INFORMATION PROTECTION PROGRAM

West Florida HEALTHCARE

HIPAA/HITECH Privacy and Security Training for New Employees

Facility Privacy Official (FPO)

- Each facility has a designated FPO
- Every workforce member should be familiar with the facility's FPO
- Our WFH FPO is Debbie Wroten, VP of Quality
- This is the "go-to" person for:
  - Potential patient privacy issues
  - Questions on patient privacy matters
  - Patient privacy complaints

HIPAA Definition and Purpose

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- Federal Law

What is the purpose of the law?

- Federal regulations establishing security standards for protecting certain health information that is in electronic form.
- Ensures the confidentially, integrity, & availability of all electronic protected health information (EPHI) that is created, received, maintained or transmitted.
- Protects against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protects against any reasonably anticipated uses/disclosure of such information that are not permitted or required under this rule.
- Ensures compliance with this rule by its workforce.

HITECH Definition and Purpose

What is HITECH?

- Health Information Technology for Economic and Clinical Health Act
- Federal Law

What is the purpose of the law?

- Made massive changes to existing privacy and security laws
- Creates a nationwide electronic health record
- Increased penalties for privacy and security violations

Examples of changes due to HITECH

- Criminal provisions
- Office of Civil Rights audits
- Breach notification requirements
- Changes to the patients' right to access

HITECH/HIPAA Omnibus Final Rule

- The Department of Health and Human Services (HSS) made revisions to the HITECH Act of 2009. The revisions took effect March 26, 2013, but medical organizations and business associates had until September 23, 2013 to comply.

Some of the key changes to the final ruling are:

- The definition of a business associate has been expanded and Business Associates are now directly liable under the Security Rule and some provisions of the Privacy Rule.
- There are stricter limitations on the use of protected health information (PHI) for fundraising and marketing activities under the Security and Privacy Rule.

HITECH/HIPAA Omnibus Final Rule

- A data breach is now defined to have occurred if there has been any unauthorized acquisition, access, use, or disclosure of protected health information (PHI) unless it can be proved that the likelihood that the PHI has been compromised is low.
- Penalties for violations have increased and a medical entities reasonable lack of knowledge of a violation is no longer accepted as an affirmative defense.
- Many of our HIPAA/Privacy policies were revised based on the changes made to the HITECH/HIPAA Omnibus Final Rule 2013. To ensure compliance, Specialty Hospital made the necessary changes to the policies, implemented the changes and educated our workforce by September 23, 2013.

Civil Money Penalties for Non-Compliance*

Violation Category	Each Violation	All such violations of an identical provision in a calendar year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

*As of 1/25/13

Criminal Penalties for Non-Compliance

- Applies to health plans, providers, clearinghouses and business associates that knowingly and improperly disclose information or obtain information under false pretenses.
- Apply to any “person”
  - Up to $50,000 and one year in prison for obtaining or disclosing protected health information (PHI)
  - Up to $100,000 and up to five years in prison for obtaining PHI under “false pretenses”
  - Up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm

Protected Health Information (PHI)

- Name
- Address including street, county, zip code and equivalent geocodes
- Names of relatives
- Name of employers
- All elements of dates except year (*e.g.,* DOB, admission /discharge, expiration, etc.)
- Telephone numbers
- Fax numbers
- Email addresses
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web universal resource locator (URL)
- Internet protocol address (IP)
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic or code

Covered Entity

- An entity subject to HIPAA and HITECH
- Health plans, health care clearinghouses, and health care providers that transmit electronically for billing
  - Hospitals
  - Physician Practices
  - Insurance Companies
  - Home Health Agencies
  - Hospice

Business Associate (BA)

- A person, company, corporation, or any other legal entity that creates, receives, maintains or transmits PHI to perform a function or activity on behalf of the facility or to perform certain professional services for the facility
  - Billing
  - Legal
  - Quality Assurance
  - Claims Processing
- Services covered by a Business Associate Agreement (BAA)

Affiliated Covered Entity (ACE)

- Legally separate affiliated CEs designated as a single CE for HIPAA purposes
- Typically facilities within the same Meditech market or division

Organized Health Care Arrangement (OHCA)

- Clinically integrated care setting in which individuals typically receive health care from more than one health care provider
- Most commonly found in the hospital setting

Designated Record Set (DRS)

Group of records maintained by or for facility

- Medical and billing records
- Information, in whole or in part, used by facility to make health care decisions about the individual

Minimum Necessary – "Need to Know"

- Access only those systems or information you are officially authorized to access to do your job.
- Only share sensitive and confidential information with others who have a "need to know".
- Safeguard all information as if it were about you and your family.
- Never use your system access to view the information of a fellow employee, friend, family member, neighbor, or YOUR OWN!

  Policy prohibits employees from accessing their own medical records.
- Inappropriate access may result in disciplinary actions, such as: verbal, written, and/or suspension/termination.

  WS.SWB.03 – Sanctions Process Standard

Notice of Privacy Practices (NOPP)

- Patients' privacy rights are outlined in the NOPP
  - Breach Notification
  - Right to Access
  - Right to Amend
  - Confidential Communication
  - Right to Restrict
  - Right to Opt Out of the Directory
  - Right to Request an Accounting of Disclosure
  - Fundraising and the Right to Opt Out
- Patient receives NOPP at each registration

Right to Access

- Patient (or legal representative) may inspect and/or obtain a copy of PHI contained in the DRS
- Some limited exceptions
  - Psychotherapy notes, and information compiled for use in civil/criminal/administrative actions
- Direct patients to your facility's designated department (*e.g.*, HIM)
- Individuals have the right to obtain information in an electronic format
- Individuals (except medical staff physicians) may not access their own record in any system

Right to Amend

- Patients have the right to request an amendment to records in the DRS
- Request must be made in writing to the HIMD.
- Cannot change or omit documentation already in the medical record

Confidential Communications

- Patients have the right to request to be contacted at alternate locations or by alternate means
- All reasonable requests must be accommodated
- A form must be completed by the patient or patient's legal representative

Right to Restrict

- Patients have the right to request restrictions of uses and disclosures of PHI
- The request must be made in writing to the FPO or the FPO's designee
- Do not agree to any request – refer the individual to the FPO

Opt Out of the Directory

Patients have the right to opt out of the facility directory

Cannot acknowledge the patient is in the hospital or the condition of the patient except for treatment, payment or health care operations purposes

- Clergy will not have access
- No floral or other deliveries

In the hospital setting, the confidential flag is set in Meditech

Accounting of Disclosures (AOD)

- Patients have the right to request a written accounting of disclosures of PHI to authorized individuals a facility has made during the six years prior to the date the report is requested
- Every facility must have a process in place to log AOD entries (*e.g.*, MEDITECH MRI Correspondence Module, spreadsheet)

Patient Privacy Complaints

- Route all patient privacy complaints to the FPO
- FPO must acknowledge the complaint
- Complaint log maintained by the FPO in accordance with the facility's policy
- No retaliatory actions can be made
- Disposition of the complaint must be consistent with the facility's sanctions policy

HIPAA Compliant Authorizations

- Form signed by the patient or patient's personal representative authorizing the release of PHI to a third party or individual
  - Not required for treatment, payment, or health care operations disclosures (unless otherwise required by State law)
- Certain required elements in order to be "HIPAA Compliant"
  - Always use the facility's form, when possible

Sanctions

- Every facility must have a sanctions policy to address privacy and information security violations
- Workforce members may be sanctioned (e.g., written warning, termination) for privacy and security violations
- Contact your FPO for a copy of your facility's policy

Uses and Disclosures Required by Law

- PHI may be disclosed about an individual the facility believes to be a victim of abuse, neglect, or domestic violence to a government authority authorized by law to receive it
- PHI may be disclosed in the course of any judicial or administrative proceeding
- PHI may be disclosed to law enforcement in certain scenarios:
  - If required by law, including reporting certain types of wounds or injuries
  - In response to law enforcement official's request for PHI for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person; or if the individual is, or is suspected to be, a victim of a crime
  - To alert law enforcement of death resulting from criminal conduct
  - If the facility believes in good faith that a crime has occurred on the premises

Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is not Required

- Disclosures for Public Health Activities
- Certain Disclosures of Immunizations
- Health Oversight Activities
- Certain Disclosures about Decedents
- Disclosures to Avert a Serious Threat to Health or Safety
- Disclosures for Specialized Government Functions
- Disclosures for Workers' Compensation

Uses and Disclosures to Other Covered Entities

PHI may be disclosed to other covered entities without the patient's HIPAA compliant authorization

- For treatment activities of a health care provider
- For the payment activities of the entity that receives the PHI
- For limited health care operations activities, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship
  - For limited health care operations
  - For the purpose of health care fraud and abuse detection or compliance
- To other members of the OHCA for health care operations

Uses & Disclosures of PHI for Involvement in the Patient's Care and Notification Purposes

- To notify a family member, personal representative, or another person responsible for the care of the patient of the patient's location, general condition, or death
- To an entity authorized to assist in disaster relief efforts, for the purposes of coordinating the permitted uses and disclosures
  - Patient agreed
  - Patient was provided opportunity to object and did not
  - Inferred based on professional judgment that patient did not object
- Relevant PHI may be disclosed to any person to whom the patient has given his or her passcode

Verification of External Requestors

- Must verify the identity of any person or entity that is unknown to the workforce member and is requesting PHI
- Exceptions
  - Facility directory
  - Disaster relief purposes
  - Disclosures for the involvement in the individual's care and notification purposes

Incidental Use and Disclosures

- Disclosure that cannot be reasonably prevented, limited in nature, and occurs as a by-product of a permitted use or disclosure of PHI
- Must have appropriate safeguards in place
- Examples:
  - Discussions overheard at the nurses' station
  - Physician speaking with a patient in a semi-private room
  - Telephone conversation overheard at the registration desk

Safeguarding Oral PHI

- Do not discuss PHI in public areas or with anyone without a need to know – even if you don't use the patient's name
  - Some exceptions (e.g., in an emergency situation for treatment purposes, incidental disclosures)
- Use lowered voices or step away from others
- Verify recipients of PHI prior to disclosure
- Ask permission to speak in front of visitors
- Only leave messages containing PHI on answering machines in accordance with facility policy

Safeguarding Paper PHI

- Properly dispose of PHI (*e.g.,* shredding bin)
- Do not leave PHI in public view
  - Example: Charts left unattended on the counter of the nursing station
- Secure PHI after hours
- Verify recipients of PHI prior to disclosure
  - Example: Hand discharge paperwork belonging to another patient to the wrong patient
- Never remove PHI from the facility unless relevant to your job function and approved in advance by your manager

Safeguarding Faxed PHI

- Use fax cover sheets
- Use pre-programmed fax numbers when applicable
  - Have a standard process for periodically reviewing programmed numbers for changes
  - Test programmed numbers prior to initial use
- Double-check fax numbers prior to hitting “send”
- Verify intended recipient got the fax

Information/Electronic Security

Employee Privacy

Users should have no expectations of privacy when using company information systems.

- Everything you do when using the HCA network creates network logs. Network logs are like footprints in the sand, leaving traces of the places you have been on the network.

For example, network logs are created for things like:

Internet and email use
Accessing systems and applications
Making changes to data

- Data saved to company computers/devices also should not be considered private.

USER ID and Password

- Your name and Social Security number provide identification on a paper document like your User ID and Password identifies and authenticates you as a valid user of an electronic system or application.
- Most systems provide documentation of work performed and information reviewed by tracking movement in the system and detailing tasks. In order to insure proper documentation, never write down or give your User ID or Password to anyone else, and never use anyone else's User ID and Password.

Creating Quality Passwords

- Eight(8) characters or more.
- Contain 3 of the following 4 variables: Uppercase characters, Lowercase characters, Special characters (such as $, # *), and/or Numbers.
- Easy for you to remember and hard for others to guess.
- Use a “pass phrase” where the first character of each word is used. Example: “All good cows like to eat green grass” gives you the pass phrase of “Agcl2egG”. (Do not use this example as your password!).
- Never use your work passwords for personal accounts or your personal passwords for your work accounts.

❖Note: Some HCA systems may have different password requirements.

Bad Passwords

Your user ID or Account Number

Your Social Security Number

Your name

Birth, death, or anniversary dates

Family member names (including pets)

Your favorite song, artist, author, sports team, etc.

A word or name found in any dictionary

Passwords like: password, 123456, asdfjkl;, letmein, trustno1, qwerty

- If your password is similar to any of the above, change your password immediately!

Social Engineering (Phishing) and Verbal Communication

- Social engineering refers to the tricks (i.e., emails, websites, phone calls, etc.) attackers use to fool victims into performing an action which reveal private personal or business information. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.
- Occasionally the attacker, or social engineer, will pretend to be an employee from IT, PC help, or system maintenance from another company. This is also known as ***Phishing***.
- In email attacks, social engineers will often lure victims by using aggressive language, current events, or warnings of a pending monetary fine.

Social Engineering (Phishing) and Verbal Communication

You can help combat Social Engineering by:

- Being aware of your surroundings and who listens to your conversations.
- Identifying as fully as possible anyone asking you for information.
- Never providing information about the computer system or applications, telephone connections, or network to anyone over the telephone unless you initiated the call and specifically know to whom you are speaking.
- Never clicking on a link or opening an email attachment from an unknown source.

Workstation Security

You must make a commitment to:

- Keep hard copy information, portable storage, or hand-held devices in a secured (locked) place.
- Shield information that is on any screen or paper from casual public view or from others without a 'need to know.'
- Ensure screensavers and screen timeouts are always enabled.

  If applicable, always activate the screensaver or "lock" your PC when you leave the workstation (especially those public area workstations).
- Physically secure (locked) PCs to a heavy object (desk) whenever possible.
- Use surge protectors on all equipment containing electronic information.

Workstation Security

- Only use company approved, licensed, and properly installed software.
  - *New software that needs to be installed, from the Internet or disc, on any workstation should be done by the appropriate member of the IT staff.*
- Always save critical business data and/or ePHI on an approved network drive. This ensures that the information will be saved and backed up. Do not save this type of information to the local workstation hard drive.
- Exit applications and systems as soon as you complete your work.
- "Log off" your PC before leaving work each day.

Mobile Computing

- Definition: "…working on or with a device that can connect to the company network anywhere/anytime through such means as teleworking or telecommuting." Off-business premises or locations include, but are not limited to, home, airports, hotels, conference centers, etc.
- Mobile devices and any work information should be kept in your control and in sight at all times.

  Tips when traveling with mobile devices:

  Store any mobile device(s) in the locked trunk of the vehicle you are traveling in.

  If staying overnight at a hotel, keep the mobile device(s) with you, inside the hotel room.

  At the airport, put the laptop bag on ground between your legs with your foot through the strap. Also, if able, bring the mobile device(s) on the plane with you.
- Never connect a company owned device to any unsecured internet network/connection.
- Always "log off" or "lock" the mobile device(s) when you are finished using it.

Electronic Communications: Your Responsibility

- Use e-mail and the Internet in a productive manner. Personal use of these resources should be highly limited. Refer to *Appropriate Use of Company Communication Resources and Systems Policy, EC.026.*
- Use secure methods specifically approved in advance by Information Technology and Services (IT&S) Security to transmit information to appropriate individuals outside the company.
- When communicating in a personal capacity, it is important not to create the impression that you are communicating on behalf of HCA. The only exception is if you have been specifically authorized by the company to do so.

Social Media

- Policies EC.026, IS.SEC.002 and the HCA Social Media Guidelines should be adhered to by any employee seeking to engage in social media activity.
- Unrestricted areas of the Internet (e.g. social media, discussion groups, bulletin boards, chat services, unsecured web site, etc.) should never be used to transmit or display Company-privileged or sensitive/confidential information of any kind.

  Comments about patients or events that happened during work should not be made during personal use of social media sites, discussion boards, etc.
- Employees must identify themselves as employees of the appropriate HCA affiliate when posting comments or responses on the employer's blog or a social networking site.
- Only authorized use of social media while at work is permitted.

Email Security

- Emailing sensitive/confidential information within the HCA network is considered a secure communication.
- Emailing sensitive/confidential information to any external (non-HCA) recipient is considered an *unsecure* communication. **Never** transmit unsecured patient identifiable or other sensitive and confidential information.
- If you are emailing sensitive data to someone outside of HCA, or you are uncertain whether the recipient's email address is within HCA, you are required to secure, or **encrypt**, the email or file(s).

  *An email can be encrypted simply by entering **[encrypt]** including the brackets, i.e., <encrypt>, (encrypt), {encrypt}, or [encrypt] at the start of the email subject line. *DO NOT LIST SENSITIVE INFORMATION IN THE SUBJECT LINE**

  DO NOT send any type of Sensitive Data to text pagers. Text pagers are not encrypted and the data they send is publically monitored.

  If you have any questions or would like additional email encryption information, contact your facility IT Director or your Zone FISO. You may also search Atlas keyword: encrypt

Unacceptable Uses of HCA Resources

Never:

- Harass, intimidate, or threaten others.
- Access or distribute obscene, sexually explicit, abusive, libelous, or offensive material.
- Impersonate another user, or mislead others about your identity.
- Access another person's e-mail (unless specifically authorized to do so).
- Distribute copyrighted material not authorized for reproduction or distribution.
- Use electronic communication for any purpose which is illegal, against company policy, or contrary to the company's best interest.
- Bypass system security mechanisms.
- Automatically forward messages using mailbox rules to Internet e-mail addresses outside the company.

Practice good Information Security by following these guidelines:

- Use only your own unique User ID and Password to access any system or application.
- Create a "hard to guess" password and never share it.
- Always exit or “log off” the workstation when stepping away and at the end of the work day.
- Follow all policies, procedures, and standards when using HCA technology resources.
- Take advantage of the **Password Reset Tool**! Search Atlas keyword: “password reset”

  This tool helps you unlock or reset your Windows network account, Meditech account password, or HOST system password without calling the Help Desk.
- Only access information if there is a “need to know.”