HFS DATA SECURITY TRAINING

WITH TECHNOLOGY COMES RESPONSIBILITY

Illinois Department of Healthcare and Family Services

Training Outline:

- Training Goals
- What is the HIPAA Security Rule?
- What is the HFS Identity Protection Policy?

Training Goals:

- ✓ To educate users
- ✓ To establish appropriate procedures for users to securely utilize all forms of data and technology resources available
- ✓ To inform users about the HFS Identity Protection policy regarding use of Social Security Numbers
- ✓ To inform users of important HFS security policies

HIPAA Requirements

- **Health Insurance Portability and Accountability Act (HIPAA) -** The HIPAA regulations require health care providers, health plans (such as Medicaid), clearinghouses and their business associates and contractors to develop and follow procedures that ensure the privacy and security of protected health information (PHI) when the PHI is transferred, received, handled or shared
- HIPAA has privacy and security requirements
- HIPAA requirements apply to all forms of PHI, including paper, oral and electronic, etc.
  - Furthermore, only the minimum necessary health information needed to conduct business is to be used or shared

HIPAA Privacy and Security Rule

- **HIPAA Privacy and Security Rules** work together and govern how we handle Medicaid client information
  - The HIPAA Privacy Rule covers how we can use and disclose PHI
  - The HIPAA Security Rule provides standards for safeguarding and protecting health information, specifically, electronic protected health information (E-PHI)

What is the HIPAA Security Rule?

- Federal Legislation designed to protect the confidentiality, integrity and availability of electronic protected health information (E-PHI)
- Comprised of three main categories of “standards” pertaining to the administrative, physical and technical aspects of E-PHI
- Applies to the security and integrity of electronically created, stored, transmitted, received or manipulated personal health information

E-PHI

- **E-PHI = Electronic Protected Health Information**. Examples are:
  - Medicaid Recipient ID number, Medical record number, account number or Social Security Number
  - Patient demographic data, e.g., address, date of birth, date of death, email/web address
  - Dates of service, e.g., date of admission, discharge
  - Medical claims, records, reports, test results, medications

E-PHI with Privacy and Security

Remember, HIPAA Privacy and Security rules apply to all protected health information, whether in paper or electronic format.

- **Secure all paper media containing confidential information**
- **Secure all electronic media containing confidential information**

HIPAA SECURITY STANDARDS

HIPAA Security standards serve two purposes:

1. Implementing the appropriate security safeguards for electronic protected healthcare information(E-PHI) that may be at risk
2. Protecting an individual’s health information while permitting appropriate access and use promotes the use of E-PHI in the healthcare field.

HIPAA Security Rule Requirements

The Security Rule requires HFS, business associates and HFS contractors to maintain reasonable and appropriate administrative, technical and physical safeguards:

1. Ensure the confidentiality, integrity and availability of all E-PHI that we create, receive, maintain or transmit
2. Identify and protect against reasonable anticipated threats to the security or integrity of E-PHI
3. Ensure compliance by the HFS workforce

Potential Consequences of Security Violations

- Risk to integrity of confidential information, e.g. data corruption, destruction
- Risk to security of personal information
- Loss of client trust, employee trust, public trust
- Loss of confidentiality, integrity and availability of data
- Agency embarrassment, bad publicity, media coverage
- Reporting to oversight authorities
- Internal disciplinary action(s), termination of employment
- Penalties, prosecution and potential for sanctions/lawsuits

Violations

Federal Laws

Violations of the HIPAA Privacy and Security Laws can result in serious sanctions:

- Civil penalties (fines) can be imposed on HFS
- Criminal sanctions (imprisonment) and fines can be imposed on individual employees

HFS Identity Protection Policy

- In 2010, HFS adopted an Identity Protection Policy as a result of the Illinois Identity Protection Act.
- The Policy requires HFS to implement an Identity Protection Policy in order to ensure the confidentiality and integrity of Social Security Numbers and reduce identity theft.

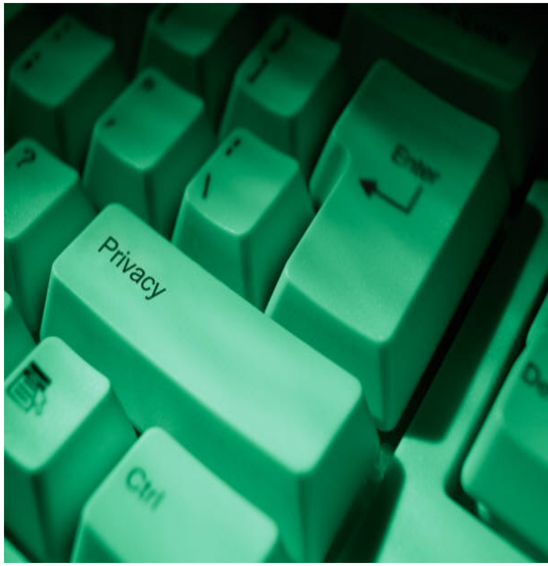
HFS Identity Protection Policy and SSNs

Did you know…?

- SSN numbers shall not be encoded, embedded in or on a card or document using a bar code, chip, magnetic strip or other technology.
- Whenever an individual is asked to provide a SSN, HFS shall provide that individual with a statement of the purpose or purposes for which HFS is collecting and using the SSN. (See the Identity Protection Policy on the HFS InfoNet)

SSN Do's and Don'ts

- Don't publicly post or display an SSN in any manner
- Don't print an individual's SSN on any card required for the individual to access products or services provided to HFS
- Don't require an individual to transmit an SSN over the internet, unless the connection is secure or the SSN is encrypted. If you are not sure, please contact your LAN Coordinator.
- Don't print an individual's SSN on any materials to an individual through US mail, private mail, electronic mail unless State or federal law requires the SSN.



SSN Don’ts

- Don’t collect, use or disclose a SSN from an individual unless required to do so under state or federal, law, rules, or regulations or the collection use or disclosure of the SSN is necessary for the performance of the responsibilities of HFS.

- Don’t require an individual to use their SSN to access or communicate with an HFS internet website.
- Don’t use the SSN for any purpose other than the purpose for which it was collected.

SSN - Do’s

- ✓ Do limit employee access to SSNs only to those employees that need to have such access.
- ✓ Do check with the HFS Security Officer or the HFS Privacy Officer if you have questions regarding the use of a SSN.

SSN - Do’s

- Do use common sense when it comes to the use of an individual’s SSN.
- Do redact SSNs from the information or documents containing all or any portion of an individual’s SSN before public inspection or copying of the information or documents.

The Three Main Principles of Data Security Are:

- **CONFIDENTIALITY** - The assurance that information is not disclosed to unauthorized individuals, programs or processes
- **INTEGRITY** - Information is accurate, complete and protected from unauthorized modification
- **AVAILABILITY** - Ensures reliability and timely access to data and resources for authorized individuals

LAPTOP USERS BE AWARE!

- Maintain the physical security of the laptop
- Do not store passwords, scripts or macros on the laptop
- Back-up the laptop regularly.
- Maintain up-to-date virus protection
- If you print something with protected health information, you must secure it

Keep Confidential Client Information -

What is Considered Confidential Information?

- **PII - Personally Identifiable Information -** is information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual
- **PHI - Protected Health Information -** is any information about health status, provision of health care or payment for health care that can be linked to a specific individual
- **IIHI - Individually Identifiable Health Information -** is information that is a subset of health information, including demographic information collected from an individual

What is Considered Confidential Information?

- Confidential information is handled in many areas
- It's not just health information that must be kept secure. You may use other confidential information in your work. For example:
  - Processing child support payments via credit card or checks
  - Making inquiries into child support cases that contain federal income tax information
  - Handling documents that contain Social Security Numbers

What is Considered Confidential Information?

- Child Support information, financial, credit card related information is confidential information
- Payment Card Industry (PCI) – has specific security standards that were developed to protect card information during and after a financial transaction. HFS employees, contractors and temporary staff need to comply with those requirements.
  - PCI compliance is required by all credit card brands

What is Considered Confidential Information?

If The Information Contains Social Security Numbers or Tax Information

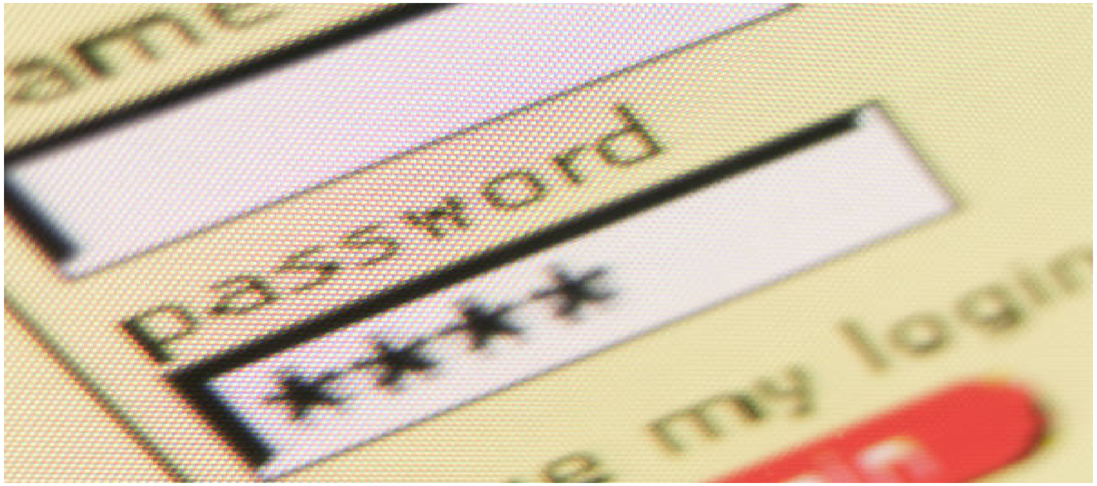
- **SSN - Social Security Number -** is a nine-digit number issued to U.S. citizens, permanent residents and temporary (working) residents under section 205(c)(2) of the Social Security Act
- **FTI – Federal Tax Information -** any tax return-derived information received from the IRS

Do Not Disclose Confidential Information Via:

- Phone
- Through unencrypted Email or as an attachment
- Trash – instead, shred or place in a confidential bin
- By leaving it out for anyone to see or access

Be Sure To Physically Secure Any Printed Documents That Contain Confidential Data

- Do not store documents containing confidential information in an unsecured location
- Do not leave documents with confidential information open for viewing
- Shred documents with confidential information or place documents in a locked recycle container when no longer needed



A Password is the First Line of Security Defense!

Keep it SECRET! **Keep it SECURE!** **Change it OFTEN!**

PASSWORD SECURITY

- Choose a secure password
- Don’t write it down anywhere near your computer, place it in a secure location
- Log-off or lock your work station when leaving your desk

User Responsibilities:

Password Security

- Change passwords often
- Don’t use the same password for multiple accounts
- Don’t email or share your password with others
- Do not store or embed your password in shortcuts or scripts

User Responsibilities

WHEN SENDING EMAIL:

- **Review Attachments**
- **Double Check Addresses**
- **Use Encryption with Confidential Data**
- **Do Not Use Personal Accounts**
- **Do Not Share Your Password**
- **Remember That All Emails Are Saved**

Encryption Requirements

- If you have confidential information (PII, PHI, IIHI, PCI, SSN, FTI) that you are emailing, saving to a portable electronic device (CD, DVD, removable storage device) or sending through a file transfer, it **MUST BE** encrypted
- Encrypting the confidential information will encode the information in such a way that only authorized parties can read it

SECURITY BREACH

A data breach is a security incident in which sensitive, protected or confidential information is copied, transmitted, viewed, stolen or used by an individual who is unauthorized to do so.

SECURITY INCIDENTS

A security breach can occur through either:

- a mistake or
- a malicious act!

Hackers and intelligence professionals have a variety of tricks up their sleeve.

Hacker Tricks

- Phishing is a hacker technique of fraudulently obtaining private information
- Typically, the phisher sends an email that appears to come from a legitimate business—a bank or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The email usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN

Reporting: Security Incidents

If you suspect confidential information has been inappropriately disclosed or stolen, **you must report** the incident to the HFS Computer Security Manager **immediately.**

HFS Security Manager
Carl Conner
Carl.Conner@Illinois.gov
217-782-2669

Reporting: Security Incidents

Examples of a data security breach that must be reported:

- A laptop or phone with confidential data on it is lost or stolen
- A USB drive with confidential data is lost or stolen
- You see someone who is not authorized accessing a file that contains confidential data
- Printed documents with confidential data are thrown in an unlocked garbage container, left in a car or left on a desk unattended

REMEMBER

- NEVER give out your password
- Do not click on links in emails that come from people you do not know
- Use encryption when sending confidential information
- If you suspect confidential data has been inappropriately exposed report the incident to the HFS Security Manager **immediately**