IRB, HIPAA, and Clinical Research

A presentation by
CHS Privacy and Security Offices
UAB Institutional Review Board
UAB Health System
UAB/UABHS HIPAA Operations Team
Getting Started...

HIPAA
“No, it’s not a female Hippopotamus, anyone else know?”
A Quick Review

The Health Insurance Portability and Accountability Act of 1996 was signed into law on August 21, 1996. The portions of the regulations that are important for our purposes are those that deal with protecting the privacy and security of protected health information.
HIPAA Covered Entities

The Children’s Hospital of Alabama, Children’s Health System, and all Private Practices

UAB
- School of Dentistry
- School of Health Professions
- School of Medicine
- School of Nursing
- School of Optometry
- Joint Health Sciences Departments

UAB Health System
- University Hospital
- The Kirklin Clinic
- UA Health Services Foundation
- Callahan Eye Foundation Hospital
- VIVA Health
- Ophthalmology Services Foundation
- UAB Medical West
- UAB Highlands
The Privacy Rule regulates the ways that *individually identifiable health information* known as *protected health information (PHI)* is used or disclosed.

Researchers should be aware of the Privacy Rule because it establishes the conditions under which PHI can be utilized for research.
HIPAA Security

☐ The Security Regulations require covered entities to protect PHI against loss, unauthorized access, or misuse. The regulations include assessing the threats and risks to information and assuring confidentiality, integrity, and availability of the data being protected.

☐ If researchers are utilizing PHI, they must
  - Provide and maintain database security, including physical security and access.
  - Control and manage the access, use, and disclosure of PHI.
HIPAA and Research

HIPAA privacy and security regulations:

- impact the use and disclosure of PHI for research.
- do not replace or reproduce other federal research regulations; therefore, all existing regulations remain in effect.
- apply whether or not the research is funded by the government.
Data Protected by HIPAA

- Written documentation and all paper records
- Spoken and verbal information including voice mail messages
- Electronic databases and any electronic information containing ePHI stored on a computer, PDA, memory card, USB drive, or other electronic media
- Photographic images
What is protected health information or PHI?

Any information, **including demographic information**, that is **TRANSMITTED** or **MAINTAINED** in any **MEDIUM** (electronically, on paper, or via the spoken word) that is created or received by a health care provider, health plan, or health care clearinghouse that relates to or describes the past, present, or future physical or mental health or condition of an individual or past, present, or future payment for the provision of healthcare to the individual, and that can be used to identify the individual.
PHI Data Elements

The following identifiers of the individual, or of relatives, employers, or household members of the individual, are considered PHI:

1. Names
2. Geographic subdivisions smaller than a state (street address, city, county, precinct, zip, equivalent geo-codes)
3. All elements of dates (except year) including birth date, admission and discharge dates, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
PHI Data Elements (continued):

10. Account numbers
11. Certificate/License numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, code, except as allowed under the ID specifications (164.514c)
So that means...

Being able to link any one of these 18 PHI data elements to an identified diagnosis or medical condition means that PHI is being maintained.

Examples:
- A database entitled “Liver Transplant Recipients” containing only individuals’ names is linking 1 PHI data element with a medical condition. Therefore, the database contains PHI.
- When conducting a survey in which you contact potential research participants, if they provide you with information that is PHI and you record and/or store it, then PHI is being maintained.

Do you have PHI as part of your research data?
IRB and Clinical Research
Looking for a cartoon...
Storage and Security of Research Data

- The IRB is concerned with ensuring that the confidentiality of research participants’ records/information is maintained regardless of the data format (paper or electronic).

- Each protocol must adequately address confidentiality of participants’ records/information.
Use of Internet/Web

- The IRB is concerned with ensuring that the confidentiality of research participants’ records/information is maintained when data are sent over the Internet.
- This includes use of data sharing sites like Google.
Human Subjects Protocol (HSP) Confidentiality: Question #22

- Describe the manner and method for storing research data and maintaining confidentiality. If data will be stored electronically anywhere other than a server maintained centrally by UAB or CHS, identify the departmental and all computer systems used to store protocol-related data, and describe how access to that data will be limited to those with a need to know.

- If data will be stored electronically anywhere other than a server maintained centrally by UAB or CHS...contact HIPAA Security for guidance.
HSP Question #22 continued

- Will any information derived from this study be given to any person, including the subject, or any group, including coordinating centers and sponsors?
  
  Yes

  No

- If YES, complete i-iii:
  
i. To whom will the information be given?

  ii. What is the nature of the information?

  iii. How will the information be identified, coded, etc.?
The IRB must review research for the process in which:

- Data is maintained electronically for storage and data analysis.
- Databases used to collect/store information for current research or for future research use are maintained.

The IRB will ask about storage of data on final report form.
Database Research: Clinical? Research? Both?

- The intent of the research is to generate and maintain a database for continuing research purposes.
- Researcher is gathering information about human subjects to populate a database to be used for research purposes.
- The database may have a dual intent. If research is an intent, then it must have IRB review and approval.
Dual Intent of Database

- Dual=For purposes of clinical and research
- If clinical only, review for compliance with HIPAA security standards.
- If intent includes research, then must have IRB review.
Data collected for a protocol may not be released to others (including other researchers) without first obtaining IRB approval. This includes data from terminated protocols.

If there is a change in storage (from paper to electronic), a revision must be submitted to the IRB for review.
The following security measures must be described and/or confirmed in the research protocol to the IRB:

- Coding
- Encryption
- No data taken off-site
How Can Researchers Use or Disclose PHI in Compliance with HIPAA?

- If the Institutional Review Board (IRB) has approved the research and
- One or more of the following conditions exists:
  1. The activity is preparatory to research.
  2. The research involves only decedent PHI.
  3. The research uses a “limited data set” and data use agreement.
  4. The patients or participants have signed an authorization to use the PHI for the research.
  5. The IRB has granted a waiver for the required patient/participant signed authorization.
De-Identified Data and HIPAA

- If data have been de-identified, meaning that all 18 PHI data elements have been removed prior to receipt by the researcher, no further action is required to meet HIPAA compliance. The de-identified data are not PHI.

- See “An Overview of the HIPAA Privacy Rule and Research at UAB” regarding statistical methods to de-identify data and re-identifying codes. The overview is available at www.uab.edu/irb/hipaa/hipaa-handbook.pdf.
Recruiting and Screening

- Research recruitment techniques must meet HIPAA standards for privacy and confidentiality.
- Investigators must separate the roles of researcher and clinician and must not use their clinical access to search patient records for potential research participants.
Four Acceptable Means of Recruiting Research Participants

1. **Recruitment by treating physicians or other health care providers:**
   Physicians and other health care staff may review only their own patients’ records, which includes the records of patients within their treatment group, to identify potential research subjects. Treating physicians or staff may contact these patients to discuss with them the opportunity to participate in a research study.
Four Acceptable Means of Recruiting Research Participants

2. Recruitment by non-treating physicians or health care staff

If the researcher is not involved in the treatment provided patients, then the research must include a description of the plan for recruitment in the research protocol submitted to the IRB. These plans are reviewed by the IRB on a case-by-case basis to ensure appropriate contacts are made to the patients regarding the research study opportunity.
Four Acceptable Means of Recruiting Research Participants

3. **Screen for eligibility**

If health information will be requested from potential research participants as part of the screening process, then researchers, before the screenings, must obtain either (1) a signed authorization from the potential research participants or (2) a partial waiver of authorization from the IRB to allow the solicitation.
Four Acceptable Means of Recruiting Research Participants

4. Request that interested individuals contact the research staff

Researchers may recruit research participants by using IRB-approved advertisements, brochures, and other means of communication.
HIPAA Privacy

Details Related to Research
“A lack of privacy and confidentiality suit was filed today by a lawyer representing three white mice from a research lab.”
Release of Data

- Direct all requests to health information management, medical information services, or medical records department.
- Principal investigators or designated researchers must provide a copy of the fully executed IRB approval form to the covered entity holding the data before the data can be released for research.
- A covered entity may require the investigators complete their HIPAA compliant Authorization for Use/Disclosure of Health Information form in addition to providing the IRB approval form.
- For electronic access, PIs will be asked to submit the names of those working on the study.
Minimum Necessary Standard

- HIPAA requires that a covered entity limits the PHI it releases/discloses to a researcher to the “information reasonably necessary to accomplish the purpose.” A covered entity relies on the researcher’s request and the documentation from the IRB to describe the minimum PHI necessary to accomplish the research study.

- A signed authorization from the research patient or participant supersedes the minimum necessary restriction.
A Business Associate Agreement (BAA)...

☐ Is required before you contract a third party individual or vendor to perform research activities involving the use or disclosure of PHI.

☐ Binds the third party individual or vendor to the HIPAA regulations when performing the contracted services.

☐ Must be approved in accordance with institutional policies and procedures.

Additional information about BAAs is on the UAB/UABHS HIPAA Website at [www.hipaa.uab.edu](http://www.hipaa.uab.edu).
Patient Rights

HIPAA guarantees certain rights of privacy to patients.

If PHI is released or disclosed to a researcher, then the researcher becomes responsible for ensuring that the use and disclosure of PHI is compliant with HIPAA regulations as outlined in the UAB/UABHS HIPAA standards.
HIPAA Security
The HIPAA Security Rule

- Emphasizes security management and controls.
- Contains 18 standards in three categories for protecting ePHI:
  - Administrative: Policies and procedures to prevent, detect, contain, and correct information security violations
  - Physical: IT equipment and media protections; physical security
  - Technical: Controls, mostly IT applications, for access, information integrity, and audit trails
The HIPAA Security Rule (cont.)

- Enforces the following:
  - Confidentiality – Information is accessed only by authorized individuals with the understanding that they will disclose it only to other authorized individuals.
  - Integrity – Information is the same as in source documents and has not been altered or destroyed in any unauthorized manner.
  - Availability – Information is accessible to authorized individuals when they need it.
What are the risks associated with a breach in security?

- Risks to Individual whose PHI is compromised:
  - Embarrassment, misuse of personal data, victim of fraud or scams, identity theft

- Risks to the Institution:
  - Loss of information and equipment, trust of constituencies, reputation, future grant awards; negative publicity; penalties, fines, litigation

- Risks to Research:
  - Loss of data or data integrity, funding in jeopardy

- Risks to Investigator or Employee:
  - Loss of data, time, funding, reputation; embarrassment; disciplinary action, fines, penalties, prosecution
Sources of Data Leaks

- Email
- Portable computing/storage devices
  - Laptops
  - Thumb drives
  - External portable drives
  - Cell or Smart phones
- Web-based file shares
- Old equipment that is improperly disposed or decommissioned
The Researcher must...

- Provide and maintain database security, including physical security and access.

- Control and manage the access, use, and disclosure of the PHI.
Physical Security

- Control access to research areas.
- Store PHI in locked areas, desks, and cabinets.
- Lock offices, windows, workstations, sensitive documents, laptops, PDAs, portable computing devices, and media when unattended or not in use.
- Obtain lock down mechanisms for devices and equipment in easily accessible areas.
- Challenge persons without badges in restricted areas.
- Verify requests of maintenance, IT, or delivery personnel.
- Never prop open security doors or unarm security alarms.
Desktop/Workstation Security

- Use strong passwords and do not share the passwords with anyone.
- Arrange computer screen so that it is not visible by unauthorized persons.
- Log off before leaving the workstation or allowing others to use the computer.
- Configure the workstation to automatically log off and require user to login if no activity for more than 15 minutes.
- Set a screensaver with password protection to engage after 5-10 minutes of inactivity.
- Manage your research data. Store documents and databases with ePHI securely on a network file server. Do NOT store ePHI on the workstation (C: drive).
Portable Device Security

Portable devices include laptop, hand-held, and notebook computers, personal digital assistants, cell phones, smart phones, and portable memory devices such as thumb and jump drives.

**Basic Philosophy:** Do not use a portable device for storing ePHI.

**NOTE:** Do not use your personally owned portable device for UAB/UABHS business unless such use is specifically approved by senior management.
And more Portable Device Security...

However...If the use of a portable device is approved by senior management, security measures must be followed:

- Use passwords...STRONG passwords.
- Delete ePHI when it is no longer needed.
- Keep your application software up-to-date.
- Back-up critical software and data on a secured network.
- Follow all recommendations for workstation security.
- Use only VPN for remote wired and wireless connectivity.
- Check with IT representatives for other safeguards.
- **#1: Use encryption when transporting ePHI on any mobile computing device.** Be sure to backup encryption keys.
What is encryption?

The process of transforming data to an unintelligible form in such a way that the original data can not be obtained without using the inverse decryption process.

For your convenience, encryption software is available from UAB HSIS (934-8888), UAB AskIT (996-5555), or CHS (939-6568 or gethelp@chsys.org).
Email Security

☐ General Rule: Do NOT send emails containing PHI outside your network.

☐ Email containing PHI being sent to addresses outside the local network must be encrypted. Ask your IT representative to assist with encryption.

☐ Do not FORWARD your system emails to outside email systems, i.e. AOL, hotmail, yahoo, gmail.
Internet Security

- Do not use web-based personal file and backup media, i.e. Google docs, spreadsheets, personal backup sites, etc.
- Do not surf the web if using an account with administrator rights.
- Do not transmit any confidential information over the Internet unless it is encrypted.
Account Management

- Do not share your user account, password, token, or other system access.
- Use strong passwords, the longer the better. Include upper and lower case letters, numbers, and special characters (#, %, ?, $).
- Do not use pet names, birthdates, or words found in the dictionary.
- If you must write down your password, keep it locked up or in your wallet protected like a credit card.
- Do not enable your browser to remember your password.
- Only access PHI/ePHI for business related purposes.
- Do not use your system access to look up medical information on yourself, family, friends, or coworkers.
- Notify IT support immediately if you believe your system access has been compromised.
Disposal of Media

- Know your organization’s policies for disposal of PHI
  - Paper: usually goes in shredders or locked bins for shredding
  - Electronic media (disks, CDs, film): usually go in special purpose shredders or disposal boxes
  - Electronic files: ask IT representative for assistance—Remember that to “delete” a file does NOT get rid of the file!
Identifying Possible Security Incidents

- When logging on, watch your system for unusual or incorrect messages.
- Note if your computer suddenly becomes very slow and remains that way.
- Notice if your screen changes.

These situations often mean technical problems; however, malicious software can cause the same results. Contact your IT representative if these things occur.
What if an incident occurs?

- Contact the appropriate helpdesk: CHS at gethelp.chsys.org or call 939-6568; UAB HSIS, call 934-8888; or UAB AskIT, call 996-5555.
- Contact the IRB office at 934-3789.
- Gather as much information regarding the incident as possible.
- Document information on the appropriate incident reporting form.
- Do not delete anything.
- If information or equipment is stolen, contact the appropriate Police Department and file a report.
- Cooperate with investigators (both internal and external).
- Refer external inquiries regarding the incident to the appropriate office:
  - UAB Media Relations: 934-3884
  - CHS Privacy Officer: 939-5959
Children’s Health System Contacts

- Kathleen Street, JD, LLM, CIPP
  CHS Privacy Officer and Risk Manager
  (205) 939-5959, Kathleen.Street@chsys.org

- Pam Atkins
  CHS Information Technology Divisional Director and HIPAA Security Officer
  (205) 939-6556, Pam.atkins@chsys.org
Others That Can Help

- UAB AskIT Help Desk at 996-5555
- UAB HSIS Help Desk at 934-8888
- Your UAB/UABHS HIPAA Entity Privacy Coordinator or your UAB/UABHS HIPAA Entity Security Coordinator—contact information on the HIPAA Website at www.hipaa.uab.edu
Our HIPAA Mantra

Everyone is responsible for the privacy and security of protected health information.

Thank you!
IRB, HIPAA, and Clinical Research

Questions?