



HRSA Information Security Awareness Training 2008

Outline

- ❖ Information Security Overview
- ❖ Information Systems Security Awareness
- ❖ Technology-Specific Security
- ❖ Cyber Security Incident Response
- ❖ Privacy Awareness
- ❖ What Can You Do To Keep Information Secure?

Section 1

Information Security Overview

- ❖ Information Security Definition
- ❖ Federal Laws and Regulations
- ❖ Security Awareness and Training Requirement
- ❖ Keeping HRSA Systems Secure
- ❖ HRSA Information Security Policy

Information Systems Security: What Is It?

Information Systems Security refers to the protection of information systems by measures necessary to prevent, detect, and counter threats against:

- unauthorized access to systems and information;
- modification of information, whether in storage, processing, or transit;
- and against the denial of service to authorized users.



Principles of Secure Information Systems

A secure information system meets three main principles: confidentiality, integrity and availability of information. All three are essential in information systems security.

Confidentiality ensures that people who don't have the appropriate clearance, access level and "need to know" do not access the information.

Integrity ensures that information cannot be modified or destroyed.

Availability ensures that information services are there when needed.

Federal Laws and Regulations

There are several Federal laws and regulations developed to stem attacks against information systems. The following are a few of the laws that dictate Federal policies concerning IT security:

- [Federal Information Security Management Act \(FISMA\)](#) (Public Law 107-347, Title III), December 2002
- [Federal Information Processing Standards \(FIPS\) 200](#), *Minimum Security Requirements for Federal Information and Information Systems*, 2006
- Office of Management and Budget ([OMB Circular A-130](#)), *Management of Federal Information Resources*, 1996
- [Privacy Act of 1974](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\)](#), 1996

Security Awareness & Training Requirements

- Federal law mandates that ALL contractors, staff and authorized users of HRSA's IT resources complete the General User Security Awareness Training prior to accessing the system and at least once annually.
- Federal law also requires that IT and security personnel take Role-Based Training commensurate with their security responsibilities annually.
- Upon completing the General User Security Awareness, users must read and sign the HRSA's IT Rules of Behavior. Failure to comply may result in your network/email account being locked.

How Is HRSA Securing Its Systems?

- HRSA takes IT Security seriously. The security of HRSA's network is monitored 24 hours a day, seven days a week, using automated security processes and manual procedures, including:
 - Firewalls, which filter and block unwanted types of Internet traffic from HRSA systems
 - Intrusion Detection Systems that examine network traffic for attack patterns
 - Active Patching Process on both servers and workstations
 - Active blocking of access to restricted inappropriate websites
 - Scanning of all files on the workstations performed on a routine basis
 - Routinely updated anti-virus and anti-spyware software on all servers

How Is HRSA Securing Its Systems?

- E-Mail Security
 - HRSA scans all incoming e-mail for viruses on both the server and the workstations
- Desktop Security
 - Anti-Virus and Anti-Spyware tools **are** installed and up-to-date on all workstations
- Cyber Incident Response Team (CIRT)
 - Routinely addresses computer security incidents.
 - Evaluates threats and determines mitigation **factors**
 - Provides immediate diagnostic and corrective actions to prevent the loss of HRSA information
 - Works with United States Computer Emergency Readiness Team (US-CERT) to resolve problems
- Security policies are in place and available to all users

Computer & Internet Usage Policy

- Users may access HRSA information systems only when authorized to do so and for authorized purposes.
- Supervisors should notify the Help Desk (301-496-4357) when access to an information system is no longer required by the user.
- Users may not use a HRSA computer to intentionally access web sites containing pornographic, sexually explicit, suspected terrorist activities or gambling content.
- Any suspected information security compromise should be immediately reported to the Help Desk and the Cyber Incident Response Team.
- Peer-to-peer file sharing software (Kazaa, Morpheus, eDonkey, etc.) is *not* permitted on HRSA computers.
- HRSA retains the right to monitor system access and the usage of workstations and computing resources that the agency provides.

HRSA Password Policy

- Users must use strong passwords that contain:
 - At least 8 alphanumeric characters long
 - At least 3 of the following: uppercase and lowercase characters (A-Z, a-z), numbers and special characters (0-9,#, \$, _, etc.).
- Words such as slang, dialect, or jargon or personal information should not be used.
- Users may not disclose, lend, or otherwise compromise passwords or authentication devices.
- Users shall not re-use passwords among multiple accounts.
- For additional information, consult the HRSA Security Policy located at: <http://intranet.hrsa.gov/OIT/ISS/docs/policy.pdf> or request a copy of the policy from the IT Security Team.

HRSA Privacy Policy

- All system users must exercise due diligence and care in handling HRSA data. Personally identifiable information (PII) involving employees, consumers, and other members of the public (name, address, phone number, SSN, etc.) and other sensitive information needs to be protected.
- PII and sensitive information must be encrypted using a FIPS 140-2 compliant encryption tool when transmitted via email and stored in portable storage devices.
- No PII shall be stored in personal, non-HRSA storage devices.
- PII should only be retained as long as needed and then destroyed.
- For additional information on encryption visit HHS policy at: http://www.hhs.gov/ocio/policy/20070001001s.html#_ftn1

Rules of Behavior

Keep in mind that every time you log onto your workstation, you are using Federal equipment **and information**. Users must follow the HRSA Rules of Behavior (RoB) whenever Federal resources are being used.

The HRSA IT RoB are provided at the end of this course for you to read.



HRSA Sanction Policy

- HRSA employees, contractors and other system users who violate the policies stated in this document, the rules of behavior, or any system-specific policy may be subject to disciplinary action. Depending on the severity of the violation, management has the right to impose any of the following:
 - Reassignment of work duties
 - Disqualification from an assignment
 - Letter of warning
 - Suspension
 - Termination
 - Criminal Sanctions
- For additional information on security policies, consult the HRSA Security Policy located at: <http://intranet.hrsa.gov/OIT/ISS/docs/policy.pdf> or request a copy of the policy from the IT Security Team.

Quiz #1

Which of the following would be considered a good password?

- A. Using your birthday as your password
- B. The word “password”
- C. A word found in the English dictionary containing five characters
- D. A random set of eight characters including numbers, letters, and special characters that is easy to remember but hard to guess

Section 2

Information Security Awareness

- Threats and Vulnerabilities
- Insider Threats
- Cyber Terrorism
- Spyware and Adware

Threats & Vulnerabilities

Information Systems can fall victim to all types of incidents, particularly threats and vulnerabilities.

It is important to understand the difference between threats and vulnerabilities and how they can affect your system.

Threats vs. Vulnerabilities

A Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and/or denial of service.

A Vulnerability is a weakness in a system which allows an attacker to violate the integrity of the system.

Common Threats & Vulnerabilities

Threats

- ❖ Human Threats
- ❖ Inside Threats
- ❖ Global Threats
- ❖ Social Engineering

Vulnerabilities

- ❖ Software bugs
- ❖ Weak Passwords
- ❖ Spyware
- ❖ Viruses, Worms, and Malware
- ❖ Mobile Code

Human Threats

Human threats are caused by unintentional or intentional actions. An unintentional threat is a human input error, bad habit, carelessness, or misinformation. An intentional threat, whether caused by an insider or outsider, can be a spy, hacker, corporate raider, or a disgruntled employee.

The Intruder

- Can be anyone, from a teenager to an advanced and skilled hacker. Even more alarming is that the “intruder” can be either internal or external to your organization, or both.
- Hacking tools can be run from a remote location to detect weaknesses in your system that will enable them to connect to your computer and cause serious damage.



Inside Threats

The insider threat can originate from an employee, contractor, or someone who has legitimate access to a computer system and can exploit weaknesses that can cause grave damage.

Organizations should keep track not only of whom they hire, but also of whom they fire to avoid an insider hacking threat. Terminated employees should be stripped of their physical and computer access at the time of termination to minimize retribution opportunities.

Global Threats

- As the Internet continues to expand, and computer systems continue to become more complex and interdependent, global threats in the form of sabotage or terrorism via cyberspace may become a more serious threat.
- Security experts fear that global threats that result from cyber-terrorism may use similar tactics to attack the critical infrastructure of the United States, causing anything from economic instability to the loss of human life.
- **Cyber-terrorism** involves the leveraging of a target's computers and information systems via the [Internet](#), to cause physical, real-world harm or severe disruption of infrastructure.

A Recent Example of a Global Threat

Ring invaded computers in 100 countries, police say

TU THANH HA

From Thursday's Globe and Mail

February 21, 2008 at 4:45 AM EST

MONTREAL — From their homes in small towns such as Notre-Dame-du-Portage or Jonquières, a handful of young Quebec hackers took control of tens of thousands of computers in countries from Poland to Brazil, police allege.

In what the Quebec provincial police say is a first in Canada, they have cracked an alleged ring of 17 hackers, saying it inflicted \$45-million in damage in 100 different countries.

The scope of the ring's actions was "500 times more powerful than Mafiaboy," said police Captain Frédérick Gaudreau, alluding to the infamous Montreal hacker who disrupted Amazon, eBay and CNN websites.

Police were reluctant to reveal details, but said the accused planted hidden software called computer worms or Trojan horses on personal, corporate and governmental computers.

Social Engineering

What is it?

- “Social Engineering” is the use of any technique that takes advantage of a trust relationship, no matter how tenuous, to obtain information used to compromise a system or obtain sensitive data. The goal is to trick people into revealing passwords and other information that can be used to compromise the security of their systems.
- A Few Social Engineering Techniques:
 - Phishing e-mails
 - Spoofing e-mails
 - Spamming e-mail accounts, faxes, cell phones (i.e., Nigeria Scam)

Phishing

- Phishing refers to an individual's attempt to fraudulently acquire sensitive information, such as passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. There are three main types of phishing:
 - **E-mail** - Junk emails that contain links to fraudulent websites that mimic legitimate websites to trick the user into entering their personal information.
 - **Spoofing e-Mail** - E-mail that appears to be from a legitimate organization, like the HRSA. The e-mail usually contains an attachment that, if opened, plants a Trojan or virus.
 - **SPAM** - Emails that ask you to reply with your username and password. Most companies will NOT ask for your password through emails!

Phishing @ IRS

GCN Home > 02/20/08 web stories

(Don't) Click here for a tax refund

The number of fake IRS phishing sites has increased twelvefold in the last year

By [William Jackson](#)

 Story Tools: [Print this](#) | [Email this](#) | [Purchase a Reprint](#) | [Link to this page](#)

More on this topic from GCN

Be careful what you 'vish' for

Tech blog | Spam as economic stimulus

The Internal Revenue Service has become a popular brand with phishers, and with tax season under way we probably can expect to see plenty of e-mails purportedly from the IRS offering help with refunds and directing us to suspect Web sites.

In January, one anti-spam company reported that phony IRS e-mail accounted for 1 percent of all spam, Treasury Special Agent Andy Fried

said Wednesday at the Black Hat Federal Briefings in Washington.

Phishing is the practice of directing computer users to malicious Web sites, often with official-looking e-mails with spoofed sender addresses, so that malicious code can be loaded on the victim's computer or personal and financial information can be stolen.

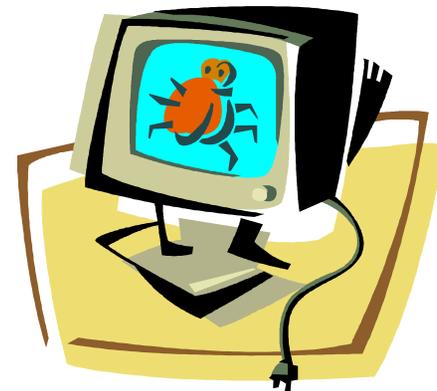
Hoaxes

- Internet hoaxes involves e-mail messages written with the purpose of spreading false information, raising false alarms or extorting money. Some hoaxes warn of “new” viruses or promote moneymaking schemes or ask to forward their message to all in the name of a fictitious cause.
- Hoaxes often slow down the Internet and e-mail services for computer users by creating additional network traffic.
- HHS Policy on email states: E-mail spamming (unsolicited commercial e-mail) - sending or forwarding chain letters, other junk e-mail, or inappropriate messages- is not permitted.

If you receive an e-mail message that asks you to forward it to all your friends and coworkers, take the time to check the facts. For additional hoax information, visit the [U.S. Department of Energy: http://www.cio.energy.gov/cybersecurity/chainmail.htm](http://www.cio.energy.gov/cybersecurity/chainmail.htm).

Software Bugs

A **software bug** is an error, flaw, mistake, failure, or fault in a computer program that prevents it from behaving as intended, producing an incorrect result. Most bugs arise from mistakes and errors made by people in either a program's source code or its design.



Spyware

- **Spyware** is now the greatest threat to the integrity and security of your workstation/laptop. Spyware can gather user information through the user's Internet connection without a users knowledge, usually for advertising purposes. There are 4 types of Spyware:
 - **System Monitors** – log activities pose the greatest threat to privacy and data, including key loggers. Estimates are that 1 in 15 computers is infected with a system monitor of some kind.
 - **Trojan Horses** – generally manage files on the computer. Spyware can move, modify, delete or rename. One (1) in five (5) computers is infected.
 - **Adware** – changes your home page, provides pop-up and pop-under ads, redirects web searches, generally slows computer performance. One in two computers has a form of adware.
 - **Tracking Cookies** – monitors Internet use and reports web sites visited to an outside server. Almost 100% of computers have tracking cookies with an average of 20 on each machine.

Viruses, Worms & Malware

- A **virus** is a computer program that can copy itself and infect a computer without the knowledge or permission of the user. The most common ways a virus can spread from one computer to another are through a user sending it over a network, by the Internet, by carrying it on removable media (floppy disk, CD, USB drive), or by email attachments or downloading files from the Internet.
- A **worm is** a self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
- **Malware or Malicious Code** is software capable of performing an unauthorized function on an information system. It is designed with a malicious intent to deny, destroy, modify or impede systems configuration, programs, data files, or routines.

E-mail Attachments

- One of the most common ways a user gets a virus, worm or trojan horse is by downloading it from an attachment in an email. They can corrupt files, erase your hard drives, or even allow a hacker to gain access to the computer.
- Use caution when opening e-mail attachments. Be wary of attachments that end in .exe, .cmd, .com, .vbs, .bat, .pif, .Trojan, .reg, .hta, .scr, or .shs.
- Do not assume that an email attachment is safe because a friend or coworker sent it. If you are unsure, reply with a new email (i.e., do not use the “reply” button) to double check that your friend/coworker sent the attachment on purpose. Always scan all attachments with updated anti-virus software before opening.

Mobile Code

- **Mobile Code**, such as ActiveX and JavaScript, are technologies used for interactive Internet applications. Because mobile code embedded in a web page runs on the user's machine (as opposed to run on the Web server) it can recognize and respond to user events such as mouse clicks, form input, and page navigation.
- Users should be very cautious about visiting unfamiliar websites. All popular browsers have options to disable JavaScript and Internet Explorer has options to prevent ActiveX controls from running.

Quiz #2

Social engineering tries to exploit weaknesses found in _____.

- Computer software
- Computer hardware
- Human nature
- The internet

Quiz #3

True or False. Cookies are not able to track your activities on the Internet.

- A. True
- B. False

Section 3

Technology-Specific Security

- P2P Communications
- Other Security Concerns

Peer-to-Peer Communications

Peer-to-Peer communications is a violation of the HRSA security policy!

- Peer-to-peer (P2P) communications is a type of network that allows computers to directly connect with each other and share files. Computers have an equal level of authority on a P2P network and therefore eliminate the need for central servers, posing a serious security threat.
- In recent years, P2P applications have gained tremendous popularity among Internet users because of the convenience of file sharing. Some of the most popular files include copyrighted songs, videos, and movies, which are illegal in most jurisdictions and are punishable by Federal law.
- Common P2P applications include: Kazaa, Kazaa Lite, Napster, OpenNap, GUNet, Limewire, Gnutella, and BitTorrent.

Fax Machines

Faxes can be looked at as regular e-mail; data is often sent without concern for privacy and/or authenticity.

Many business fax machines have large amounts of memory which can make it possible to collect historical data (i.e. all faxes sent in the last 30 days).

Exercise caution when transmitting information over a fax machine and ensure that the machine complies with FIPS 140-2 before sending out sensitive information or PII.

Cell Phone

Remember that cell phones are nothing more than glorified transmitters. Anyone, given the right equipment, could potentially listen to your conversation. Whenever possible, use a landline phone and *never* discuss classified or sensitive information **over** a cell phone.



Portable Electronic Storage Devices

Portable electronic storage devices (e.g., PDAs, thumb drives, blackberries) pose serious security threats for their small size, storage capacity and ease of use. These devices make it easy for a person to download information from a computer or upload malicious code.

All portable electronic storage devices must be issued by HRSA and must be encrypted using a HRSA approved software, such as PKZIP if they contain sensitive information or PII. PII may not be stored on personal storage devices.

System owners shall obtain written authorization from the Chief Information Officer (CIO) if compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a mission or business function.

Laptops

As we all are very much aware, the convenience of laptops also makes them vulnerable to theft and security breaches. The following are some general guidelines for using a laptop:

- Use caution when displaying information on your screen, especially in close quarters, such as airplanes and public hotspots. Consider some type of screen guard to reduce the threat of shoulder surfing.
- Be aware of your laptop when traveling to prevent theft. *Never* leave your laptop in a vehicle or public area unattended!
- Make sure your laptop has up-to-date anti-virus and anti-Spyware software.
- If storing PII or other sensitive information, ensure your laptop is equipped with a FIPS 140-2 compliant tool, approved by HRSA.
- Back up your laptop on a regular basis to avoid loss of information.

For additional information on laptop security, visit:

http://www.hhs.gov/ocio/securityprivacy/laptop_computer_security.pdf 41

Quiz #4

When using a laptop, which of the following options should you avoid?

- A. Protecting the information from public view when in close quarters, such as airplanes.
- B. Leaving the computer unattended in public areas or in a car.
- C. Ensuring the computer contains updated anti-virus software.
- D. Encrypting PII and sensitive information.

Section 4

Cyber Security Incident Response

Cyber Incident Response

HRSA employs a cyber security **incident response process** to detect, analyze, respond and report incidents to management and legal authorities.

HRSA also has a Cyber Incident Response Team (CIRT) responsible to disseminate incident information, and respond to incidents as they occur in a consistent fashion.



Security Events and Incidents – What's the Difference?

- There are generally two types of potential violations: an “event” and an “incident”. The difference between the two is the impact or adverse affect on the Agency and how it should be handled.
 - ✓ **Incident** - Any real or suspected adverse event in relation to the security of computer systems or computer networks. An incident also refers to the violation, or imminent threat of violation of an explicit or implied security policy, acceptable use policies, or standard security practices.
 - ✓ **Events** - certain natural adverse events, such as floods, fires, electrical outages, and excessive heat that can cause a system to crash.
- *Note: **Events** are detected and classified in the same way as incidents, but may impact the systems differently.*

Examples of Incidents

Unauthorized Access

- Involves improper use of a valid account or unauthorized access to files and directories stored on a system or storage media.

Unauthorized use of services

- Conducting unlawful, disruptive, or other malicious activities within or outside an HHS or HRSA computing environment.
- Using abusive language in transmitting public or private messages.
- Surfing inappropriate Web sites.

Unauthorized Changes

- Unauthorized modification of Web content or defacing a website.
- Unauthorized alterations or compromise by an individual who either inadvertently or intentionally changes, releases, or steals information.

Incident Reporting

Ten things you can do when an incident occurs:

1. Report the incident immediately to the OIT CIRT, Security Team, or Helpdesk (301-496-4357).
2. Pinpoint the machine that has suffered an incident.
3. Lockdown the machine/office. Allow NO ONE to logon or enter the office.
4. Leave the system connected but make no changes to the system.
5. Assist the OIT CIRT in resolving the incident.
6. Provide all requested materials (i.e., event logs, firewall logs, etc.).
7. Answer all questions from HRSA OIT CIRT.
8. Follow recommended mitigation steps.
9. Report when system has been restored to the OIT Security Team.
10. Obtain a final incident report from the OIT CIRT/Security Team for your records.

Cyber Incident Response Team

The following are the CIRT members and their contact information:

- Doug Burgess (Team Lead)
301-443-9644 or DBurgess@hrsa.gov
- Steve Davis (CISO)
301-443-9660 or SDavis@hrsa.gov
- Lynn Dennie (Network/Helpdesk)
301-443-9283 or LDennie@hrsa.gov
- HRSA Helpdesk
301- 496-4357 or Helpdesk@nih.gov

Quiz #5

While using Federal IT resources the following are all inappropriate activities except:

- A. Occasionally checking personal e-mail
- B. Using e-mail for solicitation or spam
- C. Introducing malicious code
- D. Gambling on the Internet

Quiz #6

If an incident occurs, you need to do the following:

- A. Notify the Helpdesk
- B. Lock the computer and office immediately
- C. Notify the Cyber Incident Response Team
- D. All of the above

Section 5

Privacy Awareness

- ❖ What is Privacy and Why is it Important
- ❖ Privacy Legislation

What is Privacy?

- **Privacy** refers to a set of fair information practices to ensure that an individual's personal information is accurate, secure, current, and that individuals know about the uses of their data.
- **Privacy** also involves the protection of PII, which can be used to identify, contact, or locate the person to whom such information pertains

Why is Privacy Important to HRSA

- Identity theft, perhaps the most damaging consequence of poor privacy and security practices, continues to increase progressively. You are also responsible for protecting sensitive information and PII involving employees, consumers, and other members of the public.
- Privacy breaches cause consumers, citizens, and, in the case of Federal departments and agencies, perhaps Congress, to lose trust.
- Keep in mind that your right to privacy is limited when using Federal IT resources. When you log on to a government system, you give your consent to monitoring. Everything you do can be monitored and tracked.
- For additional information on privacy, consult the privacy flyer located at: <http://intranet.hrsa.gov/OIT/pdf/privacyFlyer.pdf>

Privacy Legislation

The purpose of federal privacy legislation is to ensure fairness. The following are Privacy Laws that apply to all HRSA system users:

- **Privacy Act of 1974:** provides guidance for the collection, use, management, and disclosure of PII
- **E-Government Act 2002, Title II and III:** guidance for agencies to assess impact of privacy for systems that collect data about members of the public
- **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule:** restricts use and disclosure of personal health information and grants individuals access to records
- **Children's Online Privacy Protection Act (COPPA):** requires parental consent for certain websites who knowingly collect PII on children under the age of 13
- **Agency Guidance:** regulatory agencies provide guidance to implement privacy legislation

Sensitive Information

Information is considered sensitive if *the loss of **confidentiality, integrity, or availability** could be expected to have a **serious, severe or catastrophic** adverse effect on organizational operations, assets, or individuals.*

Do not base the sensitivity of information on personal judgment; information can be viewed differently by all users. When in doubt, contact the HRSA IT Security Office before sending/handling questionable data.



Personally Identifiable Information (PII)

PII is any information that can be used to identify, contact, or locate an individual.

PII may include, but is not limited to:

- Home Phone Number
- Social Security Number
- Photographic Identifier (e.g., photo, x-ray, video)
- Financial Account Information and/or Number
- Driver's License
- E-mail Address
- Date of Birth
- And more

For a complete list, please contact the OIT Security Team at ITSecurity@HRSA.gov

Quiz #7

True or False. When using federal-issued computers and equipment, your right to privacy is fully protected and the federal agency cannot monitor or track your usage.

- A. True
- B. False

Quiz #8

Which one of the following is not a form of PII?

- A. Work phone number
- B. Home address
- C. Social Security Number
- D. All of the above

Section 6

What Can You Do To Keep Information Secure?

Prevent Inside Attacks

- Be aware of your surroundings and report suspicious behavior such as "shoulder surfing" or unauthorized persons using a restricted computer.
- Report any suspicious user activity to the Helpdesk immediately.
- Managers, notify the system administrator immediately when an employee has been terminated or laid off so that the user account can be disabled.
- Managers, secure the system and all information of a disgruntled employee immediately.

Protect Your Passwords

- Follow HRSA's policy on creating strong passwords.
- Memorize your password! Don't write down or share your password or user-id!
- NEVER use a password that has been shown as an example on ANY website.
- Do NOT use personal information or anything related to your interests and avoid using words or phrases that can be found in a dictionary.
- Change your password immediately if you think it has been compromised.

Be Aware of Social Engineering

- Verify the identity of all callers.
- Don't give out information about other employees, including names and positions.
- Be cautious about opening attachments to e-mail that you were not expecting.
- Ensure that virus protection software is up to date on both your workstation and any device connected to the HRSA system.



Keep Information Safe

- Protect your information! Lock your workstation every time you leave it unattended and place PII in a locked drawer if away from your desk
- Dispose un-needed or unwanted documents or media containing PII appropriately
- Promptly pick up documents containing PII or sensitive data after printing
- Do not send sensitive information or PII via e-mail unless encrypted with a HRSA approved tool. **Do not use WinZip as a form of encryption!**
- Do not store sensitive information or PII on portable or external storage devices unless encrypted and approved by HRSA. Do not store PII on personal portable storage devices.
- **Think before you share any information;** maybe a co-worker needs your name and phone number, but do they really need your SSN?

For additional information on information safety, visit the HRSA Intranet site at <http://intranet.hrsa.gov/broadcast/protect.asp> or send an email to ITSecurity@HRSA.gov

Common Sense Rules

- **Do NOT** use a computer to harm other people.
- **Do NOT** use a computer to steal.
- **Do NOT** attempt unauthorized access of information.
- **Do NOT** snoop in other people's files.
- **Do NOT** steal other people's intellectual property.
- **Do NOT** send threatening, obscene, harassing, intimidating, abusive, sexual, or offensive material to or about others
- **Do NOT** use abusive or objectionable language.

Congratulations!

You have just completed the 2008 HRSA Information Security Awareness Training!

If you have any questions about this training or want to report security infractions or suspicious behavior, please contact:

HRSA IT Security Team

Steve Davis, CISO	(301) 443-9660
Sharon Kelser	(301) 443-9399
Doug Burgess	(301) 443- 9644
Rodney Washington	(301) 443-6104
Donald Palmer	(301) 443-0545
Margarida Nighswander	(301) 443-3359
Roey Katz	(301) 594-4213

or
Help Desk
(301) 496-4357

Please read and sign the Rules of Behavior.

Note: You **MUST** sign the Rules of Behavior to receive credit for the 2008 HRSA Security Awareness Training.