Catholic Health
HIPAA/ HITECH

HEALTH INSURANCE PORTABILITY ACCOUNTABILITY ACT

and HITECH Health Information Technology for Economic and Clinical Health Act
Objectives of HIPAA & HITECH Training

• Understand HIPAA & HITECH
  – Rules and Regulations affecting patient privacy
  – How to Safeguard PHI (Protected Health Information)
  – Your responsibility for access, use, and disclosure of PHI
  – Your duty to immediately report suspected or actual HIPAA breaches

• HIPAA/Concerns/Violations
  – Identify examples of HIPAA violations
  – Know how to report concerns
  – Penalties for HIPAA breaches
HIPAA is

- A patient privacy right
- Legal requirement

Safeguarding

*patient protected health information helps to ensure quality of care and enhances the patient experience.*
American Recovery & Reinvestment Act (ARRA)
- Stimulus Bill contains a section called the HITECH Act
- Calls for adoption of Electronic Health Record by 2014

Imposes:
- Stricter HIPAA Requirements
  - Modifications to Patient Rights
    (outlined in the CHS Privacy Notice to Patients)
  - Notification for Breaches
- Stiffer Penalties for Violators
- Increased Enforcement
What is Protected by HIPAA?

Individually identifiable health information

Also known as

Protected Health Information (PHI)

• Transmitted or maintained in any form or medium
What is Protected Health Information (PHI)?

- Names (includes names of relatives, household members, names of employers)
- Geographic subdivisions smaller than a state
- All elements of dates related to: birthday, admission date, discharge date, date of death, and ages over 89
- Telephone (cell phone) and fax numbers
- Social Security Numbers
Additional Protected Health Information (PHI)

- Biometric identifiers (i.e. finger prints)
- (Full face) Photos
- Medical record number
- Health plan number
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- E-mail and web addressees
- Any other unique identifying data
Privacy Notice Document

Informs patient of their HIPAA rights to:

- **Restrict use and disclosure**
  May request to opt out of patient directory, if self-pay may request no notice to insurance

- **Inspect & copy PHI**
  Requests must be submitted in writing-unless physician agrees & present

- **Amend PHI**
  Subject to physician approval

- **Receive accounting of disclosures**
  Written request needed for a log of disclosed medical info

- **Notification of Unsecured Breach to Individual**
  Allows for individuals of a breach to recover damages through civil action

- **Restrict Use and Disclosure**
  Self-pay patient restriction requests –ie. to insurance co, must be honored

- **Inspect & Copy PHI**
  Extends to request in electronic format and requested in electronic format

- **Minimum Necessary/Limited Data Set**

- **Receive Accounting of Disclosures**
  From Electronic Health Record

- **Restrictions on Marketing Communication**
  Opportunity to opt-out of fundraising- not new to CHS
Consent and Authorization from Patient

- Consent and financial agreement is obtained from the patient upon presenting for treatment and allows disclosure for:
  - treatment
  - payment
  - & healthcare operations
  (i.e. Case Mgmt, Quality Assessment, DOH/JCAHO surveys)

- Authorization from the patient is needed for disclosure of health information that exceeds the Privacy Rule (treatment, payment & healthcare operations)
What Information Can Health Care Providers Share?

- Information necessary for treatment, payment or healthcare operations based on job function and need for the information
- With family and friends of the patient after obtaining the patient’s permission or if unable to obtain permission based on professional judgment that is in the best interest of the patient.
- Necessary health information with licensing and credentialing agencies as required by law
  (see HIPAA policies for additional information)
“Authorized” Access, Use or Disclosure of PHI

Access, Use and/or Disclose PHI based on job function and the need to know the information for treatment, payment or healthcare operations

(review HIPAA policy PRIV-24 for additional information)
Restrictions

Restrict access, use and disclosure to the minimum amount necessary for payment or healthcare operations.

There are disclosure restrictions for:

- HIV information
- Psychotherapy notes (mental health)
- Drug and alcohol treatment

The types of information listed above are protected by federal and/or state statute and may not be faxed or photocopied without specific written patient authorization, unless required by law.

Additional signed authorization must be obtained for restrictions noted above. (see HIPAA policy PRIV-02)
Personal Representatives who have rights to PHI

(See policy HIPAA PRIV-23 for additional information)

- Health Care Agent (Proxy)
  implemented/rescinded upon written order of the attending physician or medical director when the resident/patient no longer has capacity to make health care decisions

- Guardian of adult patient
  if authorized by Judge

- Executor or administrator of deceased
  must have legal authority

- Parent or guardian for minor
  exceptions: mental health notes, drug & alcohol treatment, HIV & STD, pre-natal care, emancipated minors
HIPAA Policies are found

Compliance 360

This includes both:
- Privacy Policies
- Security Policies
Sample of HIPAA Privacy Policies

Located on intranet in Compliance 360 and/or in Department Manuals

Priv 01- Notice of Privacy Practice
Priv 02- Consent & Authorization to use and disclose information
Priv 03- Treatment, Payment, Healthcare Operations
Priv 16- Family and Friends
Priv 18- Required by law
Priv 23- Personal Representatives
Priv 24- Minimum Necessary, use, disclosure & requests
Priv 25- Faxing Medical Information
Priv 26- Storing and Safeguarding
Priv 27- Destroying and Disposing of Medical information
Priv 36- Restrictions on Uses and Disclosures
Hospitalized Patient Request Access to Medical Records

- Attending physician is notified
- A physician or a member of Health Information Management (HIM) will be present during review of the medical record.
- The physician or member of HIM must document in the medical record the verbal request and information reviewed.
- In the event the patient requests copies from the record, the request should be in writing and forwarded to the Health Information Department.
HIPAA Safeguards
Computer Security Policies

• Computer accounts and passwords are confidential and are not to be shared with others
• Do NOT download any programs or software without permission from the IT department
• All e-mail with PHI sent outside CHS needs to be encrypted
• Log off computer screens and close charts containing PHI before leaving area
• Never leave Mobile Computing Devices (ie. Laptops, etc) unsecured and report thefts immediately
• Do NOT open suspicious e-mail attachments or respond to spam
• Do NOT post patient PHI to Social Media sites
• Be aware of your surroundings when discussing PHI
  Lower your voice
Correct Disposal of PHI

• Use the shredder cabinet
• Follow documentation storage policy
• Computer devices must be rendered unreadable
Risk of Identity Theft

Use minimal identifiers and appropriate security.

Careless protection of health information along with unauthorized access/disclosure of PHI can put patients at risk for Identity Theft.
Breach of Protected Health Information (PHI)

Definition of a Breach:
Unauthorized acquisition, access, use or disclosure of “unsecured” PHI.

Secured = Encryption or destruction

A risk assessment is conducted to determine if significant financial, reputational or other risk is present which would require notification.
CHS must provide
Breach Notification

• **Individual**
  Intentional and unintentional disclosure of “unsecured” PHI with financial, reputational, or other harm to the individual

• **Media (TV, Radio, newspaper)**
  if more than 500 people involved

• **Health and Human Services**
  via an annual log and immediately for a breach affecting 500 or more individuals
Unintentional, Incidental Disclosures

Steps have been taken to avoid disclosure but disclosure may have accidentally occurred

While not considered a HIPAA violation...

• Do the best that you can to maintain confidentiality under the circumstances

• Be mindful of areas at risk:
  – Emergency Room
  – Semi-private room
  – Waiting room
Potential HIPAA Violations
(All concerns are to be reported)

- Careless mistakes
- Personal Use
- Personal gain
- Curiosity

Unauthorized access, acquisition, use or disclosure
UNAUTHORIZED ACCESS or DISCLOSURE OF PATIENT INFORMATION

Curiosity can be a normal human trait… however, unauthorized access or disclosure of health information of family members, friends, co-workers, persons of public interest or any other person is a ... VIOLATION and can result in fines, being sued, jail time

Individuals are NOT allowed to look up their own health records
Your Computer Usage can be monitored

Information Technology is able to audit all associate’s internet usage.

Associates should have no expectations of privacy while using CHS computer resources.

Texting of PHI may not be secured during transmission. Check with your phone provider if encryption is available.
Example of HIPAA VIOLATION
Carelessness/ Failure to Safeguard

“…let’s see there are four different Doctor’s with the same last name…hmmm I’ll pick the first one and fax it there. I don’t have time to be looking up all this stuff.”
Example of HIPAA VIOLATION
Unauthorized Disclosure of Medical Record

“Joe, I just thought I’d give you a call and let you know that your neighbor Mrs. Smith had heart surgery last week – I am looking at her record now. You might want to go over and check on her later.”
“Did you hear what happened with Dr. Careless?”

“It was unfortunate that he left that instrument in Mrs. Blaine. She almost died from an infection.”

hmm...that's my doctor. I think I will need to find another doctor...
Example of **HIPAA VIOLATION**

**Social Media & Face Book Entries Regarding PHI & Events at Work**

“...a guy came into the lab today and stole one of the laptops with patient information from the workstation. The guards were unable to find him...”

“...at our nursing home a confused patient got dressed and wandered out of the building...it took the staff 4 hours to find her – she was 10 blocks away...”
Example of HIPAA VIOLATION

Sale of Patient Information

“...thank you for supplying that list of pregnant patients...we would be happy to send them information on our new child care products”

“...It was no problem...anytime you need this information I’ll provide it ... of course I’m assuming you’ll still be providing me $5 for every referral”
Example of **HIPAA VIOLATION**

**Unauthorized Access of Medical Record**

“...Is that a patient from our group?

“...No, my newborn niece is under the care of Dr. Trouble and has had some problems. I just want to see if her test results are back yet.”
Penalties for HIPAA Violations

• Applicable to Catholic Health and to the individual responsible for the breach

• Penalties (Civil & Criminal)
  - Knowing and wrongful disclosure
    up to $50,000 and 1 year in prison
  - Disclosure under false pretenses
    not more than $100,000 and 5 years in prison
  - Disclosure with intent to profit or maliciously harm
    not more than $250,000 and 10 years in prison.

• Mandatory Civil Monetary Penalties
  for “willful neglect”- tiered based on type of breach ($25,000 to $1.5 Million)

• The State Attorney General on behalf of the patient can sue the person responsible for the breach.
HIPAA In the News

- 2008 UCLA employee faces up to 10 years in jail for selling information (PHI) to news outlets.
- February 18, 2009 CVS pays $2.25 million to settle HIPAA privacy case—disposed PHI (Rx bottles) in industrial trash.
  July 2010—Rite Aid agrees to pay $1 Million for similar event.
  August 2011—Walgreens under similar investigation.
- February 19, 2010 22yo Hawaiian mother of 3 children
  One year Jail term for HIPAA violation— for accessing and posting PHI to MySpace.
- April 28, 2010 UCLA Healthcare researcher (licensed Cardiothoracic surgeon from China)
  Jail time for HIPAA violator (snooping)
- April 2011 Providence RI. Physician’s post to FaceBook allowed for identification of patient.
  Disciplined by State board, lost Emergency Room privileges. Irreparable career harm.
Unauthorized Physician Access

July 2009- An Arkansas physician admitted that, after watching news reports on television, he logged on to his hospital’s patient records from his computer at home and accessed a patient’s files to determine if the news reports were accurate. He admitted he accessed the file because he was curious, even though he had had HIPAA training and understood he was violating HIPAA when he accessed the file.

The physician was temporarily suspended from the hospital’s medical staff and pled guilty to a misdemeanor violation of HIPAA

- He was eventually fined $5,000 and sentenced to 50 hours of community service
Unauthorized Access or Disclosure of PHI

- Violates HIPAA/HITECH
- Fails to support patient rights
- Is not in alignment with CHS core values
- Violates CHS HIPAA Policies
- Opens potential for Fines & Penalties
- Can negatively impact upon CHS
- Can negatively impact the person committing the breach
- Can negatively impact the patient
Responsibilities

• Safeguard Protected Health Information (PHI)
  – Lower your voice when discussing PHI
  – Apply correct disposal of PHI
  – Maintain computer security measures

• Only access PHI related to your job function and only disclose PHI to those whose job duties require them to know.

• Report suspected HIPAA concerns immediately
Catholic Health
HIPAA Contacts

Compliance & HIPAA Privacy Officer
Anne Mason 821-4469

IT Help Desk 828-3600, or Sally O’Brien

CHS HIPAA Hotline 862-1790

Corporate Compliance Line (24/7) 1-888-200-5380

All calls are confidential