VA Privacy and Information Security Awareness Course

July 9, 2010

U.S. Department of Veterans Affairs
Office of Information and Technology
National IT Training Academy

Table of Contents

Introduction 1
Course Overview 1
Why Do You Have to Complete This Training Annually? 2
Course Objectives 3
Course Outline 4
Course Introduction 5
Introduction to Privacy and the Protection of Privacy 6
Personally Identifiable Information (PII) 6
Use of PII 7
Consequences of Unauthorized Disclosure of PII 8
Your Responsibilities in Regard to PII 9
Knowledge Check—Your Responsibilities in Regard to PII 10
How to Avoid Privacy Breaches 11
What About Security Breaches? 12
Confidentiality 13
Maintaining Confidentiality 14
Knowledge Check—Maintaining Confidentiality 15
Consulting with Your Privacy Officer (PO) and Information Security Officer (ISO) 16
Rules, Regulations, and Laws 17
Privacy and Information Security Laws 17
Fair Information Practices 18
Privacy Act 19
Knowledge Check—Privacy Act 20
Privacy Act Exceptions 21
Knowledge Check—Privacy Act Exceptions 22
Consequences for Non-Compliance with Privacy Act 23
HIPAA 24
HITECH 25
Improper Disclosure under HIPAA 26
Consequences for Non-Compliance with HIPAA 27
Scenario—Privacy Act and HIPAA 28
Knowledge Check—Consequences for Non-Compliance with HIPAA 29
Other Privacy Statutes 30
Knowledge Check—Privacy and Information Security Laws 31
Knowledge Check—Other Privacy Statutes 32
Disposing of Records 33
Disposing of Computers 34
Knowledge Check—Disposing of Records 35
Ethics 36
Secured Data 37
Importance of Passwords 37
Strong Passwords 38
Remembering Your Password 40

Protecting Your Password....41
Knowledge Check—Passwords....42
Email Privacy and Security....43
Chain Letters and Hoaxes....44
Email Hints....45
More Email Hints....46
Scenario—Email....47
Knowledge Check—Email....48
Fax Security....49
BlackBerry® Use....50
Laptop Security....51
Knowledge Check—Laptop Security....52
Removable Storage Media....53
Social Networking....54
Social Networking Tips....55
What Is Social Engineering?....56
Social Engineering Methods....57
Social Engineering Example....58
You Are the First Line of Defense....59
Scenario—Social Engineering....60
Knowledge Check—Social Engineering....61
Secured Connection....62
Authorized Use of Government Equipment....62
Limited Personal Use of Government Equipment....63
Inappropriate Use of Government Equipment....64
More Examples of Inappropriate Use of Government Equipment....65
Knowledge Check— Inappropriate Use of Government Equipment....66
Remote Access....67
Knowledge Check—Remote Access....68
Wireless Network Security....69
Wireless Network Dangers....70
Peer-to-Peer File-Sharing....71
Peer-to-Peer File-Sharing Dangers....72
Malware Symptoms and Prevention....75
Malware Prevention Tips....76
Knowledge Check—Malware....77
Knowledge Check—Malware Symptoms and Prevention....78
Importance of Backups....79
Your Role in Backup Routines....80
Knowledge Check—Backups....81
Incidents: What Are They, What Do You Do About Them, and How Do You Prevent Them?....82
What Are Information Security Incidents?....82
What Do You Do About Information Security Incidents?....83
How Do You Prevent Information Security Incidents?....84
Knowledge Check—What Are Information Security Incidents?....85

Knowledge Check—What Do You Do About Information Security Incidents? 86
Summary 87
References 88
VA Directives 88
Federal Policies 88
Important Terms 89
The VA National Rules of Behavior 91

Introduction

Course Overview

Audio:
Welcome to the Privacy and Information Security Awareness Course. You are taking this course because it is mandated by law that all VA employees, contractors, and all other users of VA information and VA information systems complete privacy and information security training.

Text:
The Privacy and Information Security Awareness Course will take approximately 60 minutes to complete.

Once you complete the course, you will have a deeper understanding of practices that can drastically reduce the risk of a privacy or information security incident.

This training focuses on important practices and procedures. It includes information which all VA employees, contractors, business associates, volunteers, students, and Veterans Service Officers need to know in order to protect information about Veterans.

If you are taking the paper version of the course, you must work with your supervisor and learning management system (LMS) administrator to ensure that you receive credit for completion. In order to receive credit, you must print out and sign two copies of the VA National Rules of Behavior, located at the end of this course. One copy will go to your supervisor and you will keep the second copy for your own records.

Why Do You Have to Complete This Training Annually?

Audio:
This training will satisfy the annual privacy and security training requirement mandated by the Privacy Act, 5 U.S.C. § 552a (e) (9) and the Federal Information Security Management Act, 44 U.S.C. § 3544(b) (4).

Text:
Annual privacy and security awareness training is a Federal Information Security Management Act (FISMA) 44 USC 3544(b) (4) and Privacy Act § 552a (e) (9) requirement. Completing this mandatory training will satisfy the following training requirements mandated by FISMA and the Privacy Act for all VA Employees:

- Annual Privacy Awareness Training
- Annual Information-Security Awareness Training
- Reading and signing the VA National Rules of Behavior annually

If you have access to protected health information (PHI), you are **required** to take the more detailed Veterans Health Administration (VHA) Privacy Policy training in addition to this course, per the Health Insurance Portability and Accountability Act (HIPAA) training requirement.

Failure to comply with the training requirements identified above will result in denial or removal of your access rights and privileges to VA information and information systems, which may have an adverse impact on your performance of duties.

Course Objectives

Audio:
The objectives of this course are to help you understand the importance of information security and privacy, and to help you understand how important you are in keeping Veterans' Personal Health Information (PII) and other VA sensitive information safe.

Text:
Upon completion of this course, you will be able to:

- Examine Personally Identifiable Information (PII), its use, and your responsibilities in regard to it
- Indicate privacy and information security laws and the consequences for improper disclosure
- Identify the elements required to maintain secure data
- Indicate the elements required to maintain a secure connection
- Recognize, respond to, and prevent Information Security Incidents
- Review and accept the VA National Rules of Behavior

Course Outline

Audio:
This course covers several important privacy and security topics, and provides you with the VA National Rules of Behavior.

Text:
The following topics will be covered in this course:

1. Introduction to Privacy and the Protection of Privacy
2. Rules, Regulations, and Laws
3. Secured Data
4. Secured Connection
5. Incidents: What Are They, What Do You Do About Them, and How Do You Prevent Them?

Course Introduction

Audio:
In the next hour, you will review your role in protecting the Personally Identifiable Information of our nation's Veterans. This course is designed to help you understand privacy and information security and make you aware of your responsibilities for protecting PII related to health care and Veterans' benefits.

Text:
Privacy and Information Security Awareness helps protect VA sensitive information and information systems. It is more than policies, procedures, laws, and regulations.

Much of what you learn in this course will not only help you protect VA sensitive information, it will also help protect you as a computer user.

This course will help ensure:

- Confidentiality, integrity, and availability of VA records and information systems
- Timely and uninterrupted flow of information throughout VA systems
- The protection from fraud, waste, and abuse of Veterans' and employees' Personally Identifiable Information and of VA information systems

Introduction to Privacy and the Protection of Privacy

Personally Identifiable Information (PII)

Audio:
Now that we have provided you with an overview of the course goal, objectives, and introduction, let's take a look at privacy and what you need to know and do in order to protect VA sensitive information.

Text:
Personally Identifiable Information (PII) refers to any information about an individual maintained by an agency, including (1) any information which can be used to distinguish or trace an individual's identity and (2) any other information that is linked or linkable to an individual.

Examples of PII include, but are not limited to, the following:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as Social Security Number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above examples

Certain transmissions of PII may require email encryption. If you have any questions concerning this, please contact your Privacy Officer (PO).

Use of PII

Audio:
VA cannot fulfill its mission unless it collects and uses personal information about Veterans, as well as communicating with Veterans about personal information. However, VA is a branch of the Federal Government and must abide by the Federal privacy statutes. As such, VA must collect personal information for the benefit of Veterans, use personal data only for authorized purposes, protect personal data from unauthorized access, and disclose personal information only when authorized by law.

Text:

Privacy of Personal Information

- VA must collect and use personal information about Veterans.
- VA also collects PII about employees.
- Information is collected for the benefit of Veterans and the United States.
- Information is used only for authorized purposes.

Privacy of Communications

- VA must communicate with Veterans about personal information.
- Personal data is protected from unauthorized access.
- Personal information is only disclosed when authorized by the law.

Consequences of Unauthorized Disclosure of PII

Audio:
Unauthorized or wrongful disclosure of Personally Identifiable Information, either inadvertently or intentionally, can result in serious consequences for Veterans, their dependents, VA, and you. The consequences of disclosing Personally Identifiable Information depend on the situation.

Text:
There are three levels of situation that can result in the unauthorized disclosure of PII. These three levels and associated consequences are listed below:

1. Accident, ignorance, or mistake—If an employee discloses PII accidentally or mistakenly, or does so out of ignorance, he or she may be disciplined. You should report the disclosure as soon as possible; failure to do so will be considered negligence.
2. Negligence—This is defined as a failure to exercise that degree of care which a person of ordinary prudence would exercise under the same circumstances. If an action is determined to be negligent, the employee will be disciplined.
3. Malice or intent to harm—If an employee releases information with the intent to harm, he or she will be disciplined; the employee may even be terminated. Criminal charges may also be pursued.

Your Responsibilities in Regard to PII

Audio:
VA holds a vast repository of Personally Identifiable Information gathered in the course of providing medical treatment, establishing entitlement to benefits, and providing employment. It is your responsibility as a VA employee to recognize PII, whatever the form in which it appears; to understand what constitutes a breach of privacy; and to understand what you can do to protect the privacy of the Veterans, dependents, and employees. This involves preventing use by, or disclosure to, unauthorized persons. VA is also responsible for preventing the improper modification or disposal of employees and Veterans' Personally Identifiable Information.

Text:
It is your responsibility as a VA employee to do the following:

- Recognize PII in whatever the form in which it appears.
- Respect the privacy of Veterans, their dependents, and your co-workers.
- Never discuss private information in public places.
- Understand what constitutes a privacy breach.
- Prevent use by, or disclosure to, unauthorized persons.
- Prevent the improper modification or disposal of Veterans' personal information.

Knowledge Check—Your Responsibilities in Regard to PII

Instructions: Read the question; then select the correct answer.

Which of the following actions undermines the goal of ensuring privacy?

A. A co-worker asks you to release private information to a person waiting in the reception area, but before doing so, you make sure this was authorized.
B. VA no longer needs some outdated files that contain personal information. The files are shredded and disposed of appropriately.
C. You believe one of your co-workers may be sick, because she has not been looking well. You consider looking at her personnel file, but decide to ask directly if anything is wrong.
D. You believe a patient is not receiving proper care. You share this person's file with a friend who is not a VA employee to get a second opinion. [Correct answer]

How to Avoid Privacy Breaches

Audio:
There are many possible causes for a privacy breach. Being careless with sensitive information can cause many negative effects. Ignorance of agency policies and procedures can also cause inadvertent disclosures; this ignorance is not an excuse. Breaches can also be a direct result of criminal activity, including personal vendettas, mischief, and theft.

Text:
Information-system vulnerabilities can leave an organization open to attacks. The United States has many enemies and as a U.S. Federal Agency, we are targeted by many who desire to get into our computer systems or gain access to sensitive information within our facilities. As a result, you need to be very careful about what information to disclose and how best to protect sensitive information.

There are many causes of privacy breaches:

- Carelessness
- Ignorance
- Information system vulnerabilities
- Flawed policies and procedures
- Criminal behavior
- Attack by enemies of the United States

The overall agency privacy policy is found in VA Directive 6502, VA Enterprise Privacy Program.

What About Security Breaches?

Audio:
As a VA employee, you must do your part to prevent attacks that would breach the security of the systems and the information they store in ways that could interrupt care of our Veterans.

Text:
The work we do at VA is an important part of our nation's security, and this puts VA's information systems at risk. To do your part in protecting the VA's information, you must protect your equipment, any documents and records to which you have access, and any sensitive information with which you might be working. You should ensure that equipment and information are kept in a secure place.

If an incident occurs, report it to your PO or Information Security Officer (ISO) immediately. If your ISO is not available, contact your Network ISO.

Confidentiality

Audio:
One of your most important responsibilities is keeping VA sensitive information confidential.

Text:
Confidentiality at VA means that personal, sensitive, or protected information is available only to those people who need it to do their jobs. At VA, confidentiality is a must.

In order to keep sensitive information confidential, you should do the following:

- Understand what information you have access to and why.
- Read and follow remote-access security policies.
- Access information systems only through approved hardware, software, solutions, and connections.
- Take appropriate steps to protect PII, network access, passwords, and equipment.
- Don't use automatic password-saving features found on websites.
- Report to your PO or ISO any misuse of the remote-access process; if VA sensitive information has been compromised, report it *within one hour of discovery*.
- Understand the National VA Rules of Behavior, which we discuss later in this course.

Maintaining Confidentiality

Audio:
There are some simple rules that go a long way toward keeping VA sensitive information secure. VA computer systems are set up to protect confidentiality; however, you also have to do your part.

Text:
To maintain confidentiality, you should do the following:

- Lock your computer (Press **Control**, **Alt**, and **Delete** at the same time, then select **Lock Computer**) when you walk away from it. This will prevent an unauthorized user from performing tasks or accessing information using your account.
- If you print VA sensitive information, make sure you take it from the printer right away and keep it stored in a secure place.
- Protect all sensitive information and access only information that you need to do your job.
- Never discuss information about a Veteran in a public place or with anyone who does not have the need to know to perform his or her assigned duties.
- Never take VA sensitive information home unless you have your supervisor's and ISO's prior written permission. If you do have permission to do this, you need to take extra precautions to protect the information.

Knowledge Check—Maintaining Confidentiality

Instructions: Read the question; then select the correct answer.

Which of the following are rule violations that should be reported?

A. A co-worker sends PII to an outside email address via unencrypted email.
B. A stranger whose presence you believe to be unauthorized is sitting at a VA computer.
C. A Veteran's personal medical information is left on a desk, copier, or computer screen where unauthorized individuals can see it.
D. All of the above. [Correct answer]

Consulting with Your Privacy Officer (PO) and Information Security Officer (ISO)

Audio:
The VA considers the protection of VA sensitive information extremely important. It is so important that VA has hired and trained people to specialize in these areas. These specialists are Privacy and Information Security Officers. Privacy Officers deal with what we have to protect and Information Security Officers deal with how we protect it. Any questions you have regarding privacy should be directed to your Privacy Officer (PO). If you have any questions regarding information security, always start with your Information Security Officer (ISO).

Text:
Your PO and ISO are there to help you understand the rules and requirements to keep Veterans', dependents', and employees' PII and VA's sensitive records and systems secure.

Every VA facility has a PO and ISO who can help you with issues like those mentioned above. If you do not know your PO or ISO, ask your supervisor to identify him or her for you. If you suspect VA sensitive information or VA systems have been compromised, report this to your ISO or PO *within one hour* of discovery.

Your POs and ISOs can assist you with issues such as:

- Knowing what to do if PII has been wrongfully disclosed
- Knowing what to do if your computer is infected with a virus
- Knowing what to do if you find or suspect someone using computers inappropriately or using them for theft or fraud
- Understanding your role in protecting the privacy, confidentiality, and integrity of VA sensitive information
- Understanding your role in your facility's contingency plan

Rules, Regulations, and Laws

Privacy and Information Security Laws

Audio:
Now that we have provided you with a quick introduction about PII and privacy, let's take a look at some of the laws that protect the privacy and security of information. You should have a general understanding of how to comply with them while performing your job.

Text:
Listed below are some privacy and information security laws that will assist you in performing your job, especially when it comes to protecting Veterans' information and VA's systems and data.

To learn more about each of these laws, go to the References page.

- Clinger-Cohen Act of 1996
- Computer Matching and Privacy Protection Act of 1988
- Computer Security Act of 1987
- Federal Information Security Management Act (FISMA) Title III, 2002 E-Gov Act
- Freedom of Information Act (FOIA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- NIST Special Publications—Computer Security Resource Center—CSD—800 Series
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information
- OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 17, 2006)
- Paperwork Reduction Act of 1995
- Privacy Act of 1974
- Title 38 U.S.C Statutes 5701, 5705, and 7332

Fair Information Practices

Audio:
Let's first take a look at the Fair Information Practices (FIPs), also called Fair Information Practices Principles (FIPPs). These are a set of internationally recognized practices that address the privacy of information about individuals. Fair Information Practices are important because they provide the underlying policy for many national laws addressing privacy and data protection matters.

Text:
The international policy convergence around FIPs as core elements for information privacy has remained in place since the late 1970s. Privacy laws in the United States often reflect some elements of FIPs, but not as consistently as the laws of other nations. Fair Information Practices were initially proposed and named in a 1973 report by an advisory committee of the U.S. Department of Health, Education and Welfare (now the Department of Health and Human Services). The committee was established in response to a growing use of automated data systems containing information about individuals. Its charge included automated data systems containing information about individuals maintained by both public- and private-sector organizations. The committee devised a code of five "Fair Information Practices" to safeguard personal privacy in automated personal data systems.

These five principles and the committee's findings, published in the 1973 report, are generally credited with supplying the intellectual framework for the Privacy Act of 1974 (although in drafting the statute, the Congress, influenced by its own inquiries, expanded the five principles to eight). For additional information, please go to http://www.privacyrights.org/ar/fairinfo.htm

VA's FIPS

VA's Fair Information Principles are the principles stated in VA Directive 6502, VA Enterprise Privacy Program. These are specific to VA and are the practices that VA must follow for the collection, use, and disposal of PII: http://www1.va.gov/vapubs/search_action.cfm?dType=1

Privacy Act

Audio:
We briefly mentioned the Privacy Act of 1974 when we discussed Fair Information Practices Principles. Let's go into more details about what it is and how it affects you and your job at VA. The Privacy Act sets the standards for protection and proper disclosure of information. It addresses Federal agencies' use and disclosure of personal information about individuals maintained in a system of records.

Text:
When a Federal agency collects and/or maintains information about an individual that is retrieved by that individual's name or any other unique identifier, such as Social Security Number (SSN), that information is protected by the Privacy Act, and a Privacy Act System of Records Notice (SORN) must be published in the *Federal Register* describing that System of Records. VA has published approximately 113 Privacy Act Systems of Records notices, which are available at http://www.gpoaccess.gov/privacyact/index.html.

Under the Privacy Act, individuals are granted the right to:

- Determine what records about them are being collected, maintained, used, or disseminated by VA
- Gain access to their records, subject to the Privacy Act exemptions
- Request an amendment to a record
- Obtain an account of disclosures
- Sue the Government for violations of the statute, such as permitting unauthorized individuals access to their records

Knowledge Check—Privacy Act

Instructions: Read the question; then select the correct answer.

Which of the following is not true about VA's commitment to personal privacy?

A. Information collected from a Veteran is used only for legitimate purposes.
B. Only authorized personnel within VA have access to personal data.
C. Supervisors at VA have the authority to disclose personal information at their discretion. [Correct answer]
D. VA communicates openly with Veterans about their personal information.

Privacy Act Exceptions

Audio:
The Privacy Act permits release of an individual's information without an authorization to employees of Federal agencies who need it to perform their assigned duties. There are exceptions to the prohibition on disclosure under the Privacy Act; the exceptions include the various situations listed below.

Text:
There are various requirements for Government disclosure of information. An agency may disclose information only if it has permission from the individual or if it can meet one of the following conditions:

- Disclosure is made to an agency employee who normally maintains the record and needs it in the performance of his or her duty.
- Disclosure is made to a law enforcement agency for an activity authorized by law upon receipt of a written request.
- Disclosure is required under the Freedom of Information Act (FOIA) Disclosure to protect the health or safety of an individual.
- Disclosure is for a "routine use" as defined in the Privacy Act System of Records Notice (SORN).
- Disclosure is made pursuant to a court order when signed by an appropriate official, such as a judge.
- Disclosure is made to the Census Bureau for census survey or related purposes.
- Disclosure is made to Congress regarding matters within its jurisdiction.
- Disclosure is for statistical research purposes and the record is to be transferred in a form that is not individually identifiable.
- Disclosure is made to the Comptroller General in the course of the duties of the Government Accountability Office.
- Disclosure is made to the National Archives and Records Administration and has significant historical value.
- Disclosure is made to a consumer reporting agency in accordance with certain conditions found under 31 U.S.C. 3711(e).

Knowledge Check—Privacy Act Exceptions

Instructions: Read the question; then select the correct answer.

To which agency does the Privacy Act authorize the disclosure of Personally Identifiable Information for use in population data reports?

A. VHA (Veterans Health Administration)
B. NARA (National Archives and Records Administration)
C. Census Bureau [Correct answer]
D. GAO (Government Accountability Office)

Consequences for Non-Compliance with Privacy Act

Audio:
There are criminal and civil penalties for non-compliance with the Privacy Act. You personally may be liable if you knowingly or willfully obtain or request records under false pretenses; disclose privacy data to any person not entitled to access; or maintain a system of records without meeting public notice requirements.

Text:

You may be charged with misdemeanor criminal charges, may be liable to pay a fine of up to $5,000 for each offense, and/or may face administrative sanctions.
Courts may also award civil penalties against an individual or VA for:

- Improperly/unlawfully refusing to amend a record
- Improperly/unlawfully refusing to grant access to a record
- Failing to maintain accurate, relevant, timely, and complete information
- Failing to comply with any Privacy Act provision in such a way as to cause an adverse effect on the subject of the record

Penalties for these violations include actual damages, payment of reasonable attorney's fees, and termination of employment.

HIPAA

Audio:
The HIPAA Privacy Rule is another law that we will be covering. It is a comprehensive Federal regulation that protects the privacy of individually identifiable health information. The rule protects health records and other personal health information maintained by certain health-care providers, hospitals, health plans, health insurers, and health-care clearinghouses. This includes the Veterans Health Administration (VHA).

Text:
HIPAA stands for Health Insurance Portability and Accountability Act; it protects the privacy of individually identifiable health information. Its main goals are to:

- Ensure privacy protections while maintaining access to quality health care
- Guarantee that patients have access to their medical records or health information
- Give people more control over the use and disclosure of their protected health information
- Provide a clear avenue of recourse if an individual's privacy is compromised

HITECH

Audio:
The Health Information Technology for Economic and Clinical Health Act, known as HITECH, became effective in February 2010. HITECH implements rules for reporting information disclosure, limiting use of personal medical information for marketing, and strengthening Federal privacy and information security laws.

Text:
The Health Information Technology for Economic and Clinical Health Act (HITECH) provides funding to establish an infrastructure to allow the electronic exchange of health information between entities such as hospitals and doctors. It also strengthens Federal privacy and information security laws to increase the protection of health information.

Because this legislation anticipates a massive expansion in the exchange of electronic protected health information, the HITECH Act also widens the scope of privacy and security protections under HIPAA.
Enhancements include the following: establishing a notification system in case unauthorized disclosure takes place; expanding privacy rules to entities that do work on behalf of providers and insurers; providing audit trails of all electronic record disclosure; and increasing penalties for violations. HITECH also increases the potential legal liability for non-compliance, and it provides for more enforcement.

Improper Disclosure under HIPAA

Audio:
The privacy of health information is vitally important and the consequences of divulging it can be significant.

Text:
Maintaining the privacy of health information saves lives because without the assurance of privacy, people may avoid life-enhancing and life-saving treatments.

Even patients who have insurance may delay treatment until their condition worsens. They may opt to pay for treatment themselves rather than risk revealing their condition to a health-care system they don't trust with their information. In addition, patients who seek treatment may withhold important information from treating physicians out of concern for their privacy.

Consequences for Non-Compliance with HIPAA

Audio:
HIPAA established Federal civil and criminal penalties for knowingly and wrongfully using and disclosing protected health information. Criminal penalties range from a $50,000 fine and one year in prison to $250,000 in fines and 10 years in prison, depending on the crime. Civil penalties increased under the HITECH Act. These penalties can extend up to $1.5 million. Let's look at each crime separately.

Text:

Crime

- Improperly obtaining or disclosing protected health information
- Obtaining protected health information under false pretenses
- Obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm

Punishment

- Up to $50,000 fine and one year in prison
- Up to $100,000 fine and five years in prison
- Up to $250,000 fine and 10 years in prison. The HITECH Act increased civil penalties up to $1.5 million

Scenario—Privacy Act and HIPAA

Instructions: Listen to the following situation and decide what you would do.

Voice: Edward has not been looking too healthy lately. I think he's sick. Hmmm…. I have access to his medical records. It wouldn't hurt anything if I just took a peek, as long as I don't tell anybody.

Possible Responses:

A. This is a violation. Since you don't have a legitimate need to review Edward's records, you must respect his privacy. [Correct answer]
B. This is a not a violation. Since you have access to his records, you can view them at any time as long as you don't share the information.
C. This is not a violation. You can use your access to look at Edward's medical records whenever you like.
D. This is not a violation. Since Edward might be ill, you have a right to view his medical records.

Knowledge Check—Consequences for Non-Compliance with HIPAA

Instructions: Read the question; then select the correct answer.

According to the Federal criminal penalties established by Congress, what is the maximum penalty a person can receive for wrongfully obtaining or disclosing protected health information with intent to sell for personal gain under HIPAA?

A. Up to $25,000 fine per person, per year for each requirement or prohibition violated
B. Up to $50,000 fine and one year in prison
C. Up to $100,000 fine and five years in prison
D. Up to $250,000 fine and 10 years in prison [Correct answer]

Other Privacy Statutes

Audio:
Other statutes that we will be discussing briefly are Title 38 U.S.C. 5701, 5705, 7332 and the Freedom of Information Act (FOIA). When making a disclosure, you must also have authority under these statutes to allow you to do it.

Text:

- Title 38 USC 5701: VA Claims Confidentiality Statute provides for the confidentiality of all VA patient and claimant names and home addresses, and permits disclosure of the information only when specifically authorized by the statute.

- Title 38 USC 5705: Confidentiality of Healthcare Quality Assurance Review Records provides for the confidentiality of records and documents created by VHA as part of a designated quality-assurance program. Such records and documents are confidential and privileged and may not be disclosed to any person or entity except when specifically authorized by the statute.

- Title 38 USC 7332: Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus (HIV), and Sickle Cell Anemia Medical Records is the most restrictive of the privacy laws and provides for the confidentiality of special protected diagnoses such as Sickle Cell Anemia, treatment of or referral for Drug Abuse, treatment of or referral for Alcohol Abuse, or treatment of or testing for infection with Human Immunodeficiency Virus (HIV).

- Freedom of Information Act (FOIA—5 USC § 552): The Freedom of Information Act compels the disclosure of reasonably described VHA records or a reasonably segregated portion of the records to any person upon written request, unless one of the nine exemptions applies.

Knowledge Check—Privacy and Information Security Laws

Instructions: Read the question; then select the correct answer.

Disclosure of Personally Identifiable Information is allowed when it is required by which Act?

A. HIPAA
B. Privacy Act
C. Freedom of Information Act [Correct answer]
D. All of the above

Knowledge Check—Other Privacy Statutes

Instructions: Read the question; then select the correct answer.

Which of the following best answers this question?

What should you do if you find a document with PII in the trash?

A. Review it to see what is in it.
B. Share it with your co-workers.
C. Shred it so no one sees the information.
D. Give it to your Privacy Officer. [Correct answer]

Disposing of Records

Audio:
When disposing of both electronic and paper records containing Personally Identifiable Information, be sure that the information cannot be viewed or retrieved by unauthorized persons. Shredding is an example of a proper disposal technique. Throwing the document into a wastebasket or unsecured recycling bin is not.

Text:
Some records can be disposed of simply by destroying them. However, other records need to be archived in a formal manner. The term "disposition" refers to the transfer of records to a storage facility, transfer of permanent records to the National Archives, destruction of records, and/or other appropriate methods of disposal.

Records may not be disposed of without proper disposition authority, as approved in a valid Records Control Schedule (General Records Schedules), and there are penalties for improper disposal, such as fines and imprisonment. Follow your local policies and procedures for disposing of printed paper copies containing sensitive information by contacting your ISO for media destruction procedures. These documents should be destroyed to a degree that renders them incapable of being read or reconstructed. More information on the destruction of temporary paper records can be found in VA Directive 6371, Destruction of Temporary Paper Records.

If you are unsure as to whether the information you have to dispose of is an official record and/or whether you have the authority to dispose of it, contact your immediate supervisor, your Privacy Officer, Records Control Officer, or Records Management Officer.

Disposing of Computers

Audio:
How would you feel if your personal information were stored on a computer, and then the computer were given to someone who didn't have the authority or the need to see that information to perform their assigned VA duties ? This would be a breach of your privacy and you wouldn't like it. To prevent this, the VA has in place strict guidelines to ensure the proper sanitization and disposal of media containing VA sensitive information.

Text:
Privacy issues arise when it is time to retire old computer equipment. Here is what you can do to prevent such issues from arising:

Disposing of Computers:

- Ensure that sensitive information stored on computers is disposed of properly before it is removed from service.
- If you see computers being thrown out without proper disposal, let your ISO know. Understand the concept that clicking the **Delete** button doesn't really delete a file completely from your computer.
- When possible, store information on your facility's network drives—not your desktop computer or your laptop. Using this technique can prevent data loss in the event of hardware failure.
- Contact your ISO or Information Technology (IT) staff if you have any media that need to be destroyed. There is a media destruction process to destroy old or damaged hard drives.

Knowledge Check—Disposing of Records

Instructions: Read the question; then select the correct answer.

Appropriate methods of disposing of protected records include all of the following except:

A. Transferring records to an approved storage facility
B. Placing records in the dumpster [Correct answer]
C. Transferring records to the National Archives
D. Destroying records using approved procedures

Ethics

Audio:
Ethics is about what is right and what is wrong. This goes beyond legal obligations and deals with actions that affect other people.

Text:
Within VA, ethics needs to be focused on providing the best health care, benefits, and services for our nation's Veterans. Applied to our computing practices, this means that we need to ensure that we are operating our computers in a manner that supports the VA's mission.

Taking this a step further, we need also to make sure that we implement appropriate computer practices and do not do anything that could introduce problems into the VA's computer network or tarnish our reputation.

If a mistake is made that could bring this about, it is ethical to bring this mistake to your supervisor's and ISO's attention as soon as possible, to prevent the issue from causing additional harm.

Secured Data

Importance of Passwords

Audio:
Now that we have covered some of the privacy and information security rules, regulations, and laws, let's look at passwords and their importance. Passwords are an essential part of any security program. To do your part in protecting the VA's information, you must protect your password. This means that you must have a Strong password that is not shared with anyone.

Text:
Passwords are important tools for protecting VA information and information systems and getting your job done.

They ensure that you and only you have access to the information you need. Keep your password secret.

If you have several passwords, store them in a safe and secure place that no one else knows about.

Strong Passwords

Audio:
"Strong" passwords have at least eight (8) characters and include uppercase and lowercase letters, numbers, and special characters.

Text:
VA requires Strong passwords on all information systems. Passwords must:

- Be changed at least every 90 days
- Have at least eight characters (i.e., Gabc123&).
- Use at least three of the following four kinds of characters:
  - Uppercase letters (ABC…)
  - Lowercase letters (…xyz)
  - Numbers (0123456789)
  - Special characters, such as #, &, *, or @

Using these rules will provide you with a Strong password.

Passwords: Rules of Thumb

Audio:
When hackers or crackers attempt to break into computing systems using passwords, they begin with common everyday words. They actually use lists of dictionary words and names in automated password-cracking tools. Other ways they use to try to crack passwords include using birthdays, Social Security Numbers, and addresses. To ensure that you are using Strong passwords, stay away from using any of these items.

Text:
Keep these rules of thumb in mind when creating Strong passwords:

- Don't use words found in a dictionary or use any combinations of letters that constitute words.
- Follow the rules for Strong passwords.
- Don't use personal references (names, birthdays, addresses, etc.).
- Change your passwords at least every 90 days. If you suspect someone may know your password, change it immediately and inform your ISO.
- Never let anyone stand near you while you type your password. Ask people to turn away while you type it, and don't let them see your keyboard while you type.
- If you have several passwords to remember, you **may** write them down, but keep them **in a locked place** so no one else can get to them.

Remembering Your Password

Audio:
Strong passwords can be developed by using parts of each word in a phrase. This, in combination with numbers and special characters, can help you develop a Strong password that is easy for you to remember.

Text:
Many people have played secret code games since childhood. Think of your password as a secret code you must remember. Take a minute and create your own secret code for a password you need to remember.

One way to develop a Strong password is to combine parts of words from a phrase. For example, the phrase, "I love my dog Rex" could help develop the password $1L0mDgX.

For more information about passwords, ask your ISO.

Protecting Your Password

Audio:
As mentioned earlier, Strong passwords are an essential part of any information security program. In order to do your part, do not share your password with anyone. This would compromise the VA's security and possibly cause issues for you.

Text:
Your username and password protect you and the information stored on VA computers.

When you log in to a VA system, the combination of your user name and password identifies YOU as the person accessing the system and information. All actions taken after you log in to the system are identifiable back to you, so it is important that you **NEVER** share your login information.

If someone else uses your account information, you are responsible. Guard your password and never disclose it to anyone!

Knowledge Check—Passwords

Instructions: Read the question; then select the correct answer.

Which of the following are secure password practices?

A. Using uppercase, lowercase, numbers, and special characters [Correct answer]
B. Using words found in a dictionary
C. Using names, birthdays, or locations
D. Using Social Security or license plate numbers

Email Privacy and Security

Audio:
Email isn't like a personal letter delivered to you in a sealed envelope by the Post Office. Think of email as a postcard that is delivered dependably, but can be read along the way by many people. Since email is **not private**, never use email to send VA sensitive information about Veterans or employees unless the information is encrypted. If a work-related issue requires you to send Personally Identifiable Information (PII) about a Veteran or VA employee in an email message, you are required to encrypt the message.

Text:
Don't expect privacy when using email to transmit, store, and communicate information.

Email is a great tool on which we have come to depend to do our jobs faster, but using email also has risks. Use it appropriately to protect our Veterans' and employees' information, and take certain precautions to reduce the risk of spreading viruses.

In order to exchange securely encrypted email messages within VA and with a growing number of Government and private-sector partners, the United States Government is deploying Public Key Infrastructure (PKI) digital certificates widely.

Chain Letters and Hoaxes

Audio:
Chain letters and hoaxes are email messages that waste our time and slow down VA's network. Don't participate in forwarding any of these to other computer users.

Text:

Chain letters and hoaxes clog up the network and may contain dangerous code. **NEVER** forward or reply to these messages. **DELETE** them without opening them. If you accidentally open the email, **CLOSE** it and **DELETE** it. **NEVER** open any attachments that come from an unknown source. **NEVER** reply by saying, "Please stop." **NEVER** forward or create hoaxes or ask people to modify their computer systems.

Email Hints

Audio:
Safe email practices go a long way toward preventing information security issues from arising. The old adage "an ounce of prevention is worth a pound of cure" has proven to be very true in the information security world.

Text:
Here are a few tips on using email safely:

- Use virus protection software to scan all emails and attachments you send or receive and keep it up to date.
- Learn to recognize the signs of a virus infection.
- Always be cautious when opening email and email attachments from people you don't know, since most computer viruses are spread by email.
- Replying to unsolicited spam email is actually more likely to increase the number of messages sent to your email address, because it validates that address.

If you have any questions about how to deal with spam or how to encrypt a message, talk to your local IT staff (also known as IRM, for Information Resources Management).

More Email Hints

Audio:
Here are a few more email hints that could help you to protect our Veterans.

Text:
Keep these tips in mind when using your email:

- Never open emails with inappropriate subject lines.
- Use "Reply to All" sparingly. Ask yourself if everyone in your large email group really needs to see your response.
- Don't participate in mail-storms by sending messages saying "me too", "thanks," or even "please stop."
- Don't spread rumors using email. Be suspicious of any message that tells you to forward it to others.
- If you receive an email asking for personal information or your password, delete it. A type of attack called "phishing" uses well-known website names to fool users into giving their usernames and passwords or other sensitive information.

Scenario—Email

Instructions: Listen to the following situation and decide what you would do.

Voice: Someone just sent me an email with a really funny video in it. My friend who works for the State Department would get a good laugh from this one. I think it would be okay to send it to her from my VA email account.

Possible Responses:

A. It is not okay to send the video. Don't send anything which could compromise systems within the VA or elsewhere using your VA email account. [Correct answer]
B. It is not okay to send the video, because the State Department computers might not have the correct software to open it.
C. It is okay to send the video as long as there is no possibility of a virus being attached to it.
D. It is okay to send the video as long as the file size is under 5MB.

Knowledge Check—Email

Instructions: Read the question; then select the correct answer.

What should you do if you receive an email attachment from someone you don't know?

A. Open the attachment if the subject line seems harmless.
B. Reply to the email and ask for more information.
C. Do not open the attachment. [Correct answer]
D. Open the attachment if your virus software doesn't tell you not to.

Fax Security

Audio:
Many people at the VA need to fax documents to complete their jobs and care for our Veterans. When these faxes contain sensitive information, special precautions must be implemented to ensure that that information is kept private.

Text:
Users should transmit VA sensitive information via fax only when there is no other way to provide the requested information in a reasonable manner or timeframe.

If you must fax sensitive information, the following security controls must be implemented:

- Use a VA-approved fax statement on all cover sheets.
- Double-check the recipient's fax number prior to sending the fax.
- Contact the recipient prior to sending the fax to ensure that he or she is available to retrieve it and to ensure that the fax machine is located in a controlled area.
- Ask the recipient to confirm receipt of the fax.
- Save transmittal summaries for periodic review.
- Remind regular fax recipients to provide notification if their numbers change.

BlackBerry® Use

Audio:
The BlackBerry® is a smart phone that keeps you connected via voice, messaging, email, and a task manager to keep you on time for all of your appointments.

Text:
If you use a BlackBerry, using Public Key Infrastructure (PKI) email encryption is vital to ensure that VA's information and information systems are secure while you maintain connectivity when away from the office. PKI encryption protects messages and attachments, ensuring that only the intended recipient can open or decrypt a message's or attachment's contents.

Sending emails without the appropriate encryption is a violation of the Information Security Program in VA Directive 6500. You should work with your ISO to implement encryption and to learn how to use Personal Identity Verification (PIV) on your BlackBerry.

Laptop Security

Audio:
Laptops are very useful tools in today's computing world. If you use a laptop, there are many steps you can take to protect the information on it.

Text:
Protection of data stored on laptops is a very important component in securing our Veterans' data. Laptops can contain large amounts of data that could fall into the wrong hands if proper precautions are not taken. To assist in protecting the data on laptops, follow these steps:

- Ensure that the hard drive is encrypted.
- Make sure that your system administrator maintains your laptop and that all the latest software upgrades are installed. This includes antivirus software, personal firewalls, software patches, and Virtual Private Network (VPN).
- Physically secure your laptop. This includes keeping it close to you while traveling and using locking cables if you must leave it in a hotel room.
- Tape contact information, such as a business card, to the bottom of a laptop; this could help in recovery, if the laptop is lost or stolen.

Knowledge Check—Laptop Security

Instructions: Read the question; then select the correct answer.

Practices that contribute to secure laptop use include:

A. Encrypting the hard drive
B. Ensuring that the systems administrator is keeping the laptop updated
C. Keeping the laptop protected while traveling
D. All of the above [Correct answer]

Removable Storage Media

Audio:
Removable storage media may be convenient, but in order to use them, certain security requirements must be followed. VA sensitive information outside VA's protected environment must be encrypted.

Text:
Only VA-approved, -procured, and -encrypted removable storage media are allowed within VA. Any of these media—thumb drives, external ports, etc.—that connect to VA's resources via USB ports must be encrypted with FIPS 140-2 approved encryption. Access to unauthorized removable media will be blocked through the use of port security.

In order to store VA sensitive information on removable storage media, you must have permission from your supervisor and your ISO. According to the Security Program of the VA Handbook 6500, written permission is required from both of them to obtain an encrypted thumb drive.

Social Networking

Audio:
Although social networking sites are great tools for collaboration and information-sharing, they are also powerful means for hackers and other cybercriminals to steal information. Prior approval must be granted if a VA employee needs to use any of these tools.

Text:
Social networking tools—blogs, wikis, instant messaging, and Facebook—facilitate communication within and outside the VA. These tools are "Web 2.0" applications and can be helpful in accomplishing our mission if they are used properly. Prior supervisory approval must be received if a VA employee needs to use any of them. Make sure you consult with your local Public Affairs Officers and Privacy and Information Security Officers as well.

Policies and laws need to be upheld even with these technologies. Also, all content not approved for public release must be limited to posting on the VA intranet.

Social Networking Tips

Audio:
Here are a few tips for social networking within the VA.

Text:
Within the VA, remember the following social networking tips:

- Use only instant messaging services that are approved by the VA.
- Do not use your VA username or password to set up login information for social networking site accounts.
- Prior to starting a social networking page—Facebook, Twitter, YouTube—obtain approval from the Office of Public and Intergovernmental Affairs.
- Protect PII and other sensitive information. Keep in mind that laws such as HIPAA and the Privacy Act apply.
- Only official spokespeople are permitted to comment on VA-mission-related legal matters.
- Do not post copyrighted materials or trademarks unless you have written permission.
- Be professional—don't use vulgar language, make personal attacks, or make offensive comments that target any group in particular. Do not promote products, political organizations, or anything illegal.

What Is Social Engineering?

Audio:
With well-protected networks, hackers or crackers have a hard time breaking in using technological approaches. In such cases, they will resort to social engineering and depend on people's kindness or sense of trust to steal information or resources.

Text:
Social engineering happens when a person tries to gain your trust in order to get information and resources which he or she can use for harm. This is an important information security issue!

Social Engineering Methods

Audio:
If people ask you for VA Sensitive Personal Information (SPI), make sure you know who they are and whether they have proper authority for access to the information.

Text:
A social engineer may try to trick you into revealing your password to gain access illegally to your system or to information about VA's patients, beneficiaries and dependents, and employees. We know you want to be helpful, but social engineers may try to take advantage of your kindness.

If people ask you for VA SPI, make sure you know who they are and whether they have proper authority for access to the information.

Social Engineering Example

Audio:

If someone asks you for something that seems unusual, contact your supervisor before proceeding. A social engineer posing as an IT specialist can gain access to a lot of resources if you hand over your password.

Text:

One example of social engineering that hurt a VA facility was a phone call from someone claiming to be from "the phone company." The thief said he was testing lines and long-distance circuits. The thief then asked an employee to dial a special code, which gave him access to a long-distance service. This scam resulted in thousands of dollars worth of unauthorized calls being made at VA's expense.

You Are the First Line of Defense

Audio:
You have to be diligent in protecting the VA from the tactics of social engineers, because you are our first line of defense.

Text:
As we learn more about the tactics hackers use to get access to VA's information and computer systems, hackers continue to look for new ways to get around our protections. Social engineers will rarely ask for sensitive information directly, but will work on gaining your trust and manipulating you into helping them to get the information and resources.

You have to be diligent in protecting the VA from the tactics of social engineers, because you are our first line of defense.

Scenario—Social Engineering

Instructions: Listen to the following situations and decide what you would do.

Voice: A person just called me and said he was a computer technician. He said that there was an issue with my account and he wanted to verify my user name and password. When I refused to give him my password, he insisted I give it to him since he was authorized to receive it. Should I have given it to him?

Possible Responses:

A. No, it is not okay to give your password. Make sure you report the incident to your ISO. [Correct answer]
B. Yes, it is okay to give your password as long as you confirm the person is a VA employee.
C. Yes, it is okay to give your password because the person on the phone said he was authorized to receive it.
D. No, it is not okay to give your password over the phone. You can send it by email.

Knowledge Check—Social Engineering

Instructions: Read the question; then select the correct answer.

Social engineering is a way for people to gain your trust so they can get you to give them information or access to VA resources they shouldn't have.

A. True [Correct answer]
B. False

Secured Connection

Authorized Use of Government Equipment

Audio:
Not only is it important to secure data, but also it's crucial to secure connection in order to ensure that Veterans' sensitive information is secure and safe. So, let's first take a look at the authorized use of equipment; in some situations, you may have limited personal use of certain Government resources.

Text:
The American people, especially our Veterans, expect us not to abuse or misuse the resources provided to us to accomplish our mission. As a VA employee, you may have the privilege of some "limited personal use" of certain Government resources such as computers, email, Internet access, and telephone/fax service.

Limited Personal Use of Government Equipment

Audio:
Some locations permit employees limited use of equipment. If this is the case at your facility, check the guidelines to make sure you do not violate the rules governing what is allowed.

Text:
This benefit is available only when it:

- Does not interfere with official VA business
- Is performed on the employee's non-work time
- Involves no more than minimal expense to the Government
- Is legal and ethical

These benefits may be limited or eliminated at any time, especially if you abuse these privileges. Restrictions on personal use of resources can vary between VA facilities. To protect yourself, you should discuss your limits and responsibilities with your supervisor and ISO.

You can read more about limited personal use of Government equipment in VA Directive 6001, Limited Personal use of Government Office Equipment Including Information Technology.

Inappropriate Use of Government Equipment

Audio:
Here are some examples of misuse of Government resources. If you have any questions about whether an action would be considered inappropriate, ask your ISO and supervisor.

Text:
Examples of misuse or inappropriate use are:

- Using VA systems to get unauthorized access to other systems
- Posting VA information to external newsgroups, bulletin boards, or other public forums without permission; this includes any use which may make someone else think the information thus posted came from a VA facility, or any uses that are at odds with the VA's mission or position
- Accessing, using, copying, or sending VA computer software or data, private information, or copyrighted or trademarked information without permission
- Using Government systems or equipment to make money, to get a non-Government job, or to do any business activity—consulting for pay, sale or administration of business transactions, sale of goods or services—or using Government systems in such a way as to cost the Government money

More Examples of Inappropriate Use of Government Equipment

Audio:
Here are some more examples of misuse of Government resources. If you have any questions about whether an action would be considered inappropriate, ask your ISO and supervisor.

Text:
More examples of misuse or inappropriate use:

- Slowing down, delaying, or disrupting Government systems or equipment with continuous data streams, video, sound, chain letters, or other large files
- Participating in activities which are illegal, inappropriate, or offensive to fellow employees or the public. These include hate speech or material that ridicules others because of their race, creed, religion, color, gender, age, disability, national origin, or sexual orientation
- Creating, downloading, viewing, storing, copying, or transmitting materials that are sexually explicit, sexually oriented, or related to gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities

Be sure to discuss your limits and responsibilities with your supervisor and ISO.

Knowledge Check— Inappropriate Use of Government Equipment

Instructions: Read the question; then select the correct answer.

Which of the following is considered inappropriate use of Government resources?

A. Running a side business
B. Applying for a VA job during your lunch time
C. Gambling
D. Visiting a news website during a break
E. Choice A and C [Correct answer]
F. Choices B and D

Remote Access

Audio:
Remote access provides users who are traveling with the ability to work while they are on the road. If you use remote access, make sure that you follow VA policies to ensure that VA's sensitive information is protected. Safety in this area includes obtaining permission from your supervisor and ISO before connecting remotely, not sharing passwords, and not removing VA sensitive information from VA's protected environment without permission.

Text:
You are allowed to access, use, or send VA sensitive information while offsite only if you have the permission of your supervisor, facility CIO, and ISO. Also, you can do so only when the following security steps have been taken:

You must:

- Have your supervisor's permission to obtain remote access
- Apply for this permission through your ISO
- Have your supervisor's permission to transport, transmit, access, and use VA sensitive information outside of VA facilities
- Not share your username or password—or instructions on how to access the VA network—with anyone else
- Always have encryption on the VA-owned laptop or VA-owned thumb drive that you use offsite

For non-VA equipment, you must have a waiver from the VA CIO to access sensitive VA information.

Knowledge Check—Remote Access

Instructions: Read the question; then select the correct answer.

Which of the following are appropriate security steps to take when working remotely?

A. Not sharing sensitive VA data with any unauthorized individual outside of VA. Obtaining your supervisor's permission to work remotely
B. Not sharing your username and password
C. Not storing VA sensitive data on your system without appropriate approvals and encryption
D. All of the above [Correct answer]

Wireless Network Security

Audio:
Because of the convenience of wireless technology, it is being used by many Federal agencies. An important fact to note here is that a computer is permitted to connect to the VA network wirelessly **only** if the connection is encrypted. Remember: The same general information security and privacy rules that govern the use of a local area network should apply to the use of a wireless network.

Text:
If you use a wireless network, it is important that you know how to use it safely and know the potential consequences if you don't. Wireless networks that use radio waves to transmit data are being used more often by Federal agencies. They allow users to do their work while moving from one location to another. Poorly controlled wireless networks can allow sensitive information, passwords, and other information to be read, changed, or transmitted by unauthorized users. If a wireless local area network is set up, it needs to be approved by OI&T and it must be encrypted using a FIPS 140-2 validated method.

All wireless networks should be approved by the facility CIO and set up based on the national wireless LAN policy. Local IT Staff should be consulted if you want to connect your VA-issued laptop to the local facility wireless network.

The use of a wireless network at your facility may not be allowed; please check your local use policy prior to connection and use of personal wireless networks.

Wireless Network Dangers

Audio:
Improperly used wireless technologies can introduce a multitude of vulnerabilities into the VA's network. If you are using this technology, be aware of the potential issues and take all necessary precautions.

Text:
Wireless Dangers

Here are some examples of the dangers associated with wireless networks. An attacker can do any of the following:

- Eavesdrop on a transmission between two workstations.
- Pretend to be you to get access to private information, to change data, or to send them to someone else by intercepting your login information by eavesdropping on a transmission.
- Analyze traffic to learn more about an organization's communication patterns, such as set days or times at which personal information is sent from one employee to another.
- Become "the man in the middle" by changing, intercepting, deleting, or transmitting messages to someone else.
- Jam a wireless network with extra radio signals to stop you from accessing information.

Peer-to-Peer File-Sharing

Audio:
Peer-to-peer file-sharing can cause major security issues within the VA and is prohibited.

Text:
Public peer–to–peer file-sharing (commonly known as "P2P") refers to programs that allow anonymous files to be shared between computers. There are times when using P2P is helpful. But most of the time, these programs break the law by sharing copyrighted music, videos, and games. Some common public P2P programs are Kazaa, Freewire, Grokster, and Morpheus.

Public P2P is not allowed at VA.

Peer-to-Peer File-Sharing Dangers

Audio:
Please protect our computers by not using peer-to-peer file-sharing.

Text:
P2P programs can be used to spread viruses and spyware. Spyware programs track what you do on your computer and send information to thieves and hackers—without you knowing it. For example, someone could use spyware to get information about you, your co-workers, Veterans, and Veterans' families. This information could be used to steal your identity, buy items on a Veteran's credit card, or collect personal financial information about a VA employee. In addition, P2P file-sharing makes the VA network run more slowly.

Don't be a victim. Use your computer wisely. If you think your computer may have P2P software or spyware, tell your ISO.

Malware

Audio:
Malware is the name for dangerous programs written with malicious intent to do harm or steal information. Viruses are among the many different malware programs that could infect your computer equipment. Worms are malware viruses that replicate over and over. The intention behind a worm is to tie up computer and network resources so that users will have a difficult time working and communicating.

Text:
High-tech vandals have created dangerous programs that infect computer systems. These programs vary in how they infect and damage systems, and are collectively called malware. When our systems become infected with malware, they may not operate properly.

Examples of malware include:

Term	**Definition**
Viruses	Viruses are one type of malware that attacks computers. Viruses find their way into computers by attaching themselves to files that are downloaded or transferred between computers. They can be spread in many ways—from a CD, DVD, removable storage devices, website, or email. It takes time and money to defend against viruses.
Worms	Worms infect systems and then replicate themselves. A worm is a simple virus that can copy itself over and over. A worm can be dangerous because it quickly uses all of the available memory on your system and brings the system to a halt. Viruses that can get around VA protections and attack one computer after another are even more dangerous.

Term	Definition
Malicious email	Malicious email hoaxes are not viruses, but they can still be dangerous. In most cases, the sender asks you to forward a warning message to everyone you know. A good example of an email hoax is one that has a subject line saying, "Delete this file immediately." The message tells you how to locate a computer file and delete it. A hoax may offer a way to help you fix a problem, but when you do what it asks, it actually disables your system. Even harmless messages can cause problems. Harmless messages forwarded to many other people slow down the VA network, which also slows down the process of serving America's Veterans.
Trojan Horses	Another type of virus is a Trojan Horse. The term "Trojan Horse" comes from a story in Virgil's Aeneid (c. 21–19 BCE). During the Trojan War, the ancient Greeks left a giant wooden horse outside the walls of the enemy city, Troy. When the curious Trojans moved the horse inside the city walls, Greek warriors swarmed out of the giant hollow structure and opened the city gates to their fellow soldiers. This allowed more Greeks to enter Troy and destroy it. Trojan Horse programs may seem harmless. Even though they do not replicate themselves, they can be just as destructive as viruses and worms. Their mission is to get destructive viruses inside computers and networks.

Malware Symptoms and Prevention

Audio:
Odd computer behavior can be a sign of malware. Having up-to-date antivirus software installed on your computer is essential to protect your system and the VA network from an infection. If you have any doubt that the antivirus software installed on your computer is up to date, contact your IT Staff or ISO.

Text:
There may be a problem if your computer has any of these symptoms:

- Reacts more slowly than usual
- Stops running for no apparent reason
- Fails to start ("boot")
- Seems to be missing important files
- Prevents you from saving your work

All VA computers must have virus protection software. To work properly, virus protection must be kept up to date. New updates are issued nearly every day. Contact your ISO or Information Technology Staff if you are not sure if it is up to date. While many sites automatically update virus protection software on network computers, some systems are not updated automatically. It is critical to update your antivirus protection regularly.

To learn more about computer viruses and your role in antivirus defense, talk to your ISO.

Malware Prevention Tips

Audio:
As with most information security practices, prevention goes a long way. Opening email attachments and clicking on links inside emails are very prominent ways in which malware can infect your system.

Text:
Here are a few tips to help you deal with malware:

- Set your virus protection software to scan your emails and attachments.
- Never stop or disable your antivirus program.
- Make sure your files are backed up on a regular schedule. Check with your IT Staff to ensure that your information is being backed up.
- Be wary of email messages from unknown senders or messages with unusual subject lines, such as "Open this immediately."
- Be very careful if someone sends you an attachment containing executable code. You can recognize these by the file extensions, such as: .exe, .vbs, .js, .jse, .wsf, .vbe, and .wsh.
- Do not delete any system files when asked to do so in an email; report this to your ISO.

Knowledge Check—Malware

Instructions: Read the question; then select the correct answer.

Software specifically designed to damage, corrupt, and disrupt a computer or network is known as:

A. My Favorites
B. Malicious software or "malware" [Correct answer]
C. Junk mail
D. Spam

Knowledge Check—Malware Symptoms and Prevention

Instructions: Read the question; then select the correct answer.

If you think your computer is infected with a virus, you should tell:

A. Your computer manufacturer
B. Your Information Security Officer (ISO) and your supervisor [Correct answer]
C. Acme Virus Protection, Inc.
D. Your friends
E. None of the above

Importance of Backups

Audio:
Backing up your information is an essential part of protecting VA information. We must always remember that computers are mechanical equipment and that all mechanical equipment will eventually fail. Therefore, the information stored on your local hard drive needs to be stored somewhere else as well, such as on a drive mapped to a server.

Text:
Any work you do on VA's computers is important. It is important to you because of the time and effort expended to create it. It is important to VA and to Veterans because it supports our mission. There are some resources we can't afford to lose, so database backups are systematically and routinely created on systems such as Veterans Health Information Systems and Technology Architecture (VistA), Benefits Delivery Network (BDN), and others. Backups are cheap insurance.

Your Role in Backup Routines

Audio:
Information that resides on your computer is very valuable and it needs to be backed up. Consider all the hard work that you have done to complete those documents. You would not want a hardware failure to ruin weeks or even months of your hard work.

Text:
VA Information Technology Staff work hard to make sure the VA data are safe and routinely backed up. The question is not **if** you will ever need to use your backup—the question is **when**; making backups is a smart practice for your home computer, too.

Things you can do to assist in this matter include the following:

- Keep your files in one location, on a mapped network drive. This will make it easy to find and create backup files.
- If you are a remote user or travel a lot, check with your IT Staff to ensure that your data are being backed up.
- If you have any concerns about how your system is being backed up, contact your IT Staff or ISO.

Knowledge Check—Backups

Instructions: Read the question; then select the correct answer.

Which of these are recommended practices for data backups and their importance?

A. Store files in a single location on a mapped network drive.
B. Your data should be backed up on a regular basis.
C. If you are not sure that your backups are occurring regularly, contact your ISO or IT Staff.
D. All of the above. [Correct answer]

Incidents: What Are They, What Do You Do About Them, and How Do You Prevent Them?

What Are Information Security Incidents?

Audio:
Now that we have discussed privacy, the rules and laws related to it, secure data and secure connection, let's look at information security incidents and how to prevent them. Unfortunately, privacy and information security incidents do happen. However, your response during one of these incidents can prevent a catastrophe. For instance, if a new virus that could harm all the computers in the VA hits your computer first, notify your IT staff and ISO of the incident so they can take proper action.

Text:
At VA most of the data we keep should be kept private and secure. Any security incident might jeopardize our Veterans' or employees' sensitive information.

Security incidents include the following:

- Lost or stolen portable equipment—causes major security breaches. These data breaches violate our promise to our Veterans and put them at risk for identify theft.
- Virus attack
- Faxing PII
- Missing or compromised files
- Improper disposal of PII
- Mailing PII—Make sure you mail information to the proper person.
- Unattended personal information
- Accessing or sharing Sensitive Personal Information (SPI) with people who do not have a need to know
- Sending unencrypted emails containing PII

It is important to tell your supervisor and PO or ISO when you encounter such incidents.

What Do You Do About Information Security Incidents?

Audio:
If you think an information security incident has occurred, you should gather information about what happened and report it to your supervisor and PO or ISO immediately.

Text:
If you think a security incident has occurred, you should:

- Write down:
  - The date, time, and location the incident took place, as well as the computers which may have been affected
  - Any error messages that showed up on your computer screen
  - Any web addresses, server names, or IP addresses involved in the incident
- Contact your supervisor and PO or ISO in person or by telephone rather than by email.
- Do **not** contact the media (radio, TV, newspapers) or anyone outside your VA facility.
- If a crime is involved, report it to VA law enforcement. **Managing Security and Privacy Incidents** of the VA Handbook 6500.2 provides additional procedure on incident management.

Protect yourself. If you witness what you believe to be a security or privacy incident, you are obligated to report it *within an hour* to your supervisor and PO or ISO. If you fail to report such an action, you may be considered an accomplice to that action.

How Do You Prevent Information Security Incidents?

Audio:

It is your responsibility to report any and all suspected or potential breaches of privacy to the proper authorities. If in doubt, ask your Privacy Officer. Remember, it takes a unified team to ensure the privacy of information.

Text:

While at work, always do the following:

- Follow all privacy policies and procedures.
- Properly dispose of any private data you no longer need.
- Disclose only the required data and only through the proper VA channels.
- Report suspected or potential breaches of privacy to your PO or to the Network Security Operations Center (NSOC) if it is after normal work hours.
- If you are in doubt, ask your immediate supervisor.
- Work as a team to ensure privacy.

Knowledge Check—What Are Information Security Incidents?

Instructions: Read the question; then select the correct answer.

Which of the following is considered an information security incident?

A. Sitting at a VA computer is a stranger whose presence you believe to be unauthorized.
B. A Veteran's personal medical information is left unattended on a desk, a copier, or a computer screen where unauthorized individuals can see it.
C. A co-worker sends a patient's sensitive personal information (such as a combination of a full name and Social Security Number or account number) to an outside email address—even if it is the patient's personal physician—via unencrypted email.
D. You discover an open box with reams of computer printouts containing sensitive personal information standing unattended by a dumpster.
E. None of the above.
F. All of the above. [Correct answer]

Knowledge Check—What Do You Do About Information Security Incidents?

Instructions: Read the question; then select the correct answer.

If you think a computer security incident has occurred, you should:

A. Ask your friend down the hall what to do
B. Gather all the information you can, and report it to your ISO and PO [Correct answer]
C. Contact your local media
D. All of the above

Summary

Audio:
The VA and our nation's Veterans are depending on you to do your part in privacy and information security protection. Keep in mind that our information and information systems also assist with our readiness during national emergencies. Your safe practices can protect VA information and contribute greatly toward providing our Veterans with top-quality services. This will benefit you, the Veterans, the VA, and our nation. Thank you for doing a great job in this area!

Text:
VA's information and information systems are a major part of how we help Veterans. They also affect our readiness to work with other Federal agencies, such as the Departments of Defense, Health and Human Services, and Homeland Security, during national emergencies.

The FBI has warned all Federal agencies that their systems, and the information in those systems, are potential targets for attacks. Now more than ever, VA's systems and the information they contain must be available to serve our nation and its Veterans. Please be careful. Don't do anything that might damage our information and information systems.

References

VA Directives

VA Directive and Handbook 0710, Personnel and National Information Security
VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology
VA Directive 6300, Records Information Management
VA Directive 6301, Electronic Mail Records
VA Directive 6371, Destruction of Temporary Paper Records
VA Directive and Handbook 6500, Information Security Program
VA Directive 6502, VA Enterprise Privacy Program
VA Handbook 6500.2, Managing Security and Privacy Incidents
VA Directive 6600, Responsibility Of Employees And Others supporting VA In Protecting Personally Identifiable Information (PII)

Federal Policies

Clinger-Cohen Act of 1996
Computer Matching and Privacy Protection Act of 1988
Computer Security Act of 1987
Electronic Communications Privacy Act
Federal Information Security Management Act (FISMA) Title III, 2002 E-Gov Act
Freedom of Information Act (FOIA)
Gramm-Leach-Bliley Act
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH) Act
NIST Special Publications—Computer Security Resource Center—CSD—800 Series
OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
OMB Memorandum M-06-16, Protection of Sensitive Agency Information
OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 17, 2006)
Paperwork Reduction Act of 1995
Privacy Act of 1974
Title 38 U.S.C statute 5701
Title 38 U.S.C. statute 5705
Title 38 U.S.C. statute 7332

Important Terms

Confidentiality: This concept is designed to ensure that information is accessible only to those authorized to view it.

Health Information: This is any information that is created or received by a health-care provider, health plan, public health authority, employer, life insurer, school or university, or health-care clearinghouse.

Individually Identifiable Health Information: This is health information that relates to the past, present, or future physical or mental health or condition of an individual. It also includes the provision of health care to an individual or the past, present, or future payment for health care.

Personally Identifiable Information: Any unique identifying number, characteristic, code, or other data that are used to identify an individual or can be traced back to an individual.

Privacy Act Systems of Records: A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual, or by some other identifying number or symbol. Any record within such a system is protected. A record contains individually identifiable material, such as Social Security Numbers, medical history, employment history, financial data, and criminal history.

Protected Health Information: Individually identifiable health information that is transmitted by electronic media, maintained in any electronic medium, or transmitted or maintained in any other form or method.

Records: 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.

Routine Use: A routine use (RU) allows Government agencies to disclose individually identifiable information simply by stating their plans to disclose that type of information when they create or alter the database.

Sensitive Personal Information (SPI) – The term, 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.

The VA National Rules of Behavior

Audio:
The VA National Rules of Behavior ensure that everyone is aware of his or her security responsibilities and help to protect our Veterans' data. You must sign this document yearly in order to access VA information and information systems.

Text:
Everyone who accesses VA's information and information systems must understand his or her security role and responsibilities. Do's and don'ts of information security are established in the VA National Rules of Behavior.

The VA National Rules of Behavior include the consequences of inappropriate behavior. Consequences may range from a written reprimand to losing your job, depending upon the violation.

Prior to being granted access to VA's information and information systems, users must agree to the VA National Rules of Behavior, stating that they have read, understand, and will abide by these security rules. The VA National Rules of Behavior must be read and signed each year.

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