Protecting Sensitive Information Training Module

Protecting Sensitive Information

Next Scene

**Woman:** IHS’s mission is jeopardized when its information and IT systems are not protected. So federal law AND HHS and IHS policy require you to take Information Systems Security Awareness (ISSA) training to learn about your information security role and responsibilities. In this course we will introduce some important security concepts, as well as more security resources located on the web.

**Man:** But don’t worry about writing all the links down. They’re attached to the Rules of Behavior (RoB), which we emailed you when you agreed to the RoB earlier.

Next Scene

**Man:** So what’s the information we have to protect?

**Woman:** Sensitive Information!

Next Scene

Information is considered sensitive when its loss, misuse, unauthorized access, or modification could compromise confidentiality... and affect national health interests, IHS programs, or the privacy of individuals entitled under the Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA).

Next Scene

**Man:** The Resource and Patient Management System (RPMS) contains a lot of sensitive information.

Next Scene

Sensitive Information May Include:

- Financial Data
- Personnel Information
- Patient Information
- And more!

Next Scene
Sensitive information, when compromised, can have devastating long-term effects on patients and can erode the public trust.

It is media neutral and can be electronic or hardcopy.

It must be protected by administrative, technical, and physical safeguards...IT’S THE LAW!

Next Scene

Two types of sensitive information are particularly common at IHS:
- Personally Identifiable Information (PII) and Protected Health Information (PHI)

Next Scene

PII is
- Information about a person that can be used to distinguish or trace their identity.
- (Whether by itself or when combined with other data.)

PHI is
- Information about a person’s health, healthcare, or payment for healthcare that can be linked to a specific person.
- (Like any part of their medical history, whether spoken or documented.)

Next Scene

PII includes:
- Education, criminal, or employment history.
- Name, Social Security number, or date or place of birth.
- Mother’s maiden name.
- And biometric records.

PHI includes:
- Medical information created, received, transmitted, or maintained by IHS.
- Past, present, or future physical or mental health condition.
- And past, present, or future healthcare or payment for healthcare.

Next Scene

Woman: Sensitive information also includes...employee records, disaster recovery plans, facility blueprints, and more. And we count on you to help protect it!

Man: A breach can have serious ramifications. And the most common type of breach is employee error.
Woman: Sensitive information can be found everywhere….Filing cabinets, emails, portable media, or computer workstations. It must be protected in ALL formats.

Man: So how can we protect it?

Next Scene

Here’s what you can do!

Never send unencrypted emails that contain PII/PHI or forward such emails to personal accounts. And NEVER upload PII/PHI to unauthorized online storage sites.

Woman: This includes unapproved cloud services.

Next Scene

Any release of sensitive information must be tracked and approved locally and may be sent via email ONLY with FIPS 140-2 approved encryption methods, like PIV card encryption or the Secure Data Transfer Service (securedata.ihs.gov).

Next Scene

Here’s what else you can do!

Take care not to lose computer equipment, mobile devices, portable media, or hardcopy files that contain sensitive information.

Next Scene

Store sensitive materials in locked spaces when not in use and retrieve them immediately from printers and fax machines. Upload sensitive computer files to the network drive where they will be automatically backed up, rather than storing them locally on your computer.

Next Scene

Here’s what else you can do!

Use appropriate methods when disposing of sensitive information.

Next Scene

When no longer needed, sensitive data must be properly destroyed. Contact your local IT department to get rid of computer data, and destroy printed data by means of shredding, incinerating, mashing, or pulverizing. For more procedures, contact your local IT department.
IHS policy requires our business partners to protect our sensitive information too. A written Interconnection Security Agreement (ISA) must be in place between IHS and every organization we have a network connection with (like business partners and Tribal sites). ISAs outline the terms and conditions of interconnection and specify the procedures required for protecting the data.

**Man:** ISA and Memorandum of Understanding (MOU) forms can be found at home.ihs.gov/security.

*Next Scene*

Any time you have a question, please contact your local IT staff. If they don’t have all the answers, they know who will! Security contacts can be found at home.ihs.gov/security. Also, feel free to email questions to Cybersecurity@ihs.gov.

Click the Continue Button below.