Jefferson

March 13, 2012

Nursing Informatics Training
HIPAA Privacy & Security, HITECH

Ann Powers CFP, CFE, MPadm

THOMAS JEFFERSON UNIVERSITY AND HOSPITALS

What is Corporate Compliance?

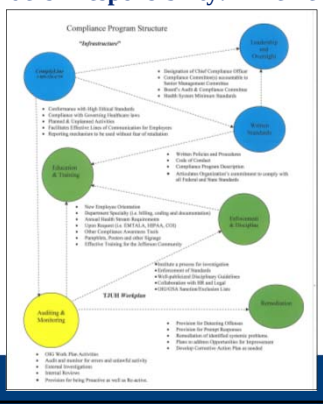
An organized approach to ensure that all employees:

- Know
- Understand, and
- Comply

with all regulatory and internal hospital policy requirements in relation to their jobs. Simply put, the Compliance Program guides us to **Do the Right Thing!**

Jefferson

Providers' Responsibility: 7 Elements



Jefferson

The Corporate Compliance Program (the "Program") is intended to provide reasonable assurance that we:

- Comply in all material respects with all federal, state and local laws and regulations that are applicable to its operations;
- Satisfy the conditions of participation in health care programs funded by the state and federal government and other payer contracts
- Detect and deter criminal conduct or other forms of misconduct by trustees, officers, employees, medical staff, agents and contractors that might expose your facility to significant civil liability;
- Promote self-auditing and self-policing, and provides for, in appropriate circumstances, voluntary disclosure of violations of laws and regulations;
- Establish, monitor, and enforce high professional and ethical standards.

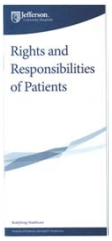
Jefferson.

The Code of Conduct is the Blueprint for all Members of the hospital to *Do the Right Thing*:

- Comply with all applicable laws (including those related to research)
- Conduct affairs in accordance with the highest ethical standards
- Avoid conflicts of interest
- Strive to attain the highest standards for patient care
- Provide equal opportunity and respect the dignity of all staff
- ***Maintain the appropriate levels of confidentiality***
- Maintain a relationship of integrity with each payer
- Conduct all business practices with integrity
- Have proper regard for safety
- Integrate the Code of Conduct into all of your activities

Jefferson.

Patient's Rights and Responsibilities



Jefferson.

Rights and Responsibilities of Patients (as examples):

Patients have the right:
- To be informed of their rights as patients
- To have an advance directive
- ***To privacy and confidentiality***
- To give informed consent
- To access his or her medical record

Patients have the responsibility:
- To act in accord with hospital rules and regulations
- To ask questions and be cooperative
- To be considerate of others
- To refrain from taking unauthorized drugs
- To answer questions fully

Jefferson.

Today's Regulatory Focus

What if you were infected with a communicable virus, would you seek treatment at your place of business?

Jefferson.

Health Insurance Portability and Accountability Act ("HIPAA")

- Overview
- Definitions
- Privacy Rules
- Scenarios

Jefferson.

Health Insurance Portability & Accountability Act of 1996 ("HIPAA")

What is HIPAA? A federal law that:

- Provides for the portability of health insurance
- Defines how "covered entities" including hospitals, can properly use or disclose medical information;
- Establishes protections and safeguards for protected health information ("PHI")
- Prevents healthcare fraud and abuse
- Facilitates uniformity and simplification of certain common healthcare transactions, and
- Includes privacy regulations and security regulations.

Jefferson.

Before we get started, let's discuss a few key terms…

- **Confidentiality:** data or information is not made available or disclosed to unauthorized persons or processes
- **Workforce:** employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
- **Covered Entity:** an entity that provides healthcare services that would use or create protected health information in the course of doing business.
- **Protected Health Information (PHI):** any information that relates to the past, present, or future health condition or treatment that could identify or could be used to identify an individual.
- **Electronic Protected Health Information (ePHI):** electronic health information that is created, received, maintained or transmitted by or on behalf of Jefferson.

Jefferson.

What is Protected Health Information ("PHI")?

- **ANY** information that could identify or could be used to identify an individual (fingerprints, research records, ANY unique identifying number)
- Any health information relating to:
  - past, present or future physical or mental health or condition
  - provision of healthcare (treatment)
  - past, present or future payment for health care
- Verbal, Written, Electronic

Jefferson.

What Else Should Be Protected…

- Name
- Address
- Phone Number
- Medical Record Number
- Social Security Number
- Email Address
- Full Face Photograph Images
- Account/Serial/License Numbers
- Diagnosis & Procedure
- Any date (birth, admit date, discharge date)

Jefferson.

Privacy Practices: Why is Privacy Important?

- Patient privacy is everyone's concern:
  - it's a basic part of patient care
  - it relates to confidentiality of information
  - it relates to respect
- Restricts authorized individuals from misusing PHI
- Clarifies who can use medical information for treatment, payment and healthcare operations
- Provides patients rights and responsibilities

Jefferson.

Privacy Practices

Examples of Permitted Uses or Disclosures of PHI:

- As required by law
- Institutional Review Board (IRB) approval, in certain circumstances (e.g., consent or waiver)
- Activities related to your job; uses and disclosures of PHI is limited to the "minimum amount necessary" to fulfill your job responsibilities- **"Need to Know Philosophy"**

Jefferson.

Privacy Practices

We should abide by procedures highlighted in the Notice of Privacy Practices:

Notice Of Privacy Practices

Jefferson.

Notice of Privacy Practices

Explains to Our Patients:

- Who we are
- How we may use and disclose health information – only for treatment, payment, and health care operations purposes
- Other uses and disclosures of protected health information for which written authorization is NOT required
- Uses and disclosures that do require a patient's specific written authorization
- A patient's rights regarding their protected health information
- Who the Privacy Officer is

Jefferson.

Applying the Privacy Regulations: "Best Practices"

- Requests for patient information may be received from individuals other than the patient and can be received over the phone or in person.
- Common requests for patient information are listed on the following five slides.

Jefferson.

Scenarios and Situations that Apply to You - #1

- Caregiver enters a patient's room to share some healthcare information with the patient. Visitors are present in the room.
  - Assume the visitors will leave, unless the patient is comfortable with their presence and requests they stay.
  - Suggested wording: (To the visitors) "Would you please excuse us. I need to have a word with Mr./Mrs. _____."
  - Or, "I would like to speak frankly with you. Would you prefer that your guest leave?'

Jefferson.

Scenarios and Situations that Apply to You - #2

- A family or friend asks support services staff for medical information about the patient.
  - Redirect the person back to the appropriate caregiver for information.
  - Suggested wording: "The nurse caring for Mr. Smith is the best person to give you that information. Her name is Kathy (give the name if you know it), and you can see her at the nurses station down the hall (give some direction if you can)."

Jefferson.

Scenarios and Situations that Apply to You - #3

- Another employee inquires about the health status of a patient.
  - Ask about the employee's involvement with the patient's care. If in your judgment they are not involved, do not provide them with information.
  - Suggested wording: "Since you are also an employee, you must know this information is confidential."
  - Provide them with an opportunity to justify their request with information about their role in that patient's care. If in your judgment, they are involved, provide them with only the amount of information necessary based upon their role.

Jefferson.

Scenarios and Situations that Apply to You - #4

- A person calls a hospital department to inquire about a patient. Upon looking up the patient, the staff member learns the patient is listed as
"no information."
  - Suggested wording: "I'm sorry but we have no information available on a person by that name."
  - If the caller persists, continue to firmly repeat that we have no available information on this person. As an alternative, suggest they contact the person's family member for information

Jefferson.

Scenarios and Situations that Apply to You - #5

- You are concerned about the health status of a fellow coworker admitted to the hospital and wish to access their medical record to see how they are doing.
  - If you are involved in the patient's care, you may access the medical record to provide the necessary care.
  - If you are not involved in the patient's care, you may not access the medical record for any reason.

Jefferson.

Other Scenarios and Situations that Apply to You

- The following are additional ways to respond appropriately to situations you may face:
  - Keep your voice down when talking about patient matters on the telephone.
  - File records with patient information and do not leave any records containing patient information in public areas.
  - Put waste paper that contains patient information in the right type of trash can.
  - Use fax machines carefully to make sure that patient information does not get sent to the wrong person.
  - Limit the amount of medical information that you leave in a telephone message for a patient. The safest message is: "This is Dr. _____, please call me back at (215) xxx -____.)

Jefferson.

Privacy Violations

- **Mass General** agreed to pay $1 million due to the loss of documents consisting of patient schedules containing names and MR#s for the patients, and billing encounter forms with the name, DOB, MR#, health insurer and policy number, diagnosis and names of providers for 66 of patients. These files were lost when a Mass General employee, while commuting to work, left the documents on the subway train.
- **Rite-Aid Corp in 2010** agreed to pay $1M and develop Policy and Procedures on the proper disposal of prescription bottles after pill bottles on which pill labels with patient names and other PHI were found in industrial trash container accessible to the public.

Jefferson.

Policies

Suggested Policies for Privacy:

- Confidentiality
- Safeguarding Protected Health Information
- Notice of Privacy Practices
- Code of Conduct
- Breach Notification

All employees/contractors/volunteers should review.

Failure to do so may result in unfavorable consequences, up to and including termination or removal from programs.

Jefferson.

HIPAA - SECURITY

- Privacy vs. Security Overview
- Security Objectives
- Security Components
- Scenarios

Jefferson.

HIPAA Security Objectives

- To ensure that the confidentiality & content of all ePHI created, received, maintained, & transmitted stays secure.
- To protect against:
  - Any reasonably anticipated threats or hazards of ePHI
  - Any reasonably anticipated uses or disclosures that are not permitted

Jefferson.

HIPAA Security Components

- As a workforce member, you are responsible to help us safeguard information. This includes:
  - Password Management
  - Location Access
  - Workstation Use
  - Virus Protection
  - ePHI Transmission
  - Log-In Monitoring
  - Security Incidents
  - Encryption
  - Portable Devices
  - Proper Handling of ePHI
  - Social Media
  - Facsimiles
  - Texting
  - Copy Machines

There should be Policies addressing physical, technical and administrative safeguards.

The following five slides address the workforce member's role in some of these areas of security.

Jefferson.

Scenarios and Situations that Apply to You- #1

Password Management

- STANDARDS
  - Do not use Dictionary words (words listed in a dictionary) or Proper names as your password
  - Do not use easily recognizable words like family or pet names, birthdays or addresses
  - Make your password unique
  - Passwords should be a minimum of 6 characters
    - NOTE: Each system has different password requirements; therefore, your system may not enforce this minimum requirement. However, you MUST comply with the organizational standard even if your system does not enforce it.
- BEST PRACTICES
  - Don't share your password (mandatory)
  - Don't post your password
  - Change your password at least every 90 days

If you share your password you could be disciplined for someone else's actions!

Jefferson.

Scenarios and Situations that Apply to You- #2

Workstation Use: Protecting Your Workstation

- Do not share access devices (i.e., ID badges, office or desk keys, key cards or key pad number codes).
  - Know what visitors (i.e., contractors, members of the community, company representatives) are in your area and what their purpose is.
  - Update locks or lock combinations when staff changes occur as necessary (i.e., employee transfers or terminations).
- In addition to a desktop personal computer, a workstation includes:
  - **Personal Digital Assistants (PDA)**
  - **Laptop**
  - **Tablet Personal Computer**
- Assure that an automatic logoff for temporary system inactivity is set.
- Logoff applications when not in use.
- Keep track of your mobile devices and password-protect them.

Jefferson.

Scenarios and Situations that Apply to You- #3

When you receive files containing ePHI:

- Make sure you are receiving this data for a job-related reason, on a "need – to-know basis"
- Do not share this data with anyone unless you have authorized approval
- Do not copy this data to any unencrypted portable storage media (e.g. flash drive, CD, DVD)
- Do not store this data to a personal device
- Destroy this data when it is no longer needed

Jefferson.

Scenarios and Situations that Apply to You- #4

When transmitting ePHI to destinations outside of your organization, it should be required that the data is encrypted.

What is Encryption?

- It is technology that assures data to be unreadable, unusable and indecipherable by an unauthorized person.
- Encryption is the process of transforming plain text with other values so that the data becomes impossible to understand during electronic transmission of the data.

Check with your Information Systems Department:

- Do they have encryption technology software to secure your information as it is transmitted?
- Is there an encryption policy on how to encrypt data located on your intranet?

Jefferson.

Scenarios and Situations that Apply to You- #5

Log-in Monitoring

- Report suspicious log-in events. Examples include:
  - A username other than yours is entered into your log-in box.
  - You leave your desk and return to find you are locked out.
  - You cannot log-in when you begin your work day.
- Report suspicious log-in events to your IS department.
- Information Systems regularly audits log-in attempts by unauthorized users.

Jefferson.

What Your Hospital should do to comply with HIPAA Security

- Provide security training and periodic reminder updates.
- Address organizational standards by implementing the following:
  - Policies and Procedures
  - Business Continuity Plan
  - Contract Approval / Business Associates Agreement
  - Auditing Controls

Jefferson.

Security Violations

- Theft of back-up tapes from a care of a TRICARE Business Associate, Scientific Applications International Corp ("SAIC) affects 5.1 M people.
- Five (5) laptops stolen from Physician Practices in Stone Oak, Texas containing names, SS#s and DOB for over 3000 patients.
- Unencrypted desktop computer was stolen from Sutter Health facility containing healthcare information on 943,000 individuals.
- UCLA Health System reported the theft of an encrypted external computer hard drive containing PHI on 16,288 patients from a UCLA employee during a home invasion. *Password with paper missing.*
- Former UCLA Health System employee became the first person in the nation to be sentenced to federal prison for violating HIPAA (4 months in federal prison). He was a licensed cardiothoracic surgeon who received notice that UCLA intended to dismiss him for job performance reasons. Over the next three weeks, the physician abused his access to the organization's EHR system to view the medical records of celebrities and high-profile patients, including Drew Barrymore, Arnold Schwarzenegger, Tom Hanks, and Leonardo DiCaprio. He accessed the UCLA record system 323 times during the 3 week period.

Jefferson.

Disciplinary Actions for Non-Compliance (cont.)

- Federal Sanctions are divided in 2 categories:
  - Civil Monetary penalties:
    - $100 per incident, up to $25,000 per claim.
- Federal Criminal penalties, which may include fines and/or prison, for the following actions:
  - Unauthorized obtaining or disclosing PHI
  - Obtaining and disclosing PHI under false pretenses
  - Obtaining PHI with the intent to sell, transfer or use for commercial advantage, personal gain or malicious harm
  - Penalties up to $250,000 plus 10 years in prison

Jefferson.

HITECH Act Breach Overview

HITECH: Health Information Technology for Economic and Clinical Health Act.

- HITECH is a part of the American Recovery and Reinvestment Act of 2009.
- It is a federal law that affects the healthcare industry.
- The Act allocated approximately $20 billion to health information technology projects.
- This act expands the reach of HIPAA Privacy and Security rules by extending certain obligations to business associates and imposed a nationwide security breach notification law.

Jefferson.

HITECH Breach Notification Provisions

- The HITECH Act applies to breaches of “unsecured protected health information”.
- Information must be encrypted or destroyed in order to be considered “secured”.

Jefferson.

HITECH – What Constitutes a Breach?

A "breach" is an impermissible acquisition, access, use or disclosure not permitted by the HIPAA Privacy rule. Examples include:

- Unencrypted laptop, flash drive or other removable media or mobile device.
- Patient reports left unattended or not properly disposed of.
- Employees who are not authorized to access PHI look through patient files in order to learn of a person's treatment.
- Nurse gives discharge papers to the wrong individual.
- Billing statements, lab results or diagnostic test results containing PHI mailed or faxed to the wrong individual/entity.
- Placing work-related PHI on your Facebook

Jefferson.

Breach Notification Requirements

- **HITECH ACT**
  - Notice to Patients
  - Notice to DHHS via posting on website
  - Notice to 3 Credit Reporting Bureaus
  - Notice to Media
- **PA and Other State Requirements**
  - Notice to PA & Other Office of Attorney Generals
  - Other Notifications as Required

Jefferson.

Who Will Enforce These Rules?

Office of Civil Rights (OCR)

- Will receive and investigate Privacy complaints
- Will receive and investigate Security complaints

May do reviews of an institution's compliance:
OCR hired KPMG to conduct 150 audits

Office of Inspector General (OIG)

- Need for all companies to understand all 7 elements of a Compliance Program
- OIG Medicare Compliance Reviews beginning 1/9/12 (multiple outpatient and inpatient error types).

Jefferson.

Federal "Wall of Shame" Statistics:

- As of December 2011, 385 incidents affecting more than 500 or more individuals
- Total: 19 Million individuals since September 2009
- Data breaches increased 32% over those reported in 2010
- The average number of lost or stolen records per breach was 2,575, up from 1,769 in 2010
- 55% have involved lost or stolen unencrypted electronic services or media
- 22% involve a Business Associate

Jefferson.

Enforcement for HIPAA and HITECH:

PHI Breaches in your workplace may warrant disciplinary actions up to and including termination.

Jefferson.

Penalty Amounts – Potential Liability

CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE -Section 1176(a)(1)

Violation Category-Each Violation:		All such violations of an identical provision in a calendar year:
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	$1,000–50,000	$1,500,000
(C)(i) Willful Neglect—Corrected	$10,000–50,000	$1,500,000
(C)(ii) Willful Neglect—Not Corrected	$50,000	$1,500,000

Federal Register / Vol. 74, No. 209 / Friday, October 30, 2009 / Rules and Regulations

Jefferson.

Best Practices

Safeguarding patient information is *your* ethical and legal responsibility as part of the workforce.

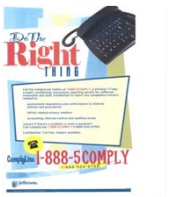
Jefferson.

What is Your Role?

- Be respectful of patient's right to privacy – put yourself in their shoes
- Protect the confidentiality of health information
- Access patient information only when you "need to know" as part of your job
- Do not access, download, transmit, PHI on a mobile device that is not password-protected nor encrypted.
- Be cognizant of when a potential unsecured breach has occurred
- Report any concerns by talking with your supervisor or contact the Compliance or Privacy Officer.

Jefferson.

Or, call the Anonymous Alert Line



Jefferson.