QUICK GUIDE TO INFORMATION SECURITY

All Indian Health Service (IHS) information system 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 then again annually for the length of their tenure at IHS. When the online course is unavailable or if IHS job duties prevent an employee from accessing the online course, new employees may review this pamphlet instead of immediately taking the online training.

IHS system users will often find themselves dealing with sensitive information. Information is considered sensitive when mishandling it could compromise confidentiality and affect national health interests, IHS programs, or the privacy of individuals.

Two types of sensitive information are particularly common at IHS:

Protected Health Information (PHI) may include anything in the patient health records such as:

- Lab results
- Medical history
- Images

Personally Identifiable Information (PII) includes:

- Name
- Date of Birth
- Social Security Number
- Email addresses
- Any information that can be used to steal a patient's identity

THINGS YOU MUST DO

As an IHS system user, you MUST:

Protect Information and Data

- Protect any sensitive information entrusted to you. Keep it out of sight when visitors are present.
- Collect sensitive information only as allowed by IHS and use it only for the purposes it was collected.
- Do not share or disclose sensitive information except as authorized and with formal agreements that ensure that third parties will adequately protect it.
- Do not knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information.
- Do not store sensitive information in public folders or other insecure storage locations.

Protect Your Workspace

- Keep your PIV card with you and don't let anyone else use it.
- Log off or lock systems when you leave them unattended.
- 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.
- If you take government-furnished equipment out of the workplace, be extra vigilant in protecting it.
- Protect removable media and mobile devices (for example, laptop, tablet, USB drive); do not leave them unattended, and lock them up or hide them when they are not in use.
- Do not connect personally-owned portable media like flash drives to any IHS system without written approval.
- Secure IHS-issued portable media when not in use.
- Don't leave hard copies of sensitive information lying around, and lock them up when you leave for the day.

Protect Your Password

- Have a complex password that meets current IHS standards and does not contain common words or personal data.
- Change your password at least every 60 days.
- Do not reuse until at least six other passwords have been used.
- Change immediately upon system installation (that is, change default or vendor-supplied passwords immediately).
- Change in the event of known or suspected compromise.
- Commit to memory or store in an approved password manager. Don't store passwords in files labeled "passwords."
- Do not post, share with others, or leave in plain sight.
- Use unique passwords, never ones used for personal accounts.

Protect the Privacy of Others

- Disclose only the minimum amount of information.
- Access information only for authorized purposes.
- Follow standards for safeguarding sensitive information.
- Report suspected privacy violations or incidents to your ISSO or the IHS Cybersecurity Incident Response team (CSIRT).
- Comply with all applicable privacy laws. For more on this, see the yearly mandatory privacy training available here: https://www.ihs.gov/privacytraining/index.cfm

Use Email and the Internet Appropriately

- Exercise caution with all email attachments, and do not open emails or attachments from suspicious sources,
- Report suspicious emails to the IHS CSIRT or ISSO.
- Do not forward chain letter emails.
- Do not use the Internet for games, chat rooms, video or music streaming, or gambling.
- Do not use peer-to-peer (P2P) file sharing software.
- Do not use social media on IHS equipment or networks unless you have a specific business need and prior management approval.
- Never post IHS information to external newsgroups, social media, public forums, or any websites without approval.
- Do not send, retrieve, view, display, or print sexually explicit or suggestive text or images, or any other offensive material.

THINGS YOU MUST PROTECT

Physical Access of Employees and Visitors

You must wear your identification badge (PIV Card) at all times in federal facilities. It will grant you access to the building and to your computer. Protect your badge, and do not lend it to anyone. Report any unusual activity you encounter to your supervisor, ISSO, or security guards. You must not permit entry to secured areas to someone who has no employee or visitor badge. And you should challenge unescorted strangers who do not have a valid employee or visitor badge.

Hardware and Software

You must 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. To do so, familiarize yourself with and obey software license restrictions. You must also protect IHS information assets (IHS assets include hardware, software, and federal records) from unauthorized access, use, modification, destruction, theft, or disclosure. Do not connect unauthorized hardware to your computer or the IHS network. Be sure to immediately report lost or stolen IT equipment to your local ISSO or the CSIRT. Dispose of all electronic storage media such as CD-ROMS, thumb drives, disks, or other rewritable media and hard-copy media in accordance with IHS sanitization and disposal procedures. For example, destroy hard copies of sensitive data by pulping, burning, or cross-cut shredding.

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 of or update to HIPAA. In addition to increased fines, the HITECH Act 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. For more on HIPAA and HITECH, see the yearly mandatory privacy training available here: https://www.ihs.gov/privacytraining/index.cfm.

Phishing Protection

You will likely encounter “phishing” attempt emails that will try to trick you into revealing sensitive information or installing malware. You must protect IHS information technology systems by never clicking on hyperlinks within an email message if you suspect the message is not authentic. If you hover your mouse over a link, you can see the website the link will take you to, but be careful not to accidentally click it. Examine a site’s web address carefully. If you are unsure if the website is legitimate, don’t take the risk of clicking it. Infecting an entire organization starts with one person clicking on a phishing email. If you aren’t sure about a hyperlink, check with your local ISSO or the CSIRT.

You should also protect your password, login name, Social Security number, and any other personal information by not revealing them to outside entities via email. Be suspicious of any email message with an urgent request for personal or financial information.

Here are some warning signs that an email might be a phish, in which a malicious actor attempts to get your private information:

- Unknown sender
- Poorly written message or writing errors
- It doesn’t address you by name
- It appeals to your sense of curiosity or urgency

Note that even an email without these warning signs may still be a phish.

If you suspect an email is a phish, don’t click any links or attachments. Don’t reply. Forward the email to Incident@ihs.gov or report the incident using the IHS CSIRT Ticketing System: https://hqabqdispswhd01.d1.na.ihs.gov

WHAT TO DO IN A SECURITY INCIDENT

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 - Record what happened, the program used, file name, symptoms, and messages or warnings you received.

GET HELP - Contact your Site Manager or local ISSO. If you cannot reach them, contact the IHS CSIRT.

Be patient - Do NOT try to fix the problem yourself.

If you think your system is infected with a virus, email Incident@ihs.gov from someone else’s computer.

Cybersecurity Help Desk Email: Cybersecurity@ihs.gov

Cybersecurity Incident Response Team Contact Information:
Email: CSIRT@ihs.gov
Call 24/7: 702-562-8201 (NOSC)

Incident Reporting Form:
Online: https://hqabqdispswhd01.d1.na.ihs.gov
Printable document: https://home.ihs.gov/sites/oittfs/themes/ihs-intranet-theme/display_objects/documents/forms/F07-02b_IRF.pdf

Important Contact Information

Help Desk Telephone Number or Email:	
My local ISSO is:	
ISSO Telephone Number or Email:	

Employee Signature / Date

Updated 4/2/2021