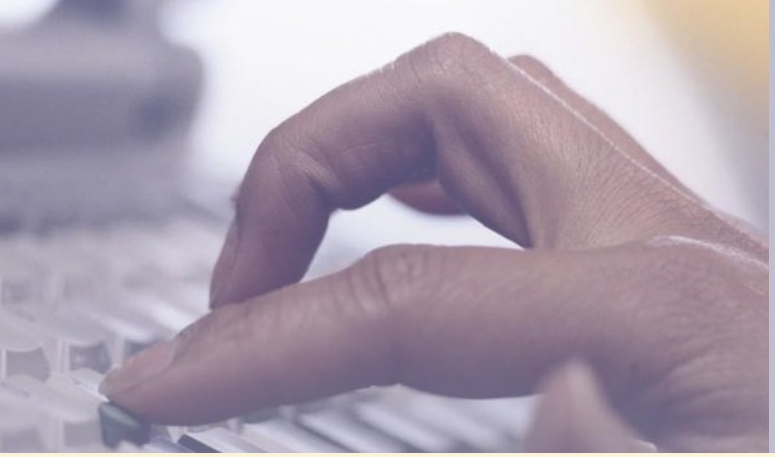
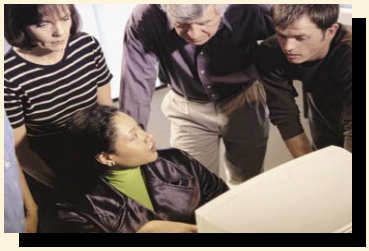


Quick Guide to Information Security

Indian Health Service Information Security Program

All Indian Health Service (IHS) users, including employees, contractors, interns, students, volunteers, and any others who have access to IHS information resources must take the Information Systems Security Awareness (ISSA) training when they begin work and again annually. When necessary, new employees may review this pamphlet instead of immediately taking the training. However, **in all cases, users must take the ISSA online training (http://www.ihs.gov/ISSA/) within 30 days of appointment or risk losing IHS system access**.



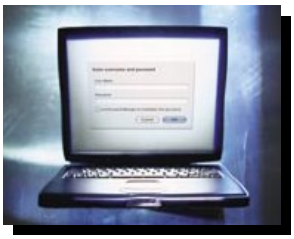
Information and Data Protection

- Adequately protect any sensitive information entrusted to you.
- Secure sensitive information when you leave it unattended, and keep it out of sight when visitors are present.
- Only use sensitive information or Personally Identifiable Information (PII) for the purposes it was collected for and in ways defined by conditions set forth in stated privacy notices and published System of Records Notices.
- Do not share or disclose sensitive information except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Do not store sensitive information in public folders or other insecure physical or electronic storage locations.
- Do not knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for your own purposes or for others.
- Store critical files on the network drives, where they are automatically backed up and available for recovery, if needed.

Work Space Protection

- Log off or lock systems when you leave them unattended.
- Do not use another person's account, identity, or password.
- Protect removable media and mobile devices (for example, laptop, blackberry, USB stick); do not leave them unattended, and lock them up or hide them when they are not in use.

Password Protection



Users must ensure that their passwords:

- Are complex, with a minimum of eight alphanumeric characters, including at least one uppercase and one lowercase letter, one number, and one special character.
- Do not contain common words found in any dictionary.
- Are not passwords that incorporate personal data elements (for example, user's name, date of birth, address, telephone number, or Social Security number; names of children or spouses; favorite band, sports team, pet, or automobile).
- Are changed at least every 60 days.
- Are not reused until at least six other passwords have been used.
- Are changed immediately in the event of known or suspected compromise, and immediately upon system installation (that is, immediately reset default or vendor-supplied passwords).
- Are committed to memory or stored in a secure place.
- Are not posted or shared with others.
- Are not the same passwords used for external, person accounts

Email Usage

- Use caution with all email attachments, and do not open emails or attachments from unknown sources or that have unusual subject lines.
- Report malicious/spam emails to your Help Desk or ISSO.
- Do not forward chain letters.

Internet Usage

- Do not use the Internet for games, chat rooms, or gambling.
- Do not use peer-to-peer (P2P) file sharing software or functionality.

Resource Usage

- Do not use another person's account or identity.
- Do not attempt to break into another computer (federal or private) that is not assigned to you.
- Do not send, retrieve, view, display, or print sexually explicit, suggestive text or images, or other offensive material.

Hardware and Software Usage

- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and is appropriately authorized before you install and use it on IHS systems.
- Protect IHS information assets (IHS assets include, but are not limited to, hardware, software, and federal

records) from unauthorized access, use, modification, destruction, theft, or disclosure.

- Dispose of all electronic storage media such as CD-ROMS, thumb drives, diskettes, or other rewritable media and hard-copy media in accordance with IHS sanitation and disposal procedures, which include destroying hard copies of sensitive data by pulping, burning, or cross-cut shredding.
- Obey software license restrictions.
- Do not connect unauthorized hardware to your computer or the IHS network.
- Report lost or stolen IT equipment immediately to your ISSO or the IHS Incident Response team (IRT).

Privacy Protection

Privacy policies and procedures require you to:

- Collect, use, and disclose personal information only for reasons that are legitimate to your job function, that support the mission of IHS, and that are allowed by law.
- Disclose only the minimum amount of information.
- Access information only for authorized purposes.
- Follow standards to safeguard personal information throughout the information life cycle.
- Report suspected privacy violations or incidents to your ISSO or the IHS IRT.
- Comply with all applicable privacy laws.

Incident Response

If you think your system is infected with a virus:

- Stop—Do NOT turn off your computer or answer any prompts. DO lock the system (for example, in Windows press Ctrl+Alt+Delete and then click **Lock Computer**).
- Take notes—Include what happened, the program used, file name, symptoms, and messages or warnings you received.
- Get help—Contact your Site Manager or local ISSO. If they cannot be reached, contact the IHS IRT.
- Be patient—Do NOT try to fix the problem yourself.

Phishing Protection

- Do not click on hyperlinks within an email message if you suspect the message is not authentic.
- Do not give people or businesses your password, login name, Social Security number, or any other personal information through email.
- Examine a site's web address carefully.
- Be suspicious of any email message with an urgent request for personal or financial information.

Employee and Visitor Access

- Wear identification badges at all times in federal facilities.
- Protect your employee or visitor badge, and do not loan it to anyone.
- Report unusual activity to your supervisor, ISSO, or security guards.
- Do not permit entry to someone who has no employee or visitor badge.
- Challenge unescorted strangers who do not have a valid employee or visitor badge.

HIPAA and HITECH

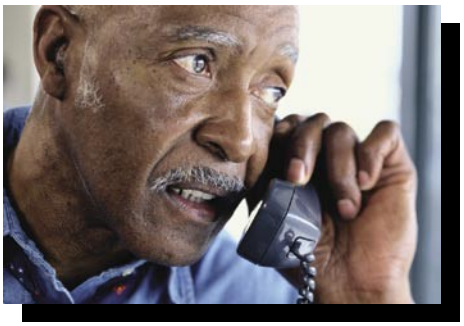
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule took effect on April 14, 2003. The Department of Health and Human Services (HHS) developed this regulation to protect the confidentiality of medical records. Many consider the Health Information Technology for Economic and Clinical Health (HITECH) Act to be an enhancement or update of HIPAA. In addition to an increase in fines, the HITECH Act also subjects both covered entities and business associates to civil monetary penalties for Protected Health Information (PHI) breaches or violations, even if those entities and business associates were unaware of the violation. Many scenarios could lead to the unauthorized disclosure of PHI.

The following is a non-exhaustive sample of violations of the HITECH Act:

- Not installing encryption on mobile devices containing PHI.
- Sharing user credentials with others.
- Losing mobile devices containing PHI or having mobile devices that contain PHI stolen.
- Emailing PHI in an unencrypted state.

Who must abide by HIPAA and HITECH?

- ALL IHS staff, including employees, contractors, and interns, must follow HIPAA and HITECH regulations related to the security of PHI and sensitive information.
- If you suspect a HIPAA or HITECH violation, contact your ISSO, Site Manager, or HIPAA Coordinator immediately.



My Help Desk contact information is:

Telephone Number: _____

Location: _____

My ISSO is:

Telephone Number (Primary): _____

Telephone Number (Alternate): _____

IRT Contact:

Email: IRT@ihs.gov

During Business Hours:
505-248-4464, 505-248-4396, or 505-248-4166

After Business Hours:
702-562-8201 (NOSC) or 1-888-830-7280 (IHS Help Desk)

Incident Reporting Form:
http://home.ihs.gov/ITSC-CIO/oit_tfs/documents/forms/F07-02b_IRF.doc