch out for online social engineers using phishing and spoofing tactics
- Report any unusual email messages or suspicious attachments or links

NEVER

- Open email from sources you do not know and trust
- Disclose PII or PHI when using social media such as Facebook, Twitter, Flickr, or SharePoint
- Connect to any other VPN when you are connected to the VA VPN
- Provide your password to anyone

Everyday Choices–1
Now it's your turn to make some choices. Will you do the right thing to protect systems, software, and networks?

Here's your first choice:

Is this statement true or false? Posting sensitive information to a VA social networking site such as a VA Facebook page is acceptable because only VA employees have access.

A. True.

B. False.

This statement is false for many reasons. Social networking sites on the Internet are accessible to the public. Sensitive information should NEVER be posted to a general audience either within or outside of VA. Access to sensitive information should only be available to those with a need to know the information to do their work.

Everyday Choices–2
Here is a challenging situation. Mario telecommutes from home two days a week. Which of these are appropriate security steps he should take when working outside secure VA facilities?

A. Never share sensitive VA data with any unauthorized individual outside of VA.

B. Obtain your supervisor's written permission to work remotely.

C. Never share your username and password.

D. Never store VA sensitive data on your system without appropriate approvals and encryption.

E. All of the above

The correct answer is E. All of these actions are ways to ensure safety when working remotely and are identified in the VA National Rules of Behavior.

Everyday Choices–3
What's the right choice in this situation? Shelley is a nurse at a VA medical center. She uses Facebook to keep in touch with her family members. Today Shelley posts that there is a new patient with measles. Has sensitive information been disclosed?

A. Probably not, but you can't be completely certain.

B. Yes. The patient's diagnosis is sensitive information.

C. Yes. The patient's diagnosis when combined with the fact that Shelley works at a VA medical center is sensitive information.

The correct answer is A, probably not. Although the patient is being treated at a VA medical center, the Facebook page does not include specific, identifying information (name, age, or patient room number). Patient diagnosis is sensitive if it is tied to the patient's name or other identifying information. It might be sensitive if this is the only measles case in the facility this year. Better choice: don't share work information in non-work settings.

Watch Out For Invisible Invaders: Part 2
Let's check back in with Will and Darien. Remember, Darien feels a bit uncomfortable about an email that requests users to upload a patch.

Darien: You know, Will, I've heard a lot about computer viruses being sent through emails lately. I think we should report this email to our ISO just in case.

Will: You're probably right. Marcy's on vacation, but you know what, I happen to have the phone number for the VA NSOC right here.

Will dials the number for the VA NSOC to report the email. Remember: when in doubt, report.

Summary
Our everyday hero in this story, Darien, followed his instincts when an email about a routine software patch didn't seem quite right. Don't let invisible invaders jeopardize VA and Veterans.

You've completed this lesson. Did you meet these objectives?

- Recognize a variety of attacks that can damage systems, software, and networks

- Identify risks and responsibilities for using social media or Web 2.0
- Recall how to use remote access to VA systems and networks
- Recognize risks in common situations
- Choose appropriate action

Report Incidents

Every Day at VA

Every day at VA we face privacy and security issues. Like the everyday heroes in our stories, you are VA's first line of defense. Veterans count on you to recognize issues and report incidents.

Throughout this course, we've heard stories about things that happen every day at VA. Let's take a look at how they were addressed.

Story	Issues/Incident	Outcome of Story
A Social Network Nightmare: Trevor's mental health issues are disclosed on Social Network.	PHI Violation	Incident Identified
Everyday Hero to the Rescue: Harold reminds Maria not to email PII to her personal account.	Data Breach	Incident Prevented
Carla Gets the Fax Facts: Natalie gives Carla PII left on the fax machine.	Personal Data Disclosure	Incident Prevented
Lock It Up or Lose It: Anaya calls the ISO when she sees laptops unattended.	Unsecured Equipment	Incident Reported
Watch out for Invisible Invaders: Darien spots a suspicious software patch.	Computer Virus	Incident Reported

Objectives

Let's face it: Everyone is tired of headlines reporting yet another story about Veterans' PII that has been inappropriately disclosed. We can do better.

In this topic, you will review how to recognize and report incidents. An incident is any occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of VA sensitive information, including any situation in which PII may have been inappropriately disclosed. Reporting incidents keeps everyone on their toes. It helps VA identify and reduce risks that could violate Veteran privacy and undermine the Department's mission. It also helps senior leadership track how VA is improving and what risks need more attention. *Reporting incidents is everyone's duty.*

You will learn how to:

- Define incidents
- Recognize consequences of incidents
- Identify how to report incidents
- Choose appropriate action.

Incidents and Consequences

So what's the big deal? Does it really matter if you leave a stack of patient claim forms or home loan applications on your desk overnight if nobody sees it? Yes, it really matters.

Every small act of carelessness or negligence makes Veterans more vulnerable and could earn you a disciplinary action. The bigger the impact of the mistake, the greater the risk to Veterans and VA—and the more likely you could be reprimanded, or lose your job, face civil or criminal charges, face court-levied fines, or even go to jail.

Incidents are evaluated based on how many people are affected and how much damage or potential damage the incident causes. Consider the impact when the incident:

- Affects only you
- Affects your entire work unit
- Harms Veterans or VA
- Creates a national security risk.

This list is arranged from least impact to greatest impact. As the impact of an incident increases, the consequences for the individuals who caused it also become more severe.

Possible consequences may include:

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

This list of possible consequences of incidents is arranged from least severe to most severe.

Checklist
Incidents can occur because you are not aware of or do not understand VA policies and procedures. Some incidents occur because systems or networks have weaknesses or vulnerabilities that allow them to be attacked. While some incidents are caused by criminal actions, most incidents are caused by ignorance or carelessness or letting down your guard. Be aware and report every incident. Ask yourself these questions about confidentiality, integrity, and availability whenever you think an incident may have occurred.

Confidentiality

- Was there a possible loss or breach of information?
- Was sensitive information involved?
    - PII
    - PHI
    - VA regulatory or program-specific information
- Was claims information involved?

Integrity

- Was the data or information stolen or misused?
- Was the data or information disclosed inappropriately?
- Was the data or information altered without authorization?

Availability

- Was equipment lost or stolen?
- Is there potential for damage to systems or software?
- Was the network caused to be offline or unavailable?
- Is there suspected criminal activity (e.g., fraud, misuse)?

How to Report an Incident
Reporting every incident is your duty, and it is also a good habit to help each other remember to be accountable. Here are some questions many people ask about reporting incidents. *When in doubt, report!*

People Questions

Question	Answer
To whom do you report an incident?	As a VA employee or volunteer, you should always report suspected privacy and information security incidents to your supervisor and to either your ISO or your PO. If none of these is available, you can report directly to the VA Network Security Operations Center (NSOC) by calling the VA Helpdesk: 800-877-4328. Listen for the automated voice prompt that states, "If you have a security emergency…" Then, follow the instructions to report both privacy and security incidents. Contractors must also report incidents to their contracting officer's technical representative (COTR) and project manager.
How do you locate or identify your ISO or PO to file a report?	You can either ask your supervisor or use this convenient national locator website: https://vaww.infoprotection.va.gov/iso%20locator/default.aspx
What if you suspect someone of unethical or criminal actions?	Report the suspected incident to your supervisor and ISO or PO. Involve local VA police and the IG if you suspect a crime, for example, if equipment is lost or stolen. Do not intervene or investigate on your own. Contact the IG Hotline if you suspect fraud, waste, or mismanagement of resources: 800-488-8244.
If your supervisor is involved in the incident, how do you report it?	Report the incident to your ISO or PO and VA NSOC.

Procedure Questions

Question	Answer
How soon must you report a suspected incident?	Always report any suspected incident immediately. Incidents must be reported to the VA NSOC within one hour of being discovered or reported to their management, ISO, or PO.
What information do you need to report?	Describe what happened, including who was involved, when it happened, what system was compromised or what information was revealed, and any other details.

Question	Answer
How soon must you report a suspected incident?	Always report any suspected incident immediately. Incidents must be reported to the VA NSOC within one hour of being discovered or reported to their management, ISO, or PO.
What information do you need to report?	Describe what happened, including who was involved, when it happened, what system was compromised or what information was revealed, and any other details.
What if the incident occurs after hours or on a weekend?	Notify your supervisor according to local emergency procedures and contact VA NSOC.

Everyday Choices–1

Sometimes it's difficult to recognize when a situation warrants reporting. Which of these listed items are considered information security incidents and must be reported?

A. Someone you don't recognize and believe to be unauthorized is sitting at a VA computer.

B. A form requesting a bronze marker for a Veteran's grave is left unattended on a desk, a copier, or a computer screen where unauthorized individuals can see it. The form includes name, social security number, date of discharge, and home address.

C. A co-worker sends a patient's name and billing account number to the patient's personal physician via unencrypted email.

D. You discover an open box with reams of computer printouts containing sensitive information sitting unattended by a dumpster.

E. All of the above

F. None of the above

The correct answer is E. Each of these situations potentially discloses sensitive information to unauthorized parties. Report all of these incidents.

Everyday Choices–2

Here's another challenge. Lisa is a volunteer in an outpatient reception area. One of the receptionists has gone to lunch. From the public side of the reception desk, she can

clearly see a list of patients and their home addresses on the computer screen. What should she do?

A. Ignore it; the receptionist is a friend and she doesn't want to get her in trouble

B. Immediately report what she has observed to her supervisor and either her ISO or PO

C. Do nothing; the reception area isn't very crowded

D. All of the above

The correct answer is B. PII or PHI may have been inappropriately disclosed. Lisa must report it immediately to her supervisor and her ISO or PO.

Everyday Choices–3
Here's another challenge. During lunchtime, Jasmine notices her supervisor printing a list of local Veterans who have recently applied for disability benefits. The list includes names, addresses, and medical diagnoses. The supervisor nervously explains it is data for a university research class assignment. It seems odd that she is working with PII and is using a paper copy. What should Jasmine do next?

A. Ask her supervisor what class it is and ask to see a copy of the final report

B. Go back to her desk and call the VA police

C. Do nothing. Jasmine cannot be sure there's anything wrong about her supervisor's actions

D. Report what she saw to her ISO and PO and to the IG Hotline (telephone 800-488-8244 or email: vaoighotline@va.gov)

The correct answer is D. If you are a VA employee and you suspect a co-worker of inappropriately using VA sensitive data or IT equipment, you have a duty to report it immediately to your supervisor and ISO (or PO) and VA Office of Inspector General (IG). If the individual you suspect is your supervisor, report to your ISO or PO and also to the IG. Do not confront the individual directly and do not attempt to investigate it yourself.

Summary

All of the everyday heroes in our stories understood this simple fact: it's everyone's job to protect Veterans' privacy and ensure information security—every day at VA. Preventing privacy and information security incidents is important.

Reporting incidents is heroic. It helps everyone remember to do the right thing.

You've completed this lesson. Did you meet the objectives?

- Define incidents
- Recognize consequences of incidents
- Identify how to report incidents
- Choose appropriate action

Review and Sign Rules of Behavior

Objectives

Remember all of the Rules of Behavior by keeping these five types of responsibilities in mind. Meeting these requirements may seem routine, but the fact is, meeting these requirements every day is heroic!

You're nearly finished with the course. Your final task is to review and sign the National Rules of Behavior. Use the five responsibilities list to remember to implement the rules in your work, every day. You may never get a medal, but you will definitely be a hero!

Your Five Responsibilities

- Protect sensitive information
- Protect computers and other IT equipment
- Protect IT systems, software, and networks
- Report incidents
- Sign and comply with the Rules of Behavior

Checklist

How are you going to do things differently on your job as a result of taking this course? Many people remember best when they write themselves a note. Why not give it a try, right now? Make a quick checklist to help you remember to protect sensitive information every day.

- Do the right thing
- Privacy is what you protect; information security is how you protect it
- Keep private information private
- Remember your Five Responsibilities
    - Protect information
    - Protect equipment
    - Protect networks
    - Report incidents
    - Sign and comply with the National Rules of Behavior

Sign and Comply with the National Rules of Behavior

There's just one more step: review, sign, and comply with the National Rules of Behavior. Protecting sensitive information and information systems is how we do

business at VA, 24 hours a day, and seven days a week. By making the Rules of Behavior the way you do business, you will be a hero, every day.

Everyone who uses VA information and information systems must accept responsibility for safeguarding these resources.

- When you sign the Rules of Behavior each year, you are agreeing to uphold all of the behaviors stated in the Rules. You must sign the Rules to gain or maintain access to VA information and information systems.
- Even if your job does not require using a computer or handling electronic or paper records, what you do with information you see or hear on the job is subject to these Rules.
- The National Rules of Behavior are the minimum compliance standards for all VA locations. Local policies may provide higher levels of protection to VA's information or information systems. Contract employees are held to contract requirements. Always follow the highest level of protection in your situation.

Accept and Acknowledge Rules of Behavior
There are two versions of the National Rules of Behavior: one for VA employees and one for contractors. First, review the definitions of VA employee and contractor.

- **VA Employees**—VA employees are all individuals who are employed under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees.
- **VA Contractors**—VA contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems.

Next, locate the National Rules of Behavior in the Appendix that are right for you.

- Appendix A provides the Rules of Behavior for VA Employees
- Appendix B provides the Rules of Behavior for VA Contractors

Print, review, and sign the Rules of Behavior.

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

Since you are taking the paper version of the course, you must work with your supervisor and TMS administrator to ensure you receive credit for completion. In order to receive credit, you must print out and sign two copies of the appropriate VA National Rules of Behavior, located in the Appendix of this course. One copy will go to your supervisor, and you will keep the second copy for your own records.

Note: If you have access to Protected Health Information, you must also complete VHA Privacy Policy Training.

Appendix A: Rules of Behavior for VA Employees

Department of Veterans Affairs (VA) National Rules of Behavior

1 Background a) Section 5723(b)(12) of title 38, United States Code, requires the Assistant Secretary for Information and Technology to establish —VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department‘s missions and functions. The Office of Management and Budget (OMB) Circular A-130, Appendix III, paragraph 3(a(2)(a) requires that all Federal agencies promulgate rules of behavior that —clearly delineate responsibilities and expected behavior of all individuals with access to the agencies‘ information and information systems, as well as state clearly the —consequences of behavior not consistent with the rules of behavior. The National Rules of Behavior that begin on page G-3, are required to be used throughout the VA.

b) Congress and OMB require the promulgation of national rules of behavior for two reasons. First, Congress and OMB recognize 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 VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g. digital, paper), are essential aspects of their job. Second, individuals must be held accountable for their use of VA information and information systems.

c) VA must achieve the Gold Standard in data security which requires that VA information and information system users protect VA information and information systems, especially the personal data of Veterans, their family members, and employees. Users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information. The Golden Rule with respect to this aspect of an employee‘s job is to treat the personal information of others the same as they would their own.

d) Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using—due diligence and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives.

2 Coverage a) The attached VA National Rules of Behavior must be signed annually by all VA employees who are provided access to VA information or VA information systems. The term VA employees includes all individuals who are employees under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and

other trainees. Directions for signing the rules of behavior by other individuals who have access to VA information or information systems, such as contractor employees, will be addressed in subsequent policy. VA employees must initial and date each page of the copy of the VA National Rules of Behavior; they must also provide the information requested on the last page, sign and date it.

b) The VA National Rules of Behavior address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management and system administrators, and serves to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

c) The VA National Rules of Behavior use the phrase—VA sensitive information. This phrase is defined in VA Directive 6500, paragraph 5q. This definition covers all information as defined in 38 USC 5727(19), and in 38 USC 5727(23). The phrase—VA sensitive information as used in the attached VA National Rules of Behavior means: All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information, financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information, information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege, and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

d) The phrase—VA sensitive information includes information entrusted to the Department.

3 Rules of Behavior a) Immediately following this section is the VA approved National Rules of Behavior that all employees (as discussed in paragraph 2a of Appendix G) who are provided access to VA information and VA information systems are required to sign in order to obtain access to VA information and information systems.

Department of Veterans Affairs (VA) National Rules of Behavior

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

1 GENERAL RULES OF BEHAVIOR a) I understand that when I use any Government information system, I have NO expectation of Privacy in VA records that I create or in my activities while accessing or using such information system.

b) 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.

c) I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting 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.

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

e) I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit‘s Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

f) 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 supervisor, 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.

g) I understand that the VA National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

h) I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

i) I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.

2 SPECIFIC RULES OF BEHAVIOR. a) I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

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

c) I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d) I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.

e) I will secure VA sensitive information in all areas (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).

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

g) I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff.

h) I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

i) I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.

j) I will not store any passwords/verify codes in any type of script file or cache on VA systems.

k) I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

l) I will not misrepresent, obscure, suppress, or replace a user‘s identity on the Internet or any VA electronic communication system.

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

n) I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.

o) I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p) I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.,

q) I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized in writing by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.

r) I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.

s) 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.

t) I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connected to any VA network.

u) If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v) I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w) I will not disable or degrade software programs used by the 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.

x) I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y) I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z) I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa) I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb) 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.

cc) 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 must use VA-provided IT equipment for remote access when possible. I may be permitted to use non-VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

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

ee) I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA‘s CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff) I will obtain my VA supervisor‘s authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA‘s protected environment.

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

hh) I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii) I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj) I will use VA-provided encryption to encrypt any e-mail, including attachments to the e-mail, that contains VA sensitive information before sending the e-mail. I will not send

any e-mail that contains VA sensitive information in an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

kk) I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior 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.

3 Acknowledgement and Acceptance

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

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

_____ _____

[Print or type your full name] Signature

_____

Date

_____ _____

Office Phone Position Title

Appendix B: Rules of Behavior for VA Contractors

CONTRACTOR RULES OF BEHAVIOR

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

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

U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

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

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

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

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

3. ADDITIONAL CONDITIONS FOR USE OF NON- VA INFORMATION TECHNOLOGY RESOURCES
    a. When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.
    b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.
    c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other

network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.

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

4. STATEMENT ON LITIGATION

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

5. ACKNOWLEDGEMENT AND ACCEPTANCE

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

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

_____ _____
[Print or type your full name] Signature

_____
Date

_____ _____
Office Phone Position Title

Appendix C: Glossary

A

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

B

Business Information—Business information is information intended for use by employees when conducting the daily operation of VA business. *Source: VA Handbook 6500*

Blog—A blog is a "web log" or online journal that individuals may publish to a web location. Content of the blog is determined by the author. *Source: Wikipedia*

C

Confidentiality—Confidentiality is to preserve authorized restrictions on information access and disclosure. *Source: VA Handbook 6500*

Contractors—Contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems. *Source: VA Handbook 6500*

D

Disclosure—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*

Due diligence—Due diligence is the care and attention to detail that a reasonable person exercises to avoid harm to other persons or their property. In VA Handbook 6500, it is stated that "Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using 'due diligence' and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives." *Source: VA Handbook 6500*

E

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

Ethical standards—Ethical standards govern behavior that is professionally right or befitting,

or conforming to an accepted standard, such as VA's Rules of Behavior. "Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using 'due diligence' and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives." *Source: VA Handbook 6500*

F

Facebook—Facebook is a web-based social networking tool for sharing information, messages or blogs, photographs, and files with users whom you permit to view your site. Users may create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profile. Facebook users must register before using the site. Additionally, users may join common-interest user groups. *Source: Wikipedia*

Flickr—Flickr is a web-based photo and video hosting service. Pictures or videos that are stored on Flickr may be posted via a web link to social networking sites such as Facebook or blogs. In addition to being a popular website for users to share and embed personal photographs, the service is widely used by bloggers to host images that they embed in blogs and social media and has an official application for some mobile devices. *Source: Wikipedia*

Folksonomy—The term folksonomy means a system of classification derived from the practice and method of collaboratively creating and managing tags to annotate and categorize content. This practice is also known as collaborative tagging, social classification, social indexing, and social tagging. *Source: VA Directive 6515*

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

G

N/A

H

Health Insurance Portability and Accountability Act (HIPAA) and HIPAA Privacy Rule (1996)—Establishes requirements for protecting privacy of personal health information. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards

are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system. *Source: Wikipedia*

I

Incident—An incident is a situation involving a violation of either privacy or information security requirements as defined in related VA policies:

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

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

Individually identifiable information—Individually identifiable information is any information, including health information maintained by VHA, pertaining to an individual that also identifies the individual. *Source: VA Handbook 6500*

L

N/A

M

Malware—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.

Mashup—A mashup is a web page or application that uses and combines data, presentation, or functionality from two or more sources to create new services. The term implies easy, fast integration, frequently using open APIs and data sources to produce enriched results that were not necessarily the original reason for producing the raw source data. The main characteristics of the mashup are combination, visualization, and aggregation. *Source: VA Directive 6515*

Microsoft SharePoint—A data repository software, typically hosted on an organization's intranet, that controls who within the organization may access stored data, enabling multiple users to view, share, and edit documents. It is typically used for web content management and document management systems. It also enables managing of intranet portals and websites, web-based collaboration, social networking tools, and other web-based functions. *Source: Wikipedia*

N

N/A

O

N/A

P

Peer-to-Peer (P2P) File Sharing—Refers to any software or system allowing individual users of the Internet to connect to each other and trade files. While there are many appropriate uses of this technology, a number of studies show that P2P is a common avenue for the spread of computer viruses within IT systems. P2P allows users to download files such as music, movies, and games using a file sharing software client that searches for other connected computers (called "peers"). Similarly, other computers on the network are able to search for files on your computer. This differs from traditional file downloading that searches servers for the requested file. *Source: Wikipedia*

Personally Identifiable Information (PII)—Personally identifiable information is any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc., alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (see Sensitive Personal Information, below). *Source: VA Handbook 6500.2*

Phishing—Tricking individuals into disclosing sensitive personal information using the computer. Phishing is a way of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications pretending to be from popular social websites, auction sites, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. *Source: Wikipedia*

Protected Health Information (PHI)—Protected health information is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. *Source: VA Handbook 6500.2*

Privacy Incident—A privacy incident is a security-related event in which PII may have been exposed through either unauthorized access or disclosure. *Source: VA Handbook 6500*

Privacy-protected information—Privacy-protected information is all individually identifiable personal information that is protected under federal law. Privacy-protected information encompasses personally identifiable information, individually identifiable information, individually identifiable health information, and protected health information. *Source: VA Handbook 6500*

Program-specific information—Program-specific information is information that VA may not release or may release only in very limited, specified situations. This category of information may include certain critical information about VA's programs, financial information, law enforcement or investigative information, procurement information, and business proprietary information. *Source: VA Handbook 6500*

R

Regulatory/Program-specific information—Regulatory/Program-specific information is information that VA may not release or may release only in very limited, specified situations. This category of information, which normally would not be released to the public under 5 U.S.C. Section 552—the Freedom of Information Act, may include certain critical information about VA's programs, financial information, law enforcement or investigative information, procurement information, and business proprietary information. *Source: VA Handbook 6500.*

Records—Records are defined differently in the Privacy Act and the Federal Records Act. Both definitions must be considered in handling VA records.

1) Records include *all books, papers, maps, photographs, machine readable materials, or other* documentary materials*,* regardless of physical form or characteristics*,* made *or* received *by an agency of the United States Government under Federal law or in connection with the transaction of public business and* preserved *or* appropriate for preservation *by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Source: Federal Records Act* (44 U.S.C. 3301)
2) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his

name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. *Source: Privacy Act*

Rules of Behavior—Rules of Behavior is a document that describes a VA information system user's responsibilities and expected behavior with regard to information system usage. All individuals who use or gain access to VA information systems must read, understand, and agree by signature to adhere to the VA National Rules of Behavior before they are granted access to VA information systems. *Source: VA Handbook 6500*

S

Sensitive Information—See also: VA sensitive information.

Sensitive Personal Information (SPI)—Sensitive Personal Information, with respect to an individual, means any information about the individual maintained by an agency, 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. *Source: VA Handbook 6500.*

SharePoint—SharePoint is data repository software, typically hosted on an organization's intranet. SharePoint allows controls to be put in place that limit who within the organization may access stored data. It enables multiple users to view, share, and edit documents.

Social Engineering—Social engineering is a broad term that means getting information by exploiting a relationship or the natural tendency of people to be friendly and trust others. *Source:* http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

It is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim. *Source: Wikipedia*

Social Media—Media specifically for social interaction that uses highly accessible and scalable publishing techniques using web-based technologies. Social media use web-based collaboration technologies to blend technology and social interaction in order to transform and broadcast media monologues into social dialogue, thereby transforming people from content consumers to content producers. These media do not include email. *Source: VA Directive 6515*

Spoofing—Refers to a person or program that masquerades as another to gain unauthorized access. In the context of network security, a **spoofing attack** is a situation in which one

person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Another kind of spoofing is “web page spoofing,” also known as phishing. In this attack, a legitimate web page such as a bank’s site is reproduced in “look and feel” on another server under control of the attacker. The main intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest usernames and passwords. This attack is often performed with the aid of URL spoofing, which exploits web browser bugs in order to display incorrect URLs in the browsers location bar, or with DNS cache poisoning in order to direct the user away from the legitimate site and to the fake one. Once the user puts in a password, the attack-code reports a password error, and then redirects the user back to the legitimate site. Other types of spoofing include caller ID spoofing, email spoofing, and file-sharing spoofing. *Source: Wikipedia*

T

Twitter—Twitter is a web-based messaging service that enables you to send short bursts of information in 140 characters or less, known as Tweets. People who want to be informed of your activities may opt to receive your Tweets. *Source: Wikipedia*

Tweets—Short bursts of information in 140 characters or less sent by the Twitter web-based messaging service. *Source: Wikipedia*

U

N/A

V

VA DIRECTIVE 6500—VA Directive 6500 establishes the foundation for VA’s comprehensive information security program and its practices that are designed to protect the confidentiality, integrity, and availability of information that is created, processed, stored, aggregated, and transmitted by VA’s information systems and business process. It provides the minimum mandatory security control standards for implementation of VA Directive 6500, Information Security Program, and the criteria to assist management in making governance and integration decisions for VA’s various security programs. Purpose: The security policies, procedures, and controls outlined within VA Directive 6500 apply to all of the following: VA employees, contractors, researchers, students, volunteers, representatives of Federal, State, local, or Tribal agencies, and all others with authorized access to VA facilities, information systems, or information in order to perform a VA authorized activity. This policy applies to all information resources used to carry out the VA mission and to the security of all information collected, transmitted, used, stored, or disposed of, by, or on behalf of VA. *Source: VA Handbook 6500*

VA Sensitive Information—Sensitive information is all Department data, on any storage

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

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

W

Web-based collaboration tools and technologies—The second generation of web development and design that facilitate communication, secure information sharing, interoperability, and collaboration on the World Wide Web. Web-based collaboration tools are designed to help people involved in a common task achieve their goals. Web-based collaboration tools include but are not limited to weblogs (blogs), video blogs (vlogs), wikis, hosted services, social networks, video sharing sites, podcasts RSS or Really Simple Syndication (RSS2) feeds, virtual worlds, web applications, folksonomies, and mashups. *Source: VA Directive 6515*

X

N/A

Y

N/A

Z

N/A

Appendix D: Resources

Privacy and Information Security Regulations

Table 1. VA Web Links and Telephone Numbers

Information Security Portal https://vaww.infoprotection.va.gov/
Privacy Laws, Regulations, and Policies http://www.privacy.va.gov/privacy_resources.asp
Locator to Identify ISOs and POs https://vaww.infoprotection.va.gov/iso%20locator/default.aspx
VA Handbooks and Directives http://www.va.gov/vapubs/search_action.cfm?dType=2
Office of Inspector General (IG) Hotline (to report fraud, waste, or mismanagement of resources): 800-488-8244
VA IT Helpdesk (to report security incidents to Network Security Operations Center): 800-877-4328

Table 2. High-Level Timeline and Description of Key Laws Related to Privacy and Information Security

1950: Federal Records Act. 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 of the agency.”
1966: Freedom of Information Act (FOIA). Requires federal agencies to disclose records requested in writing by any person, subject to certain exemptions and exclusions.

1974: The 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.
1980: 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.
1996: Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Establishes requirements for protecting privacy of personal health information.
2002: Federal Information Security Management Act (FISMA). Requires federal agencies to have a program to assess risk and protect information and information system assets that support agency operations.
2010: Health Information Technology for Economic and Clinical Health Act (HITECH). Describes when and how hospitals and doctors and certain others may safely exchange individuals' health information; it also limits use of personal medical information for marketing purposes and increases fines for unauthorized disclosures of health information. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html and see Enforcement and Penalties for Noncompliance

Table 3. Related Sections of the United States Code: Veterans Confidentiality Statutes

Title 38 U.S.C. § 5701: VA Claims Confidentiality Statute. Information about any claims processed by VA must be kept confidential.
Title 38 U.S.C. § 5705: Confidentiality of Medical Quality-Assurance Records. Information generated during a medical quality-assurance program may not be disclosed except when specifically authorized.
Title 38 U.S.C. § 7332: Confidentiality of Certain Medical Records. Health records with respect to an individual's drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or Sickle Cell Anemia are extremely sensitive.

Table 4. Related Internal Revenue Code (IRC) Specifications

IRC at 26 U.S.C.A. § 6103 (p)(4). 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. Describes penalties for disclosing tax return information without the permission of the individual.

Table 5. Selected VA Privacy and Information Security Policies

VA Directive 6500, Information Security Policy.
VA Handbook 6500, Information Security Policy; including Appendix G. Department of Veterans Affairs (VA) National Rules of Behavior
VA Handbook 6500.2, Management of Security and Privacy Incidents.
VA Directive 6502, VA Enterprise Privacy Program.
VA Handbook 6502.1, Privacy Violation Tracking System (PVTS)
VA Handbook 6502.4, Privacy Act Review
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 6. Selected Other VA Directives and Handbooks

VA Directive 6066, Protected Health Information (PHI)
VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act
VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act System of Records

VA Handbook 6300.6/1, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses
VA Directive 6371, Destruction of Temporary Paper Records
VA Handbook 6512, Secure Wireless Technology
VA Handbook 6515, Use of Web-Based Collaboration Technologies
VA Handbook 6609, Mailing of Personally Identifiable and Sensitive Information