HIPAA
Health Insurance Portability and Accountability Act

2016 JHS Annual Mandatory Education
HIPAA Roadmap

• Where will this presentation take you?
• HIPAA History
• HIPAA Goals
  – We will continuously focus on how HIPAA is meant to increase the Quality of Care provided at JHS!
• Components of HIPAA
  – Areas of Emphasis
    • How do YOU respond?
    • How components interrelate
• Myth vs. Reality
• Summary
What’s in the name?

- Health Insurance Portability and Accountability Act
  - Portability
    Intended to facilitate a decision to change your health insurance or insurance company, but also allows you to change employers by limiting exclusions such as pre-existing conditions.
  - Accountability
    Your records are kept private and secure, or there are consequences/penalties.
History

- Passed on August 21, 1996

- Enforcement began on April 14, 2003

- The HIPAA Rules are ever-changing
  - American Recovery & Reinvestment Act of 2009
  - (“Stimulus Bill”) had recent revisions
History

• Who must comply?
  The HIPAA Rule applies to:
  – COVERED ENTITIES
  – Health plans
  – Health care clearinghouses
  – Health care providers
  – Business Associates
  – …and YOU!

• Everyone in the Organization has a role with HIPAA because the purpose of our Organization is to provide quality care and quality care is dependent on trust that can be affected by patient privacy.
History

• Enforcement
  – Who Enforces HIPAA compliance?
    • Department of Health and Human Services (DHHS): Office of Civil Rights (OCR) enforces the PRIVACY RULE and SECURITY RULE

  – Increased Penalties/Enforcement
    • Penalties now range up to $50,000 per violation with maximum penalties for additional violations ranging up to $1,500,000!
      – This represents a 600% increase!
    • State Attorney General authority
    • Business Associates now subject to civil and criminal penalties in the same manner as Covered Entities
HIPAA Components

- **Title I**
  - Portability

- **Title II**
  - The Transactions Code & Sets
  - The Unique Identifiers Rule
  - The Enforcement Rule
  - The Privacy Rule*
  - The Security Rule*

* Area of Emphasis
Protected Health Information (PHI) consists of 18 identifiers:
Essentially, any information that could reveal the identity of a patient.

- Names
- All geographic identifiers
- All elements of dates
- Telephone numbers
- Fax numbers
- Electronic mail (e-mail) addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers, including tag numbers
- Device identifiers and serial numbers
- URL numbers
- IP address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images
- ANY OTHER unique identifying number, characteristic or code
Protected Health Information (PHI) consists of 18 identifiers: Essentially, any information that could reveal the identity of a patient.

- The list on the previous slide is not meant to be memorized.
- The list on the previous slide serves as an illustration of just how many different types of patient information are classified as PHI.
- It’s important to note that this information is more than just the identifiers we commonly connect with patient information (names, addresses, social security #'s).
- Ultimately, PHI can be ANYTHING that links back to the patient.
To Whom Does HIPAA Apply?
ALL OF THE ABOVE!
HIPAA Areas of Emphasis

PRIVACY RULE

• Privacy as a Core Value & Right
  – Supreme Court Justice views Privacy as the “right to be let alone.”
• State of Florida Privacy more stringent
  – Baker Act
• Why is the Privacy Rule needed at JHS?
  – We’re a Covered Entity
  – Customer Service!
  – Reduce Financial Exposure
  – Fit the Mission of the Organization.
Privacy Rule

• JHS Privacy and Procedures
  – Notice of Privacy Practices: this brochure (pictured below) explains the rights and responsibilities of patient privacy.
  – Receipt must be acknowledged and is included in the patient’s medical record.

• Training and Education
  – New Employee Orientation (NEO)
  – Annual Mandatory Training & In-Services
  – In-Services supplement the foundational education offered in both NEO and Annual Mandatory by tailoring the training to your specific organizational role.
  – In order to know your requirements, please consult your learning plan.

• To whom do we report violations or concerns?
  – Your Supervisor
  – Whenever possible, questions and concerns are to be kept within your team initially. Promote teamwork!
  – Compliance Hotline: 1-800-684-6457
  – Compliance Department: 305-585-2902
  – Privacy Officer: 305-585-2941
The Role of Authorization
With vs. Without Authorization

• Without Authorization:
  – NO Authorization needed for use and disclosure of PHI for:
    • Individual: we want to empower the patients – this is information they have a right to access and use in their decisions about health care.
    • Treatment: Privacy laws establish the security of PHI with a goal of furthering the quality of care. If an action falls under the treatment exception, authorization is NOT needed.
    • Payment
    • Health Care Operations
    • Required by Law: It’s not uncommon for a JHS employee to receive a court order, subpoena, or some other request pursuant to the law enforcement process. In these instances, there are very specific policies and procedures (500 series) that must be referenced. If there is ANY concern or question regarding the request, please call the Privacy Office immediately at 305-585-2941.
The Role of Authorization

- **With Authorization:**
  - **When Authorization is needed:**
    - Authorization is the way that patients agree to let providers use or disclose information for purposes OTHER than routine health care (or any of the exceptions listed in the previous slide).
    - Must be written in specific terms
    - Reference relevant 500 series Policies and procedures to ensure that proper JHS authorization form is being used.
    - **EXAMPLES:**
      - Releases of patient information to the media
      - disclosures to an employer of the results of a pre-employment physical or lab test
      - disclosures to a pharmaceutical firm for their own marketing purposes.
The Minimum Necessary Rule

- **Objective**
  - Information necessary to satisfy a particular purpose or carry out a function. A health care organization must make reasonable efforts to limit use and disclosure of individually identifiable protected health information (PHI) to the minimum level necessary to comply with any requests and to limit its own requests.

- **Quick Definition**
  - Information necessary to satisfy a particular purpose or carry out a function.

- **Exceptions**
  - Disclosures to or requests by a health care provider for treatment purposes.

- **Highly dependent on Organizational Policy**
  - What’s the “default” level?
    - Part of the professional judgment supported by the Regulation is the ability of health care organizations to “implement policies and procedures based on their own assessment of what PHI is reasonably necessary for a particular purpose.”

- **Issues with the Minimum Necessary Rule for Treatment**
  - Refusal of Information when it’s allowed
    - HIPAA’s rules are sometimes inappropriately used to claim that information cannot be released.
  - Offering too much information when it’s NOT allowed.
    - A huge concern is obviously when JHS or its employees share information that the patient wanted kept private.
Protect Your Stuff!

- **DO NOT** leave your electronic devices unattended
- **DO NOT** leave unlocked desktop computers unattended
- **DO NOT** leave paper medical records unattended
- **DO NOT** distribute PHI without verifying that the information is being handed to the correct patient
Paper Records = Very Sensitive
SECURITY RULE

• Compliance by April 20, 2005
  – Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality.
    • IT Security Manager: Connie Barrera or designee should be contacted for any questions revolving around security issues.
    • 900 Policies: please reference your policies in order to understand the proper procedures to implement in your role at JHS.
  – Response to new technologies
    • Secures Protected Health Information
    • Ongoing, dynamic process
Security Rule Components

- **Administrative**
  - Assignment or delegation of security responsibility to an individual and security training requirements.
  - Comprise over 50% of the HIPAA security requirements
    - This emphasizes the importance of policies and procedures
  - Security Awareness and Training
    - In-Services may be required in order to train you for specific roles in the organization.

- **Physical**
  - Safeguards are designed to protect the confidentiality, integrity, and accessibility of PHI
    - Physical Access: ensure there are only employees and people who have a right to be in a physical location.
    - Ask: “May I help you?”

- **Technical**
  - Importance increasing due to technology advancements in the health care industry.
    - JHS is currently moving to Electronic Medical Records
  - Transmission Security
    - Encryption: method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text. See your 900 policies and procedures to understand how to technically encrypt flash drives, jump drives, etc., AND how to technically SECURE email transmissions (even those which properly include only “minimum necessary” PHI)
Social Media

PHI should NOT be “SHARED”
How to use email when discussing PHI?

- Use work email
- NEVER, NEVER, NEVER use personal email
ENCRYPTION

- If sending email internally, messages are automatically secure
- Use the word ‘SECURE’ in the subject line when sending email containing PHI outside the system
HIPAA Myths

#1 HIPAA laws prevent doctors from exchanging email with their patients.

Not true. That may be a provider’s policy, but HIPAA simply requires that the information is safeguarded.

#2 My clinic will no longer be able to use a sign-in sheet.

Not true. This practice is permitted so long as the clinic uses reasonable efforts to keep disclosures to a minimum.

#3 “We heard that we can’t talk to other doctors about a patient’s care without an authorization.”

Not true! (1) Discuss items relevant and necessary for the patient’s well-being or your payment, and (2) keep your voice moderated to minimize others overhearing these private conversations.
HIPAA Reality

• Jacksonville, FL:
  A woman brought her teenage daughter to work at the hospital and left her unattended at a logged in computer. The girl looked up patient phone numbers, and phone to tell these patients that they’d tested positive for HIV. One patient attempted suicide.
  – What’s the possible effect? SERIOUS CONSEQUENCES!
  – How would your role safeguard this situation?

• Miami, FL:
  Several hundred hospital workers browsed through the records of a famous patient that had recently come to the facility, even though only a few members were actually involved in the case.
  – What’s the possible effect?
  – How would your role safeguard this information?
HIPAA Summary

• Understand WHY the HIPAA rule was created.
• Understand HOW the areas of emphasis relate to your role.
• Understand WHAT you can do to ensure the privacy of our patients.
• Understand the Compliance Team is available primarily for Support.