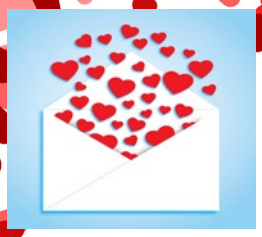

Give Love *not* Sensitive Information!

Office of Information Technology
Division of Information Security
FEBRUARY 2022

Sensitive Information

The Health Insurance Portability and Accountability Act (HIPAA) requires that we protect the confidentiality, integrity, and availability of sensitive information by administrative, technical, and physical safeguards to protect national health interests, IHS programs, and the privacy of individuals. One type of sensitive information common at IHS is Protected Health Information (PHI). PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual that is created, collected, or stored by any entity covered by HIPAA. Note that this includes any business associates of those covered entities. (https://www.hipaajournal.com/what-is-protected-health-information/)

The government also requires that IHS protect Sensitive Personally Identifiable Information (SPII). SPII is information that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. (https://intranet.hhs.gov/sites/default/files/s3fs-public/s3fs-public/2020-03/sensitive-pii-definition-and-guidance-memorandum.pdf) Social Security or driver's license numbers are examples of SPII.

IHS Email

IHS does not encrypt email correspondence by default, so anyone who intercepts email transmissions can read them. If you need to send sensitive information, you must use either email encryption or the IHS Secure Data Transfer Service (SDTS). Directions on how to use these methods are located at: https://youtu.be/cn0sh8k8OSM. If you need assistance with IHS email encryption or the SDTS, contact your local IT staff.

Personal Email

Most email providers don't encrypt personal email accounts by default either. If you have initiated communication with a store, clinic, bank, or any organization, don't email your credit card or checking account numbers, or any information you wouldn't want to be at risk of

being intercepted. Legitimate organizations will provide a method for customers to transfer their private information over the internet in a way that is more secure than unencrypted email.

You may have noticed the previous paragraph specified that you initiated the communication. If what appears to be an organization initiates communication with you asking for sensitive information (whether through email, phone call, or mail), it may actually be a scammer claiming to be the organization. If you receive an email that asks you for sensitive information, don't reply. Instead, initiate a new communication using the organization's official contact information and ask about the request you received.

If your family has a shared account for a service, would you email the user name and password to a family member? Remember, it's possible for a hacker to intercept that email and then log in to your family's account! Tell your family member in person or over the phone instead.

Quick Tips

Please consider the following tips when handling sensitive information in your possession.

- Position monitors so curious eyes can't see the screens.
- Use privacy screens over monitors when appropriate.
- Securely store hardcopies when not in use.
- Don't upload work data to your personal devices.
- Ensure physical security of mobile devices and portable media.
- Immediately retrieve sensitive information from printers and fax machines.
- Use secure wireless networks and not public Wi-Fi.
- Use IHS-approved means to shred or otherwise destroy sensitive information.
- Do not upload sensitive information to unapproved cloud applications (Dropbox, Google Drive, etc.).
- Contact local IT staff for assistance with deleting sensitive information from portable media or mobile devices.

ISSA Training

The FY 22 IHS Information Systems Security Awareness (ISSA) Training has further information on protecting sensitive information. The training is located at www.ihs.gov/ISSA and the deadline to complete this year's training is Friday, June 3, 2022.

Using the information here can help to make sure you're loved for your personality, not personal information. If you have any questions, contact Cybersecurity@ihs.gov. Report any suspicious events or activities to Incident@ihs.gov.