HI PAA/ HITECH

HELTH
INSURANCE
PORTABILITY
ACCOUNTABILITY
ACT

and

Health Information Technology for Economic and Clinical Health Act

Revised 4/4/14
Your Accountability

Quality Care
Compliance
Reputation
Do No Harm
### Protected Health Information (PHI)

- Biometric Identifiers
- Full face photos
- Medical Record Number
- Health plan Number
- Account Numbers
- Certificate/License Numbers
- Vehicle identifiers
- **Any other unique identifying data**
- E-mail and web addresses
- Names
- Geographic subdivisions smaller than a state
- All elements of dates related to birth date, admission, discharge, or date of death, ages over 89
- Telephone and fax numbers
- Social Security Numbers
- Device identifiers/serial #
Consent 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)
HIPAA Covered Entities

Healthcare providers are HIPAA covered entities. Business Associates are also bound to HIPAA

Access, Use, or Disclosure must be work related

Can Providers Share Information with Patient’s Friends and Family?
Yes, after obtaining the patient’s permission or if unable to obtain patient’s permission the use of professional judgment is allowed if it is in the best interest of the patient.
How the HITECH Act Impacts HIPAA

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

Department of Health and Human Service
Office of Civil Rights
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
HIPAA Policies on Compliance 360 - CHS Intranet

Privacy Policy 33 - Access to Medical Information (Patient)

Patient or Patient’s Representative provides written request
  – Attending physician is notified

Requests while patient is hospitalized
  – Patient or Patient’s Representative requests to see record
  – Attending Provider is notified and if approves of request
    • The review of the medical record is to be supervised.
    • Document the request and information reviewed.
    • If the patient requests copies from the record, the request should be in writing and forwarded to the Health Information Department

See Policy for specific information
Disclosure Restrictions

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.

Must obtain additional signed authorization prior to disclosure with family & friends for restrictions noted above.

(see CHS HIPAA policy PRIV-02)
Breach of Protected Health Information (PHI)

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

Secured
Encryption or destruction

Risk Assessment
Breach notification is required unless there is minimal risk that the PHI has been compromised or another exception has been met.
Risk of Identity Theft

Use minimal identifiers and appropriate security

Careless protection of health information along with improper access to PHI can put patients at risk for Identity Theft.
If required, CHS must provide Breach Notification

• **Individual**
  Intentional and unintentional disclosure of “unsecured” PHI
  ***with significant risk to the individual
  Patient at greater risk for Identity Theft if Social Security Number disclosed

• **CHS Website**
  If 10 or more individuals are unknown

• **Media (TV, Radio, newspaper)**
  If more than 500 individuals are involved

• **Health and Human Services (HHS)**
  Via an annual log and immediately for a breach affecting 500 or more individuals- HHS will post the CHS breach on the HHS web site
Business Associates

Business Associates must now also follow HIPAA and also report breaches to Covered Entity.

22% of Breaches affecting 500 or more individuals in Healthcare implicate a Business Associate.

- Business Associate must notify Covered Entity of Breach.
- Covered Entity must provide notification if required.
Unintentional, Incidental Disclosures

Steps have been taken to avoid disclosure however disclosure may have accidently 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
Curiosity can be a normal human trait.

**However** accessing or disclosing health information on family members, friends, co-workers, persons of public interest, or any others that you are not involved in the care of is a **VIOLATION** of HIPAA.

- Individuals do **NOT** have the rights to look up their own health records (need to submit a written request to HIM)

- Information Technology is able to audit all CHS computer usage
Example of HIPAA VIOLATION
Unauthorized Access of Medical Record

“Joe, I just thought I’d give you a call and let you know that our 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.”
Example of **HIPAA VIOLATION**

**Public Discussion of PHI**

“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.”

Uhmm…that’s my MD. I think I will need to find another doctor...
Example of **HIPAA VIOLATION**

**Computer Blogs & Face Book** Entries Regarding **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 to Outside Vendor

“...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 Family Member’s Medical Record

“…Is that one of our group’s patients?”

“…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.”
HIPAA Safeguards

- Do not allow others to utilize your computer account ID or password.
- Dispose of PHI correctly- shredder bin
- All e-mail with PHI sent outside CHS needs to be encrypted. Verify any faxes sent with PHI
- Log off computer screens and close charts containing PHI before leaving area
- Never leave Mobile Computing Devices (ie. Laptops) unsecured and report thefts immediately
- Be aware of your surroundings when discussing PHI
- Lower your voice
Enforcement & Penalties

- **Enforced by the State Attorney General**
  - Allows patients the ability to file for compensation (sue the violator) if harmed
  - Secretary of HHS must provide for periodic audits of covered entities and business associates to ensure they are complying with the Privacy Rule and Security Rule requirements - Effective Date: 2/2010

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

- **Criminal Penalties** for wrongful disclosure
  applies to individuals (incarceration-jail time)
  up to 10 years based on type of breach
The following is professional misconduct for a physician, physician's assistant or a specialist's assistant:

"Revealing of personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law."
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)

HIPAA In the News

• Spring 2012 Phoenix Cardiac Surgery, PC, of Phoenix and Prescott, Ariz., agreed to pay HHS $100,000 in a settlement and take corrective action to implement policies and procedures to safeguard PHI because of privacy and security violations involving an Internet-based calendar.

• July 2012 Boston hospital notifying patients of potential computer data breach. Nearly 4,000 patients’ PHI may have been compromised when a physician’s personal laptop computer was stolen from a Boston hospital, according to a July 23 report by hospital.

• August 2012 Stanford University Medical Center reported a computer containing medical and personal information for approximately 2,500 patients stolen from a Stanford faculty member’s locked office.
In the News
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
Duty to report suspected or actual HIPAA violations immediately to one of the following:

Compliance & HIPAA Privacy Officer
Leonardo Sette-Camara, Esq. 821-4469

IT Security Officer
Peter Capelli, 862-1777

IT Help Desk 828-3600

CHS HIPAA Hotline 862-1790

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

All calls are confidential