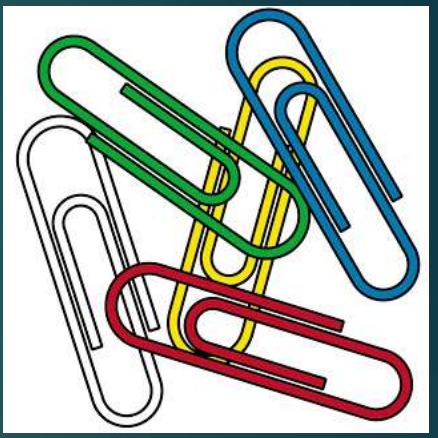
HIPAA and Research Contracts

JILL RAINES, ASSISTANT GENERAL COUNSEL AND UNIVERSITY PRIVACY OFFICIAL

Just a Few Reminders…

- HIPAA applies to Covered Entities
- HIPAA is a federal law that governs the privacy and security of "Protected Health Information" of
  - -patients
  - -health plan enrollees
  - -participants in research with a treatment protocol



- Researchers may access, use, and disclose PHI only in accordance with HIPAA and other laws
- Researchers must protect PHI in accordance with HIPAA and other laws

HIPAA Privacy and HIPAA Security

Privacy:	Paper	Verbal
	Administrative	Physical Security
Security:	Electronic Devices	Transmission
	Administrative	Storage and Back-up

What is PHI?

- Individually identifiable health information
- Created or received by a covered entity
- Related to past, present, or future physical or mental health, condition, or treatment and the payment & benefits for it
- Maintained or transmitted electronically or otherwise
- Written or spoken

What Makes Health Information Identifiable?

- Name
- Street Address
- Dates (except year)
- Telephone number
- Fax number
- Email, URL, IP addresses
- Biometrics (finger, voice)
- Unique identifying number/code/characteristic

-Social Security Number

-Account and Certificate/License Numbers

-Medical Record Numbers

-Health Plan Beneficiary Numbers

-Device and Serial Numbers

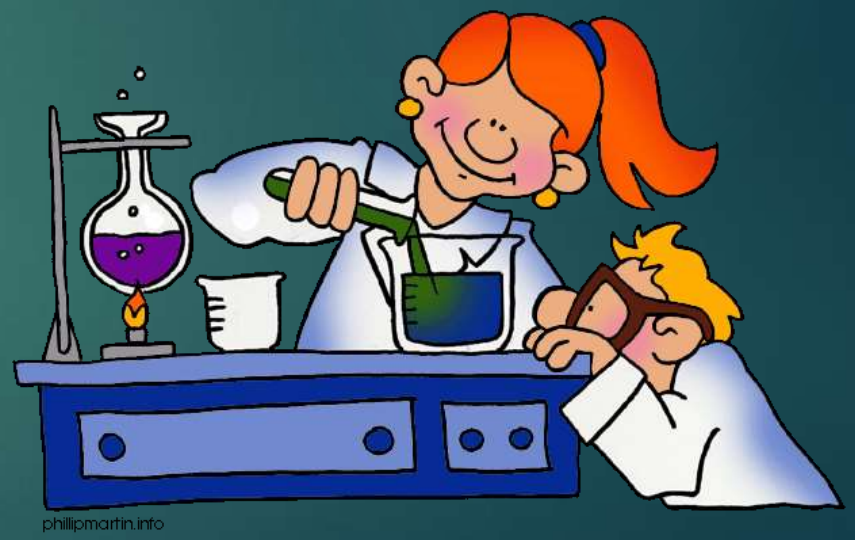
-Vehicle Numbers (VIN, tag)

-Identifying Photos

-Anything thing else that can be used to identify the individual

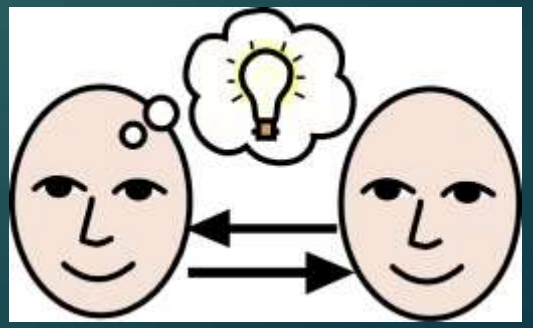
How Does HIPAA Affect Research Contracts?

- Who is the PI authorized to share the PHI with?
- Can the PHI be published?
- When should or must data be de-identified?
- What is a Data Use Agreement?
- Is there a Business Associate relationship?
- Security Issues
  - Where will PHI be stored?
  - How will it be transmitted?
  - What if my software or equipment stores PHI?



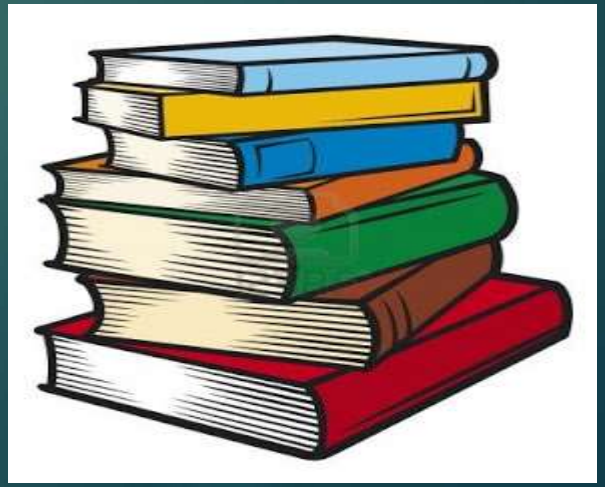
I Want to Share the Data with Other Researchers

- Let ORA and IRB know you want to be able to share PHI so they can ensure the contract, the ICF, and the HA allow for this.
- Who does the contract state will obtain participant authorization for you to share PHI? (The sponsor? OU?)
- Without authorization and approval, you can share PHI only if:
  - You can de-identify the data, OR
  - You can use a Data Use Agreement, permitting you to use only designated identifiers (a limited data set).



I Want to Include PHI in My Publication

- If your intend to publish some of your data:
  - Inform ORA so they can ensure publication is permitted in the terms of the contract
  - Review the Informed Consent Form and HIPAA Authorization to ensure they include notice of the intent to publish



The Contract Says I Must De-Identify Data

- De-Identified Data
  - Has all 16 identifiers removed PLUS anything else that can be reasonably anticipated to be used to identify the subject, OR
  - Have Been Determined By
    - an independent third party statistician
    - "with knowledge of and experience with generally accepted statistical and scientific principles and methods"
    - to have a "very small risk" of being used alone or with other information to identify the subject.

The Contract Offers Data in a Limited Data Set – What is That?

- When removing all 18+ identifiers will not leave you with sufficient data to accomplish your purpose and obtaining participant authorization is not an option, a Limited Data Set may work

- LDS may include ONLY:
  - Dates (excluding DOB if possible)
  - City, state, 5-digit zip code
  - Ages in years, months, days, or hours

HIPAA, PHI, LDS… Now a DUA??

- The law requires the use of a Data Use Agreement if you will be using or sharing PHI in a Limited Data Set
- A DUA governs how the LDS may be used, including prohibiting the recipient from trying to re-identify the subject
- A DUA must be routed to and signed by ORA

What is a Business Associate? And Am I in a Relationship?

- Individual or entity that:
  - Performs a service
  - For or on behalf of a Covered Entity
  - Using the CE's PHI

- Examples:
  - A company tests samples for a researcher
  - A company bills for a service a researcher provides
  - A company destroys

When There IS a Business Associate Relationship:

- Tell ORA if you think a BA might be involved in your study.
- Understand WHO the Business Associate is – OU? Sponsor? Other?
- Must enter into a Business Associate Agreement (BAA)
  - Common terms that may cause delays:
    - Indemnification
    - Length of time to notify of breach

Can HIPAA-Related Research Violations Occur? YES!

PRIVACY-RELATED VIOLATION EXAMPLES

- Publication of PHI without Authorization from participant
- Disclosure of PHI to sponsor, when contract required de-identified
- Sharing PHI with a Business Associate without a BAA in place
- News filming permitted in lab; name of subject visible on label
- Email to all participants; recipients not blinded
- Sent completed enrollment forms to wrong participant
- Collected data without HIPAA Authorization from participants
- Left test results on participant's answering machine
- Sent participant PHI to wrong sponsor

There ARE Consequences to not Complying with HIPAA

- Monetary penalties up to $1.5M per occurrence

- Jail time up to 10 years

- Use the safe harbor!

QUESTIONS???