Using and Disclosing Protected Health Information for Research

Lynn Combs, JD
Manager, Compliance and Privacy
lynn.combs@uvmhealth.org

February, 2023

THE University of Vermont HEALTH NETWORK

Outline

- Introduction
- PHI and HIPAA Basics
- Types of Data Sets
- Use of PHI in Research – Six HIPAA Paths
  - Subject Authorization
  - Waiver of HIPAA Authorization
  - Preparatory to Research
  - Research on Decedents
  - Limited and De-Identified Data Sets
- Special Topics
  - Aggregated Data
  - Coded Data v. De-Identified Data
  - Data Storage

PHI and HIPAA Basics

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- Federal Regulations (45 C.F.R. Parts 160-164)
- Applies to “covered entities”:
  - Health Plans (e.g., commercial insurers, Medicare, Medicaid)
  - Health Care Clearinghouses (middlemen between providers and payers)
  - **Health Care Providers who transmit electronic health information**

What is Protected Health Information (PHI)?

Protected Health Information (PHI) is all individually identifiable health information, whether oral or recorded in any form or medium, relating to the:

- Past, present, or future physical or mental condition of a patient
- Provision of healthcare
- Past, present, or future payment for the provision of healthcare to a patient

HIPAA's 18 Identifiers

- ❑ Names
- ❑ All geographic subdivisions smaller than a state
  - ➢ Includes cities, counties, street addresses, precinct, geocodes, etc.
  - ➢ Specific exemption for certain zip codes
- ❑ All elements of dates (except year) for dates that are directly related to an individual
  - ➢ Including birth date, admission date, discharge date, death date, and
  - ➢ all ages over 89 must be aggregated into a single category of age 90 or older
- ❑ Telephone numbers
- ❑ Fax numbers
- ❑ Email addresses
- ❑ Social security numbers
- ❑ Medical record numbers
- ❑ Health plan beneficiary numbers
- ❑ Account numbers
- ❑ Certificate/license numbers
- ❑ Vehicle identifiers and serial numbers, including license plate numbers
- ❑ Device identifiers and serial numbers
- ❑ URLs
- ❑ IP addresses
- ❑ Biometric identifiers, including finger and voice prints
- ❑ Full-face photographs and any comparable images
- ❑ Any other unique identifying number, characteristic, or code
  - ➢ Unique tattoo, birthmark, feature
  - ➢ Clinical trial subject number

Primary HIPAA Rule

- Without an individual patient's written permission, **we *cannot* access/use or share (disclose)** the patient's PHI unless HIPAA makes an explicit exception for it.

- Rule requires analysis of each individual data request to make sure HIPAA allows it
  - Cannot rely on the person's job title, who their employer is, etc.
  - IRB approval alone is not sufficient; must satisfy one of six HIPAA paths that permit the use of PHI for research

“Use” v. “Disclosure”

- **Use – PHI stays inside UVMHN:** “Use means the sharing, employment, application, utilization, examination, or analysis of [PHI] within an entity that maintains such information.”

- **Disclosure – PHI leaves UVMHN:** **“**Disclosure means the release, transfer, provision of access to, or divulging in any manner of [PHI] outside the entity holding the information.”

Who Is and Is Not A Part of the "Covered Entity"?

- UVMHN Affiliates are an "ACE" (Affiliated Covered Entity)
  - "ACE": Separate covered entities that designate themselves as a large single covered entity for purposes of HIPAA
  - "ACE" Members: AHMC, CVMC, CVPH, ECH, HHH, Medical Group, Porter, UVMMC
  - UVMHN is NOT a covered entity, it is a business associate of the affiliates
  - Employees and other members of the affiliates' "workforce"

- UVM, LCOM, School of Nursing, etc. are **not** a part of the covered entity/ACE (however, some individuals may be considered members of the Covered Entity workforce)

Types of Data Sets

Minimum Necessary Standard

- HIPAA requires that we only disclose the ***minimum amount of information necessary*** to accomplish the purpose of the use, disclosure or request.

- Examples:
  - If a researcher does not need to link the subject information to the actual medical records/subjects' identities then they should receive a limited data set not a full data set
  - Researchers are required to tailor their procedures to ensure they are reviewing the minimum amount of PHI necessary (e.g., not reviewing a full clinic schedule when someone on the clinic side can identify potential subjects)

Direct Identifiers v. Indirect Identifiers

- Direct identifier: An identifier that links to one specific person, can be used by itself to identify someone.
  - Name, social security number, medical record number, medical device number, email address, phone number, etc.

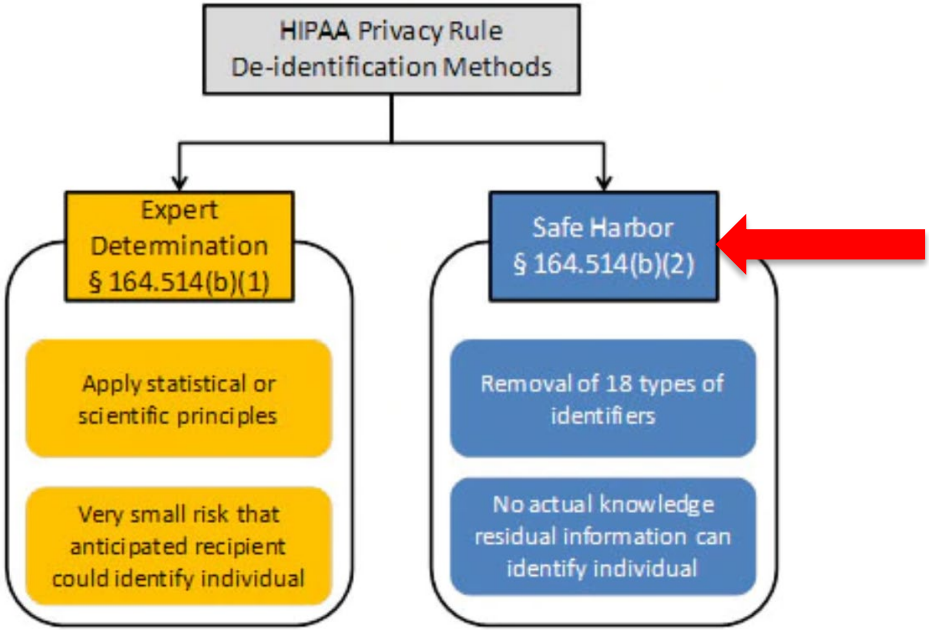
- Indirect identifier: An identifier that does not link to one specific person but can be used in combination with other information to identify a person.
  - Dates, including date of birth/death, dates of treatment, zip codes, cities, counties, etc.

Types of HIPAA Data Sets

- De-Identified Data Sets
- Limited Data Sets
- Full Data Sets

De-Identified (Under HIPAA) Data Sets

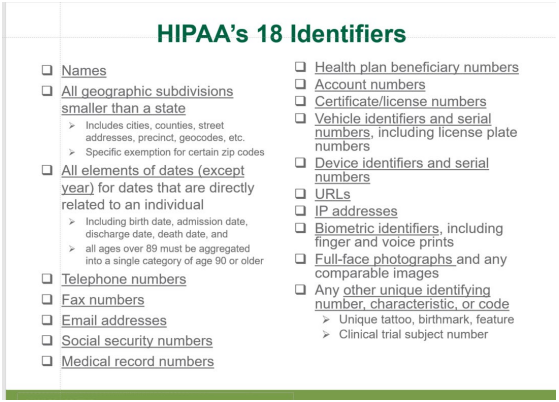
Under HIPAA, “de-identified” data sets do not contain PHI ***but*** must satisfy one of the HIPAA standards for de-identification.



HIPAA's Safe Harbor Provision

Remove All Identifiers

(for patient and relatives, employers, household members)



+

No actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Limited Data Sets (LDS)

- Data sets that only contain *indirect identifiers* (no direct identifiers)

- Can use or disclose LDSs for research purposes ***with*** Data Use Agreement (DUA) that meets HIPAA requirements

- Pros:
  - More data than de-identified data sets (e.g., dates)
  - Not human subjects research (so no need to get IRB approval)

- Cons:
  - Can't be used to link back to particular patients or to re-identify subjects

LDSs & DUAs: Requirements

LDSs **cannot** include direct identifiers:

- ❑ Names
- ❑ Postal address information, other than town or city, State, and zip code
- ❑ Telephone numbers
- ❑ Fax numbers
- ❑ Electronic mail addresses
- ❑ Social security numbers
- ❑ Medical record numbers
- ❑ Health plan beneficiary numbers
- ❑ Account numbers
- ❑ Certificate/license numbers
- ❑ Vehicle identifiers and serial numbers, including license plate numbers
- ❑ Device identifiers and serial numbers;
- ❑ URLs
- ❑ IP addresses
- ❑ Biometric identifiers, including finger and voice prints
- ❑ Full face photographic images and any comparable images.

Data use agreements **must** include:

- ❑ Permitted uses and disclosures of the data by the limited data set recipient.
- ❑ Define who may receive the data
- ❑ The data recipients will
  - ❑ Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law
  - ❑ Use appropriate safeguards to prevent improper use or disclosure of the
  - ❑ Report to the covered entity any inappropriate use or disclosure
  - ❑ Bind any of the recipients' agents who may get the data to the same restrictions and conditions that apply to the recipient
  - ❑ Not identify the information or contact the individuals

Fully Identifiable Data Sets

Data sets that contain direct identifiers

- ❑ Name
- ❑ MRN
- ❑ SSN (only in special circumstances)
- ❑ Addresses
- ❑ Email addresses
- ❑ Telephone numbers
- ❑ Vehicle ID numbers, driver's license numbers, etc.
- ❑ Medical device numbers
- ❑ Biometric information
- ❑ Etc.

**** Sets contain the **most sensitive data** so have the **strictest requirements** for disclosure****

Use of PHI for Research

Use of PHI for Research

- UVMHN may use and disclose PHI for the purposes of research

- Required documentation depends on the PHI being disclosed and the reason it is being sought.

- Research: "[A] a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."
  - Same definition of "research" as the Common Rule
  - Important to recognize difference between "QI" and "research" because the rules and documentation requirements differ

- Must satisfy one of the 6 permissible HIPAA "paths"

6 “Paths” for Use/Disclosure of PHI

- ❑ Authorization from the research participant/subject
- ❑ Waiver of HIPAA Authorization issued by IRB/Privacy Board
- ❑ PHI preparatory to research (PHI cannot be shared outside of UVMHN)
- ❑ Research on PHI belonging to decedents
- ❑ Limited data set (containing no direct identifiers) and compliant DUA with researcher(s)/data recipients
- ❑ De-identified Data Sets

Subject Authorization

- Similar requirements to the requirements for a standard HIPAA authorization
- May only use/disclose information identified in the consent/authorization
- May only use/disclose to researcher(s)/recipients identified in the consent/authorization
- Likely part of study consent/authorization documentation
- Approved by IRB

- **Must have authorization from subject before accessing PHI**
  - If accessing for identification of potential subjects, must have another HIPAA path

Subject Authorization
(example language)

What health information will be used and disclosed for this follow-up?
The health information we plan to collect is listed below.

- Medical history and examinations
- Your year of birth
- Estimated and actual date of delivery
- After the baby is born:
  - Your baby's birth weight and length
  - Your baby's sex
  - Whether there were any complications during the pregnancy or delivery
  - Whether your baby had any birth defects

Who is disclosing your health information for this follow-up?

- The University of Vermont Health Network
- Other doctors where medical care is sought during pregnancy and delivery

Who might use and give out information about you and your baby?

- The study doctor and the study staff.
- The sponsor of the study – Monopar Therapeutics Inc. "Sponsor" means any people and companies that
  - are working for the sponsor,
  - are working with the sponsor, or
  - are owned by the sponsor.

Your information might also be seen by:

- The U.S. Food and Drug Administration (FDA)
- Department of Health and Human Services (DHHS) agencies
- Governmental agencies in other countries
- The University of Vermont Health Network
- The University of Vermont and its Committees on Human Research

Your health information is protected by a federal law called the Health Information Portability and Accountability Act (HIPAA). Once your health information is shared outside of the University of Vermont Medical Center, we cannot guarantee that these laws will continue to apply. As a result, your health information could be further disclosed for other purposes. In the absence of a Certificate of Confidentiality, it is also possible for a court or other government official to order the release of study data. The confidentiality of your health information cannot be guaranteed if you agree it may be used in this study.

Waiver of HIPAA Authorization

- Must be issued by IRB or “Privacy Board.”
- Requirements for the waiver are set forth in HIPAA.
- **Can** be used to disclose full PHI.
- Document must contain a “brief description” of the data covered by the waiver.
  - May only disclose the data authorized by the waiver

Research – Waiver of HIPAA Authorization
(example language)

The UNIVERSITY of VERMONT
Committees on Human Subjects
Serving the University of Vermont
and the UVM Medical Center

RESEARCH PROTECTIONS OFFICE
213 Waterman Building
85 South Prospect Street
Burlington, Vermont 05405
(802)656-5040 ph
www.uvm.edu/rpo/

Waiver of HIPAA Authorization under 45 CFR 164.512(i)(2)(ii)

The issuing CHRMS board has determined, via expedited review conducted by the author of this certification and waiver, that the waiver satisfies the following criteria:

- The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
    1. An adequate plan to protect the identifiers from improper use and disclosure;
    2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    3. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;
- The research could not practicably be conducted without the waiver or alteration; and
- The research could not practicably be conducted without access to and use of the protected health information.

Brief Description of PHI under the Waiver

Constipation is a very common and potentially debilitating non-motor symptom of Parkinson disease, and there is no clear consensus on management. The goal of this project is to evaluate a cohort of patients with Parkinson disease who are treated by subspecialists at the UVMMC Movement Disorders clinic, to better understand the prevalence of constipation and approaches to management. We will also explore if involving a gastroenterology specialist affects the management of constipation in this patient population.

All protected health information (PHI) that will be accessed under the waiver (for example, specific tests, medical history, diagnosis)

- dx Parkinson disease
- Constipation
- Provider
- Patient name
- Patient DOB

- Patient MRN

- Patient sex

- Patient race

- Patient ethnicity

- Medication name and dose at most recent clinic visit; any use of medications to treat constipation from 2009 to present

- Gastroenterology evaluation: Notes from any gastroenterology evaluation 2009 to present- specifically assessment and plan / recommendations

- Past medical history: Any past medical history noted in the most recent clinic note, including diagnosis

- Past surgical history: Any past surgical history noted in the most recent clinic note, including surgery name and surgery location

- Allergies

- Procedures: Any gastrointestinal procedure, including endoscopy, colonoscopy - from 2009 to present - specifically for the indication of the procedure

- Symptom onset: Review in any clinic note from 2009 to present of the year of symptom onset

- Year of PD diagnosis: Review in any clinic note from 2009 to present of the year of PD diagnosis

- Imaging: Any brain imaging (MRI, CT, NM DAT SPECT, PET CT) from 2009 to present; any GI imaging (MRI, CT, X-ray) from 2009 to present

- Hospital admissions: Review any hospital admission from 2009 to present to see if constipation or Parkinson disease was an admission diagnosis, no dates will be recorded

- ED encounters: Review any ED visits from 2009 to present to see if constipation or Parkinson disease was an admission diagnosis, no dates will be recorded

Start and Stop Dates for the Collection Period(s) of Interest

1/1/2009 8/10/2021

Number of Records Needed for This Protocol

1343

Secondary Research with PHI
Exempt v. Expedited

- Waiver is required for secondary research using full data sets.

- Research is exempt from IRB review (under (4)(iii)) when "research involves only information collection and analysis involving the investigator's ***use*** of identifiable health information" regulated by HIPAA.
  - If PI is member of UVMHN workforce, then those reporting to PI are considered workforce too, so exempt review may be appropriate.
  - If data will be stored outside of UVMHN (e.g., LCOM servers, REDCap), the PHI will be disclosed and expedited review is required.
  - **Requests must still be submitted to the UVM Office of Research Protections for review and issuance of a waiver of HIPAA authorization.**

- Expedited review required if PHI will be ***disclosed*** (e.g., leave the covered entity).

Partial Waiver of HIPAA Authorization

- Issued for purposes of reviewing PHI to identify/recruit subjects

- Partial because it permits access to only the PHI needed to recruit, once subject is identified must get subject consent to continue to access, etc.

Preparatory To Research

- May use PHI in preparation for research
- Researcher must complete and submit form to UVMHN Compliance and Privacy Office
- Researcher must certify that:
  - The purpose is *solely* to prepare a research protocol (or for similar purposes);
  - The researcher will not remove the PHI from the covered entity;
  - The access is necessary for the research purpose.
- May only use this path for recruiting *if* the PI and members of the team are part of the covered entity
- Form may be found at: https://www.uvm.edu/rpo/uvmclick-irb-forms-library

Research on Decedents

- HIPAA protects a person's PHI for 50 years after the person dies.
- Researcher must complete form and submit to UVMHN Compliance and Privacy Office.
- Researcher must certify that
  - The use or disclosure is solely for the purpose of research on the PHI of the decedents;
  - The PHI being sought is necessary for the research; and
  - If requested by the covered entity, the researcher can provide documentation that the individuals whose information is being sought is deceased.
- Form may be found at: https://www.uvm.edu/rpo/uvmclick-irb-forms-library.

Limited and De-Identified Data Sets

- De-identified Data Sets: as long as they meet the HIPAA definition of “de-identified” the data sets are not protected by HIPAA and can be used for any purpose.

- Limited Data Sets: cannot contain direct identifiers; must be accompanied by DUA that meets HIPAA requirements.

Special Topics

Aggregate Data

- Most cases, aggregate data is **not PHI** (because it's not personally identifiable)
- Examples:
  - On March 13, 2022, the UVMMC ED treated 132 patients
  - On April 15, 2021, 15 COVID positive patients were admitted to the CVPH ICU
  - During Q1 2020, UVMMC diagnosed 347 patients as pre-diabetic
- Masking small numbers: don't provide small numbers (e.g., instead of saying "2 patients were treated for gunshot wounds in 2021" say "<11" or "fewer than 11.")
- Helpful way to provide information that is not PHI
- Need to use or disclose source data subject to HIPAA limitations, etc.

Coded v. De-Identified Data

- De-identified data: must meet specific HIPAA standards (18 identifiers + no knowledge of re-identification or expert determination)
- Coded data: Coded data is NOT the same thing as de-identified data.
- Study subject numbers cannot be included in de-identified data sets.
- Generally, permissible to use apply a unique identifier to mask individual patients provided the key is never provided to the recipients of the data (or otherwise disclosed). (Potentially used for LDSs and de-identified data sets)
- Unique identifiers cannot have any logical relation to patients (e.g., cannot be based on order of dates of service, include initials, include DOBs, etc.)

Data Storage

- Must consider where data are being stored (storage location may be a disclosure).
  - UVM REDCap: PHI stored on UVM/LCOM servers. Even if only UVMHN workforce using the data, still a disclosure because data are stored outside of the UVMHN walls (and can be accessed by non-UVMHN workforce)

- Data storage must be outlined on data management security plan
  - When DMO gets requests for data, they review data management security plan and look for who will be accessing data and where it will be stored.


Questions? Discussion?