HIPAA and HIPAA Compliance with PHI/PII in Research
HIPAA Compliance

- Federal Regulations-Enforced by Office of Civil Rights

- State Regulations-Texas Administrative Codes

- Institutional Policies-UTHSA HOPs/IRB Policies

- Affiliates Policies-UHS/VA/Christus/Methodist
What is HIPAA

- HIPAA is a federal law Title I and II
- Limits the ability of a new employer plan to exclude coverage for existing conditions
- Allows enrollment in group health plans even if you lose other coverage or other life events
- Prohibits discrimination of employees with prior medical conditions, genetic information
- Guarantees access to and renewal of health insurance policies
- Requires Covered Entities to maintain privacy and security of individually identifiable health information
What is a Covered Entity?

- Health Plans
- Health Care Providers
- Health Care Clearinghouses

Individuals or organizations who electronically transmit health information related to HIPAA billing transactions.
What is PHI?

Individually identifiable health information:

- Pertaining to past, present, or future physical or mental conditions including:
  - Diagnosis and/or treatment of health condition (i.e. medical histories, test and laboratory results)
  - Payment for healthcare (i.e. insurance information and other data that a healthcare professional collects to identify and determine appropriate care, including demographic information)

- Maintained or transmitted in electronic, paper or oral format or recorded in any form or medium.

- Created, used (accessed) or disclosed (released) by a covered entity.
Important Point

Personal Identifier + Health Information = PHI
18 Identifiers

- Name (any derivation including a patient’s initials)
- Street address, zip code
- All elements of dates--DOB, DOS, Discharge date
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- SSN (including last four digits of SSI)
- MRN
- Health plan beneficiary number
- Account number
- Certificate/license numbers
- Vehicle license plate
- Device identifier and serial numbers
- URL
- Internet Protocol (IP) Numbers
- Biometric identifiers (e.g. fingerprints)
- Full face photo images and any comparable images
- Any other unique identifying number, characteristic, or code and other info that could be used in combination with other info to identify
Handling A Person’s Identifiable Health Information (PHI)

- A researcher may be given access to someone’s PHI when a “valid authorization” is obtained from that person.
- A “valid authorization” must include all of the elements that are required by the privacy rule.
- The person has the right not to agree to the authorization and the right to later revoke their authorization.
- The authorization will state how long it will be in effect.
- If signed by a 3rd party, that person’s authority to give authorization on behalf of the subject needs to be documented.
- Researcher may only collect, use or disclose a subject’s PHI in the manners described in the authorization that was signed by the subject, unless a waiver or alteration is approved by the IRB.
Required Elements of a Valid HIPAA Authorization

- What PHI is being collected
- How the PHI will be collected
- Why PHI is needed
- Who will collect and use the PHI
- To whom the PHI will be disclosed and why
- That PHI disclosed to another entity may no longer be protected by the privacy rules
- Strategies used to protect PHI (if PHI photocopied or electronically submitted)
- How long authorization will remain in effect
- State the person has the right to decline signing
- May later be revoked and steps to follow
- If signed by 3rd party, authority to sign
- Copy provided to participant
A patient (or subject) has a right to know about PHI being disclosed without an authorization and so may request that a covered entity provide an accounting of all disclosures made without an authorization.

For that reason, the covered entity that permits a researcher to access PHI without an authorization will likely ask him/her to provide a list of the records accessed.
Ways To Obtain & Use PHI For Research

- HIPAA Authorization by Research Participant
- Waiver or Alteration of HIPAA Authorization by IRB/Privacy Board
- De-Identification of Data (removes all identifiers)
- Limited Data Set & Data Use Agreement
De-identification of PHI Data Methods

- **Expert Determination § 164.514(b)(1)**
  - Apply statistical or scientific principles
  - Very small risk that anticipated recipient could identify individual

- **Safe Harbor § 164.514(b)(2)**
  - Removal of 18 types of identifiers
  - No actual knowledge residual information can identify individual
Limited Data Sets
May Include Identifiable Data

- Admission, discharge, and service dates
- Date of birth
- Date of death
- Age (includes ages 90 or over)
- Five digit zip code or any other geographic subdivision, such as state, county, city, precinct
Database Security

All databases, including data containing PHI from research studies will need the following:

- A designated administrator
- Security measures taken for data security - encryption
- Policies on research databases to define location and when other approvals needed.
- Use of RedCap and CIRD access
Business Associates and Their Subcontractors

Person or entity that carries out, assists with the performance of, or performs a function, service or activity for a covered entity using that entity’s PHI

- Contractual agreement

- Subject to compliance with HIPAA privacy and security rules
HIPAA and IRB

- Authorizations/Waivers/Alterations
- Locations for conducting research-affiliates
- Appropriate security of PHI
- Reportable events
- Communication with affiliates for HIPAA incidents/breaches
Other HIPAA Issues With Research

- Encryption of emails to external email domains
- Mobile device management
- Use of USBs, CDs, etc
- Access to electronic health records
- Disclosure of PHI to unauthorized individuals
- Use of personal clouds or DropBox
- Others?
Determination whether an unauthorized use or disclosure of unsecured PHI is a “breach” requiring notification

- Risk assessment completion
- Individual notification of breach
- HHS notification on-line
Mandatory Breach Notification

The HITECH Act applies to breaches of “unsecured” protected health information”.

Information must be encrypted or destroyed in order to be considered “secured”.

If you suspect a breach has occurred, promptly notify your immediate supervisor.
If a breach has occurred, reporting requirement must be satisfied.
HITECH- What Constitutes a Breach?

A “breach” is an impermissible acquisition, access, use or disclosure not permitted by the HIPAA Privacy or Security Rules.

Examples Include:

- Sending PHI by email without encryption
- Laptop containing PHI is stolen
- Researcher who is not authorized to access PHI looks through patient files in order to learn of a person’s treatment
- Researcher misplaces research documents with study subject PHI
- Researcher sends wrong sponsor study subject information including PHI
- Researchers sends sponsor more PHI than necessary
- Research office theft results in stolen PHI
- Unencrypted flash/jump drive containing PHI is lost
Safeguarding PHI

- Do not store PHI on portable devices (laptops, tablets, smartphones)
- Do not store PHI on removable media (e.g. CD, DVD, flash drive) unless it has been fully encrypted
- Do not use social media accounts (e.g. .gmail, .yahoo) and social media (e.g. LiveChat, Jabber) messaging tools for exchanging PHI
- Do not text PHI
- Do not forget to encrypt (++) any email sent and limit the PHI to minimum necessary only
- Do not fail to properly redact reports sent to study sponsor affiliates
- Do not send identified data when only de-identified data is required
Questions?