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?
- HFS Data Security Policy
  - Individual Responsibilities and Sanctions
  - Reporting
  - Security Consciousness
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
HFS Policies:

The following policies and procedures should be reviewed annually by all staff

HFS HIPAA Privacy Policy:
http://hfs.infonet/infonet/hipaamanual/

HFS Identity Protection Policy:

HFS Computer Security and Internet Policy:

HFS Security Breach Notification Policy:
http://hfs.infonet/infonet/reference/security/security.html
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
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 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


- 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
HFS Data Security Policy

• ALL computerized information is the property of the State of Illinois
• Information must be protected from unauthorized access, theft, unauthorized and/or fraudulent disclosure, modification or destruction
• All communications over, and activity conducted on, state computers are the property of the state. Staff and users of state property should have no expectations of personal privacy when using state-owned systems.
Who Does the Computer Security and Internet Policy Apply To?

IT APPLIES TO EVERY INDIVIDUAL

• All HFS employees
• All HFS contractual parties
• Temporaries and Summer Help

WE ARE ALL ACCOUNTABLE!
Individual Responsibilities:

*Consider Security Policy Compliance In All Aspects of Your Job*

- Data Development
- Data Storage
- Data Destruction
- Data Sharing
HFS will provide the resources needed to do your job
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. OIS does not provide central back-up
- Maintain up-to-date virus protection by connecting to the network regularly
- If you print something with protected health information, you must secure it
Individual Responsibilities:

Screen Savers & Wallpaper Can Cause Corruption!

Use only those offered within the agency operating software
Remember, All Information:

- Created
- Sent
- Received
- Stored
- Accessed through the Internet
- On any HFS computer system at anytime

Continued
May Be:

* Monitored
* Intercepted
* Accessed
* Disclosed
* Inspected

WITH OR WITHOUT NOTICE TO THE USER!
Individual Responsibilities:
If it is not work related,

Solitaire

Box Scores

E-Bay

Facebook

Don’t Do It
Violating the Computer Security and Internet Policy is Punishable By:

• POTENTIAL DISCIPLINARY ACTION
• POTENTIAL FOR DISCHARGE AND PROSECUTION
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?

• HFS employees handle confidential information 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) – Payment Card Industry (PCI) – has specific security standards that were developed to protect card information during and after a financial transaction. HFS employees 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 Numbers** - 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
User Responsibilities: Obtaining A User Id

Access to HFS computer systems is given by obtaining a User ID and password from the local RACF/LAN Coordinator. Completion of the HFS 1706 is required for system access.

Your **LAN Coordinator** is your first line of support for all computer Issues!
A Password is the First Line of Security Defense!

Keep it SECRET! Keep it SECURE! Change it OFTEN!
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
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
PASSWORD SECURITY

- Passwords used on documents are the responsibility of the user
- If a document must be password protected, OIS recommends using Entrust
- Entrust passwords can be recovered if they are forgotten. Microsoft passwords cannot be recovered by CMS, OIS or your LAN Coordinator
- Contact your LAN Coordinator for assistance in using Entrust
User Responsibilities:

LAN - PASSWORD RULES

1. Prompted to change every 60 days
2. Must be 8 characters or more
3. Must not have been used in the previous 12 passwords
4. Passwords must contain (3) of the following (4) Character Groups:
   • English Uppercase characters (A through Z)
   • English lowercase characters (a through z)
   • Numerals (0 through 9)
   • Non-alphabetic characters (such as !,$,#,%)
5. Passwords are revoked after 3 unsuccessful attempts
1. Passwords must change every 60 days
2. Must be 8 characters in length
3. Passwords cannot be reused for 10 password change cycles
4. Passwords must contain at least one of each of the following:
   - Alpha character (a-z, or A-Z)
   - Numeric characters (0-9)
   - Special characters (#, $, @)

Continued…
5. Cannot Contain the first three letters of the name of a month (e.g. jan, feb, mar, etc.)
6. Cannot contain first or last name
7. Cannot contain part of social security number
8. Passwords are revoked after 3 unsuccessful attempts
Email Messages Are For Work Related Purposes Only:

- Not Secure
- Not Private
- Not Confidential
- May Be Monitored With or Without Notice to the User
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
WHEN RECEIVING EMAIL:

• Accept Email and attachments only from trusted sources to avoid viruses
• Don’t participate in chain letters or “spam”
• If you receive spam or suspicious email, forward it to: spamreport@securecomputing.com
Reminder

✓ There is NO expectation of Privacy

✓ Agency management has the right to access and review all messages

✓ Abuse of the Email system may be cause for discipline - up to and including discharge
Individual Responsibilities:

APPROPRIATE USE OF THE INTERNET

- Web Browsing only for work related educational and research purposes
- Accessing news groups about work related topics
Individual Responsibilities: INAPPROPRIATE USE OF THE INTERNET

- Accessing or releasing confidential information
- Accessing for personal use or gain
- Performing illegal activity
- Political activity or lobbying
- Sexual material or harassment
- Libelous or slanderous remarks
- Vulgar, obscene or offensive language
- Deliberate attempts to degrade system performance
- Any activity that may compromise the State of Illinois
YOUR internet usage is monitored and inappropriate links are automatically blocked.

If a site is blocked in error, notify the HFS Computer Security Manager and provide justification why the site should be unblocked.
DOWNLOADING & UPLOADING FILES

- **DOWNLOAD**: Users may download research related text and data files if needed for State of Illinois business.
  - Downloaded files can be scanned prior to opening by right clicking the file and then selecting “Scan for Threats”.
- **UPLOAD**: Permission to upload to the HFS website must come from the agency webmaster.
Be respectful of copyright laws in the use of material found on, placed on or disseminated through the Internet. If there is any question, contact the owner of the copyright and request written permission for proposed use.
INTERNET SECURITY GUIDELINES

• Don’t put anything on the “net” that you wouldn’t leave on the supermarket bulletin board
• Anyone can intercept and read your messages and documents
• No add-ons or homemade connections
• Don’t debate Dept. policy, perpetuate rumors, reveal inappropriate information or handle public relations
• HFS has specific policy on internet usage
MISUSE OF THE INTERNET MAY RESULT IN:

- Losing Access to the Internet
- Disciplinary Action
- Possible Discharge
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.
Encryption

If you need confidential information to be encrypted, or have questions, please contact your LAN Coordinator for assistance.
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.
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
If you suspect confidential information has been inappropriately disclosed or stolen, **you must report** the incident to your supervisor, the Office of Inspector General and LAN Coordinator/HFS Computer Security Manager **immediately**.
Reporting: Security Incidents

Examples of a data security breach that must be reported:

• A laptop or state issued 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
All computer violations including, but not limited to, pornography, secondary employment, violence and threats of violence shall be immediately reported to The Office of Inspector General. The OIG will review the matter and when appropriate, refer the issue to the Business Manager or the HFS Computer Security Manager for handling.
Security Consciousness

- Store files electronically, rather than in hard copy
- Avoid printing Email when possible
- Be Green - Turn off the computer, monitor and radio when leaving your office
- Be Green - Set the computer to go into sleep mode when it is not being used
REMEMBER!

Maintain Physical security:

- Wear your ID badge and all visitors need badges
- Secure paper media containing confidential information
- Do not write your password down
- Lock your PC when you leave your desk
- Shut down your PC at the end of the day
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

• Do not use USB storage devices (thumb drives) unless they are provided by HFS or approved by the Computer Security Manager. USB drives can contain viruses or malicious software that can spread to your computer

• If you suspect confidential data has been inappropriately exposed report the incident to your supervisor immediately
Form Completion: Follow these instructions to confirm your completion of the Internet and Data Security Training requirement. This training is required annually.

Click on the link below to access the confirmation/certificate of understanding form.

- Fill out the form
- Print and sign the form
- Submit it to your supervisor who will sign and forward the form to HFS Bureau of Training

HFS 3853 (PDF)