Human Research and HIPAA: What You Think You Know and What You Should Know
Welcome & Introduction

Joshua Fedewa
Director, IRBMED

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Presenter/Office</th>
</tr>
</thead>
</table>
| 10:00 - 10:05 | Welcome & Introduction                                           | Joshua Fedewa, MS, CIP  
Director, IRBMED                                      |
| 10:05 - 10:25 | HIPAA – Protecting the Privacy of Research Subject’s Medical Records | Rebecca Hulea  
Director, Regulatory Compliance  
Michigan Medicine Compliance Office                        |
| 10:25 – 10:45 | IRBMED Review of HIPAA Authorizations and Waivers                | Beth Vibbart,  
Research Compliance Specialist Lead, IRBMED          |
| 10:45 – 11:05 | Secure Access to Patient Data with the DOCTR Office              | Devon Newman,  
Project Manager, Data Office for  
Clinical and Translational Research                  |
| 11:05 – 11:25 | Uses and Disclosures of PHI in Exempt and Not Regulated Projects | Allison Kanous, BS, CIP  
Research Compliance Specialist, IRBMED                |
| 11:25 – 11:45 | The HIPAA Privacy Rule and Research Involving Human Participants | Eric Ward,  
Assisting Managing Project  
Representative, Office of Research  
Sponsored Projects                                      |
| 11:45 – 12:00 | Seminar Q&A Session                                              | Ray-Nita Reynolds, MLIS, CIP  
Education Coordinator, IRBMED                          |
HIPAA - Protecting the privacy of research subjects’ medical records

Michigan Medicine Compliance Office
Rebecca Hulea, Director, Regulatory Compliance
Learning Objectives

- Understand data management principles with a law and policy mindset.
- Understand your role in complying with data management in daily research activities.
- Identify things that you can do to assure compliance with law and policy.
Health Care Privacy is Important to People

“Americans are increasingly concerned about the loss of privacy in every-day life, and especially about their health information.”

1 out of every 6 people engages in some form of privacy-protective behavior to shield themselves from the misuse of health information

- including **withholding** information
- **providing inaccurate** information
- **doctor-hopping** to avoid a consolidated medical record
- **paying out of pocket** for care that is covered by insurance
- And in the worst cases- **avoiding care altogether**

In the last two decades, a lack of privacy has led people to withdraw from full participation in their own health care because they are afraid that their most sensitive health records will fall into the wrong hands, leading to discrimination, loss of benefits, stigma, and unwanted exposure.

http://www.chcf.org/press/view.cfm?itemID=12267
Covered Entities are Required to have Appropriate Privacy and Security Controls

Largest Health Care Breach to date - As many as 80 million customers of the nation's second-largest health insurance company, Anthem Inc., have had their account information stolen. Anthem was the target of a very sophisticated external cyber-attack. Hackers gained access to Anthem's computer system and got information including names, birthdays, medical IDs, Social Security numbers, street addresses, e-mail addresses and employment information, including income data.
External Cyber-attacks are of Growing Concern

**Phishing**

Phishing for confidential information (name & passwords, credit card info, etc.

**Internet Threat**

Do NOT reply to any e-mail message that might be a phishing attempt.

Do NOT click on links or download files if you are not sure they are safe.

**What Do You Do?**

Report it
Contact IT Support for help

UM Safe Computing – Click [HERE](https://www.safecomputing.umich.edu/be-aware/phishing-and-suspicious-email/spear-phishing) to See Spear Phishing Video
Patient Permission is Needed to Use PHI in Research

Patient authorization (permission) is required for research when PHI is involved.

Exceptions to the rule:

• Waiver of the HIPAA authorization requirement (privacy board/IRB reviews)
• As a limited data set with a data use agreement
• Preparatory to research – requires “representation” that PHI being sought is necessary for the research purpose (e.g. study design, feasibility) and data does not leave the hospital (covered entity)
• Research on decedents – requires “representation” that use/disclosure is being sought solely for research of PHI of decedents and is necessary for the research.
Institutional Management and Oversight is Required

- UM IRB approval for project & data
- Patient permission for UMHS to disclose specified data
- IRB approved HIPAA Waiver of Authorization requirement
- Minimum necessary only
- De-identify to extent possible (stripped of all direct & indirect identifiers)
- Research justification for PHI
- Data Use Agreement is in place
- Data Use Plan is in place identifying how the study team will address data privacy & security protections through life cycle of project
HIPAA Considers Unaccounted for Disclosures as a Breach of Patient Privacy

**HIPAA BREACH IS PRESUMED**

requiring written notice:
- to patients
- to DHHS Office for Civil Rights (in all cases)
- to the media (in certain cases)

You Must Report
All actual or suspected violations!

UMHS Compliance Office
Will apply a 4-part test to overcome HIPAA breach presumption:

- Nature and extent of information involved, including the types of identifiers and risk of re-identification
- Unauthorized person who used the PHI or to whom it was disclosed
- Whether the PHI was actually acquired or viewed
- Extent to which risk to the PHI has been mitigated
Covered Entities Must Account for Research PHI Disclosures

Rule: an individual has a right to receive a listing, known as an accounting of disclosures, that provides information about when a HIPAA covered entity discloses the individual's information to others.

Exceptions to the “accounting” rule:
- PHI disclosed in the form of a limited data set (LDS = certain indirect identifiers)
- PHI disclosed under patients written consent (direct or indirect identifiers)

General Accounting Rules (research involving 50 + individuals)
- Date of disclosure
- Individual or entity receiving PHI
- Name/Description of protocol
- Description of data disclosed
- Recipient Contact information recipient
Data Use Agreements (DUAs) are Legally Binding Contracts

DUAs are required by law when sharing PHI.

DUAs give assurances that PHI disclosed for research will be appropriately protected by the data recipient.

DUAs address:
- Who may have access to data
- Describes purpose for sharing data
- Outlines Obligations of Data Recipient

DUAs are required by law when sharing PHI.

DUAs give assurances that PHI disclosed for research will be appropriately protected by the data recipient.

DUAs address:
- Who may have access to data
- Describes purpose for sharing data
- Outlines Obligations of Data Recipient
Where to Report Concerns

- Contact the Compliance Office
  
  Phone: 734-615-4400
  
  Email: Compliance-group@med.umich.edu
  
  Website: http://med.umich.edu/u/compliance/index.htm

- Hot Line or Web Form Submission (Anonymous):
  
  (866) 990-0111 or
  http://www.tnwinc.com/WebReport/
Compliance is a Partnership,  
Together We Make it Work.

Thank You!
IRBMED Review of HIPAA Authorizations and Waivers

Beth Vibbart, CIP

Research Compliance Specialist Lead, IRBMED
Every use and/or disclosure of PHI must satisfy the criteria under one of these provisions:

- A signed authorization from the individual
- A waiver of authorization approved by IRB MED (or, rarely, an external IRB or Privacy Board)
- A limited data set (LDS) shared under the terms of a written data use agreement
- Preparatory to research activities, such as assessing the feasibility of conducting a study
- Research involving the protected health information of decedents (deceased individuals)
- De-identified Data Sets (data will be completely deidentified before use for research purposes)
Privacy and Confidentiality

Common Rule and FDA Review

An IRB’s review of human subjects research must determine that, when appropriate, the research protocol includes "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data".

(45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7))

HIPAA Review

- An Authorization may be combined with the informed consent document for research. If the informed consent document is combined with an Authorization meeting the Privacy Rule's requirements, 45 CFR part 46 and/or 21 CFR parts 50 and 56 would require IRB review of the combined document.

- IRBs also have the authority to consider, and act upon, requests for a partial or complete waiver or alteration of the Privacy Rule’s Authorization requirement for the uses and disclosures of PHI for research.
“**Use** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information”.

“**Disclosure** means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information”.

*General Provisions: Definitions - Use - § 160.103*
Patient Consent vs. Authorization

**Patient Consent**

A covered entity *may* voluntarily obtain patient consent for uses and disclosures of PHI for treatment, payment, and health care operations.

---

**HIPAA Authorization**

Required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule.

A detailed document giving covered entities permission to use PHI for specified purposes, generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

*HIPAA FAQ 264 for Professionals*
HIPAA Authorizations for Research

**Must specify:**

- The number of elements, including a description of the protected health information to be used and disclosed
- The person authorized to make the use or disclosure
- The person to whom the covered entity may make the disclosure
- An expiration date, or an expiration event that relates to the individual or the purpose of the use or disclosure
- In some cases, the purpose for which the information may be used or disclosed.
A HIPAA Authorization for Research is included in the IRBMED standard informed consent template, and

- Biorepository consent templates
- One-time blood or specimen sample (minimal risk) informed consent template
- Survey research informed consent template
- Eligibility screening informed consent template

HIPAA Authorization is NOT included in the Exempt informed consent template or non-research consent templates (HUD, Expanded Access).
25-1.1 Identify the PHI to be used

Any PHI listed on the HIPAA authorization for research form must match the PHI indicated in 25-1.1.
25-1.2 Explain why the PHI is the minimum necessary to conduct the study

This response should explain why the study could not reasonably and effectively be conducted without the PHI.

**Examples:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>The PHI needed for this study is necessary to determine eligibility.</td>
</tr>
<tr>
<td>b)</td>
<td>The PHI is needed to meet the objectives of the study, monitor subjects for safety and properly identify the participants for study follow-up.</td>
</tr>
<tr>
<td>c)</td>
<td>Participant records, including mental health care records, alcohol/substance abuse treatment records, and AIDS/HIV, STD, and other communicable disease records are part of the subject's overall health, and these conditions could impact study participation. It is necessary that all data related to those conditions be available for review.</td>
</tr>
</tbody>
</table>

HHS.gov Minimum Necessary Requirement
25-1.3 Will HIPAA Authorization for access to the PHI be obtained from all or some subjects?

Select one:

- **Yes, always** - HIPAA authorization was/will be obtained from all subjects

- **Yes, sometimes** - HIPAA authorization will not be obtained from some subjects or from some candidates for recruitment before their records are reviewed for eligibility determination or to obtain contact information

- **No** - HIPAA authorization will not be obtained from any subjects
# Waivers of HIPAA Authorization

<table>
<thead>
<tr>
<th><strong>Full Waiver</strong></th>
<th><strong>Partial Waiver</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The waiver is for the entire project.</td>
<td>Survey portion</td>
</tr>
<tr>
<td></td>
<td>Recruitment portion</td>
</tr>
<tr>
<td></td>
<td>Specific subject group</td>
</tr>
<tr>
<td></td>
<td>Some other portion or aspect of the project (please specify)</td>
</tr>
</tbody>
</table>

The criteria that must be met for a waiver of HIPAA Authorization are the same for full and partial waivers.
Criteria for Waiver of Authorization

1. The use or disclosure of PHI involves no more than minimal risk to the privacy of individuals, based on AT LEAST the presence of the following three elements: (Qs. 25-2.2 – 25-2.4)

   a) An adequate plan to protect the identifiers from improper use and disclosure

   b) An adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law

   c) An adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted.

2. The research could not practicably be conducted without the waiver or alteration (Q. 25-2.5)

3. The research could not practicably be conducted without access to and use of the protected health information (Q. 25-2.6)

HHS.gov HIPAA For Professionals Privacy Guidance - Research
Elements of No More Than Minimal Risk Use and Disclosures

a) (Q. 25-2.2) Brief screening of medical records will only be performed by authorized representatives of the study team and will be kept strictly confidential under secure conditions.

b) (Q. 25-2.3) Recorded information will be destroyed immediately upon completion of the pre-screening process, unless the patient decides to participate in this research study, and signs the informed consent document, then the information may become part of the research record for purposes of this study.

c) (Q. 25-2.4) Recorded information will be destroyed immediately upon completion of the pre-screening process, unless the patient decides to participate in this research study, and signs the informed consent document, then the information may become part of the research record for purposes of this study.
Research Could Not Practicably Be Conducted Without The Waiver Or Alteration

(Q. 25-2.5)

• It would not be feasible to identify and contact hundreds of potential subjects for authorization to screen their medical record for study eligibility. The record review will not impact the care the patients would normally receive.

• Many of the patients potentially eligible for the study may have died.

• There is no regular contact with the patients potentially eligible for the study and the contact information available is likely not current.

• The inclusion of all records meeting the study criteria are necessary for statistical validity.

Examples:
Research Could Not Practically Be Conducted Without Access to and Use of PHI

(Q. 25-2.6)

• Access to PHI is necessary to identify the patients who meet the inclusion and exclusion criteria.

• Potential subjects could not be identified and approached by the study doctor unless PHI is accessible before screening to determine the likelihood of the patient's eligibility.

• The electronic medical record contains the information necessary to determine the subject's eligibility for clinical trial participation and would typically be more accurate than the individual’s personal recollection of their treatment history.
Unauthorized disclosures of PHI in research may be incidental or accidental.

**Incident** - A breach of confidentiality is necessary in order to comply with legal or ethical obligations, and the obligation was not noted in the informed consent document.

**Accident** – Participant PHI is sent in error to colleagues who are not authorized to receive it.

Unauthorized disclosures of PHI in research must be reported to IRBMED as an ORIO submitted through eResearch.

For known or suspected unauthorized disclosure of PHI related to research:

1. Take any practicable steps necessary to limit potential or ongoing harmful effects
2. Notify IRBMED as soon as possible
3. Promptly report the concern to the Corporate Compliance Office
Data Office for Clinical & Translational Research (DOCTR)
Data Office for Clinical & Translational Research

- Director: Erin Kaleba
- Project Manager: Devon Newman
- Data Protections Coordinator: Sheryl Flanagan
- Research Data Facilitator: Anisa Driscoll
- Data Analyst Team: Robinson Seda, Lynn Holevinski, Arina Bierdz, Hairong Geng, Johan Mosquera
- Nurse Informaticist: Lisa Day
- Training & Outreach Specialist: Arika Owens
The Data Office for Clinical & Translational Research is a unit of the University of Michigan Medical School Office of Research.

The Data Office enables researchers secure access to patient data through self-serve tools and custom data extracts.
Data Office Services

HOW WE SERVE YOUR DATA NEEDS

**Data Security, Privacy & Sharing**
Where can you safely store research data that still allows your team to use it? Read more about privacy guidelines and the latest on the campus-wide sharing policy.

**Data Access**
Get clinical, genetic or radiology data by using DataDirect® or one of our other self-serve tools. Too complicated? Also request a custom data extract from one of our experienced programmers.

**Training & Consultations**
Pull the right data for your project with individual or group training on our tools, DataDirect and EMERSE. Trainings are offered throughout the year.

- Data & Biospecimen Sharing
- Self-Serve Data Tools
- Upcoming Trainings
- Data Security & Privacy®
- Custom Data Request
- Research Data Needs
What are your data needs?

- Verify user credentials & requirements to determine if PHI is necessary
- Determine if data can be provided using DataDirect or a custom data request

<table>
<thead>
<tr>
<th>Custom Data Request</th>
<th>Data Direct</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Perform a regulatory review</td>
<td>• Access regulated based on IRB approval, PEERRS, Level 2, employment status</td>
</tr>
<tr>
<td>• Verify HIPAA compliant storage</td>
<td>• Verify HIPAA compliant storage</td>
</tr>
<tr>
<td>• Finalize data specifications</td>
<td>• Self serve</td>
</tr>
<tr>
<td>• Fee for service ($60/hour)</td>
<td>• No fee</td>
</tr>
</tbody>
</table>
DataDirect
Self-serve access to clinical data for research

Cohort Discovery (no IRB)

Pt-Level Data for Download (with IRB)

Aggregate Count
<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Data Element Examples</th>
<th>Earliest Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Demographics</td>
<td>Race, primary language, insurance, mortality, social history (smoking status, alcohol use)</td>
<td>2000</td>
</tr>
<tr>
<td>Encounters</td>
<td>Dates (admission, discharge, clinic visit), primary provider, location, BMI, Insurance</td>
<td>2000</td>
</tr>
<tr>
<td>Diagnoses</td>
<td>Billing and Problem Summary List</td>
<td>2000</td>
</tr>
<tr>
<td>Procedures</td>
<td>CPT and hospital ICD9/10 procedures</td>
<td>2000</td>
</tr>
<tr>
<td>Medications Ordered</td>
<td>Name, dose, frequency</td>
<td>2004</td>
</tr>
<tr>
<td>Medications Administered</td>
<td>Name, dose, frequency, route</td>
<td>2004</td>
</tr>
<tr>
<td>Labs</td>
<td>Test name, Order name, result</td>
<td>2004</td>
</tr>
<tr>
<td>Central Biorepository</td>
<td>Available samples for secondary use: Study name, tissue type, sample type</td>
<td>2014</td>
</tr>
</tbody>
</table>
When in Doubt – CONSULTATION

- **Regulatory (IRB) Expertise** – *what type of application do I need?*
- **Data Expertise** – *do you have tPA infusion rates?*
- **Compliance Expertise** – *can I store this on DropBox? Can an undergrad student access MiChart*
- **Technical Expertise** – *how many GPUs are available for my analyses?*
- **Data Sharing Expertise** – *can I share these data with Duke? With Industry?*
Data Sharing Services

<table>
<thead>
<tr>
<th>HIPAA REVIEW</th>
<th>DATA RELEASE COMMITTEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required when UM clinical data is leaving the institution</td>
<td>Required when sharing data with industry/commercial entities</td>
</tr>
<tr>
<td></td>
<td>*Clinical Trials are exempt</td>
</tr>
</tbody>
</table>
Researcher submits UFA for outgoing data → ORSP reviews UFA → Data Office performs HIPAA Review → ORSP (De-Identified data sharing) → Office of Tech Transfer (MTAs) → UM Compliance (Data sharing involving PHI)
What is involved with a HIPAA Review?

✓ Determine if the data to be shared is clinical or research data
  o Is the source of the data to be shared clinical or self-reported?
  o Is it a combination of both clinical and research data?

✓ Review the list of data variables to be shared and determine if it involves PHI or any sensitive data
  o Is there any clinical data that contains direct or indirect identifiers?

✓ Verify that IRB approval allows for this type of data sharing with the external entities
  o Is the external entity listed in IRB as a performance site?
  o Does the consent allow for data sharing?
  o Is there a HIPAA waiver in place if necessary?
  o Is 25-2.7 in the IRB app answered ‘YES’ if any PHI is being shared?
*Last slide provides a more in-depth overview of the HIPAA review process and decision making*
Sharing of Materials/Data with external collaborators

Determine data source:
- Research/ Clinical

Research Data Only:
- (patients consented): Data collected for purposes only for the study (e.g., surveys, interviews)
  - Route to ORSP

Clinical Data:
- Existing health record data collected originally for clinical purposes
  - Requires HIPPA Review

Combination of Research & Clinical:
- Requires HIPPA Review
  - Verify list of data elements to determine the sensitivity of the electronic medical record data being shared externally
  - Verify the type of data to be shared is consistent in IRB application
  - Provide agreement template and circulate for external signature

HIPPA Review:
- Not a De-Identified data set if the file include(s):
  - Dates – e.g., birthdates, Date of Admission/Service/Discharge, etc.
  - Age of patients greater than 89 years old
  - Any unique identifying number, characteristic, or code
  - If data to be shared is NOT de-identified data you must reflect this in section 25 of IRB application that PHI is to be shared externally (even if you are sharing a limited data set)

If data to be shared contains any identifiers (full PHI or Limited Data Set):
- Compliance provides Regent signature

If data to be shared is De-Identified:
- ORSP provides Regent signature

Materials Only

Office of Tech Transfer

If Materials & Data

Materials Only

Office of Tech Transfer
Uses and Disclosures of PHI in Exempt and Not Regulated Projects

Allison Kanous, CIP
Research Compliance Specialist, IRB MED
Every use and/or disclosure must satisfy the criteria under one of these provisions:

- A signed authorization from the individual
- A waiver of authorization approved by IRBMED (or, rarely, an external IRB or Privacy Board)
- A limited data set (LDS) shared under the terms of a written data use agreement
- Preparatory to research activities, such as assessing the feasibility of conducting a study
- Research involving the protected health information of decedents (deceased individuals)
- De-identified Data Sets
The HIPAA Privacy Rule protections apply to research use/disclosure of PHI, independent of other federal regulations on human subjects research (HSR).

For instance:

- Exempt human subjects research may require a waiver of HIPAA authorization, e.g.,
  - When using PHI to identify eligible subjects
  - When using PHI to create a research dataset,

- Activities not regulated as human subjects research that involve the use or disclosure of PHI are also regulated under HIPAA.

- Depending on the type of activity, HIPAA requirements may be satisfied by individual authorization, a waiver, or one of the other provisions.
Exempt Projects requiring *Limited IRB Review*

- **Limited IRB review** is a process that is required only for certain exemptions
  *Is not a HIPAA review.*
  
  o A review to ensure privacy/confidentiality protections are in place for exempt research that involves the collection of sensitive, identifiable data

- Exempt Projects that involve the recording of information such that the identity of the subjects can readily be ascertained either directly or through identifiers must have adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data,

<table>
<thead>
<tr>
<th>Exemption 2 – Surveys, Interviews, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exemption 3 – Benign Behavioral Intervention + Survey/Interview</td>
</tr>
</tbody>
</table>
Exempt Secondary Use 4(iii)

Secondary research for which consent is not required: Secondary research uses of identifiable private information or identifiable biospecimens, if at least one of the following criteria is met:

iii. The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR parts 160 and 164, subparts A and E, for the purposes of "health care operations" or "research" as those terms are defined at 45 CFR 164.501 or for "public health activities and purposes" as described under 45 CFR 164.512(b).

HIPAA is applicable and a HIPAA Authorization or a Waiver of Authorization would be required.
Activities ‘Not Regulated’ as HSR

- Quality Assurance/Quality Improvement
- Case Studies
- Standard Public Health Surveillance or Prevention Activities
- Certification Preparatory to Research
- Research involving only decedents
- Coded data or specimens
- De-identified data sets
Most QA/QI projects are eligible for a *Not Regulated* determination from IRBMED.

HIPAA requirements regarding patient privacy apply whether an activity is “research” or “quality improvement”.

- Projects limited to QA/QI activities involving PHI conducted for “health care operations” are subject to the Privacy Rule.
  - The privacy rule permits the use and disclosure of PHI for health care operations without requiring Authorization from the patient, or a Waiver of Authorization.
  - Any presentations or publications need to maintain the privacy of individual patients involved in the project.
Case Studies

- A report limited to **one or two individuals** identified in the course of clinical care.
- Publication of the case study is permissible.
- The case study must not include any FDA-regulated activities that require IRB approval such as:
  - test articles not been approved for use in humans;
  - test articles requiring exemption from FDA oversight;
  - test articles requiring an IND or IDE.

A **Case Series** is a chart review of 3 or more individuals and may be regulated as Human Subjects Research.

- It is preferable that HIPAA Authorization is obtained and imaged into the medical record.
- HIPAA does not apply if only HIPAA de-identified data is disclosed or shared outside the MM-covered entity via publication.
- If the write-up will include PHI, HIPAA Authorization is required. Journals may require authorization from the patients in order to publish.
Standard Public Health Surveillance or Prevention Activities

The collection and analysis of identifiable health data through public health efforts that primarily involve surveillance; prevention or control of known or suspected diseases, injuries, or other conditions; or to promote the health of a particular community.

HIPAA authorization or waiver is not needed if sending PHI to "a public health authority that is authorized by law to collect or receive such information".

164.512(b)(i)
Activities (e.g., review of medical data, queries, etc.) intended only to assess the feasibility of future research.

PHI may be used or disclosed without HIPAA authorization or waiver if the investigator affirms in eResearch:

- The use or disclosure is sought only to review PHI as necessary to assess the feasibility of future research, and
- No identifiers linking individuals to their PHI will be retained by the researcher after the feasibility review is complete.

The data collected cannot be used for a future research project. A HIPAA Authorization or waiver for recruitment/screening purposes must be obtained for any future research project using the PHI.
Research Involving Only Decedents

- Research involving only data or tissue obtained from individuals who are deceased prior to the conduct of the research.
- No interaction or intervention with living individuals and no collection of private data or specimens associated with living individuals.

To use or disclose the PHI of the deceased for research, there is no requirement to obtain Authorization from the personal representative or next of kin, a waiver or an alteration of the Authorization, or a data use agreement.

When these projects involve the use or disclosure of PHI, the researcher must affirm in eResearch that the PHI for which use or disclosure is sought is necessary for the research purposes, and if requested by any representative of Michigan Medicine, provide documentation of the death of each of the individuals whose information will be used for the project.

Michigan Medicine Tracking & Accounting of Disclosures of PHI Policy, 01-04-335
Research Involving Coded Data or Biological Specimens

Involves study data/specimens that are coded, and the researcher has no access to any code that links back to identifiers (e.g., an MRN, initials, or street address).

The HIPAA Privacy Rule protections apply if a coded or non-identifiable data set contains Protected Health Information (PHI) in the form of a “Limited Data Set.”

- A HIPAA Limited Data Set (LDS) excludes direct identifiers but may include geographic information other than street address; dates (including dates of service); and other numbers, characteristics, or codes not listed as direct identifiers.

- A table showing data elements permitted in de-identified data and limited data sets is available through the References section of the Compliance Office’s Michigan Medicine Policy 01-04-342 (level-2 login required)
De-identified Data Sets vs Limited Data Sets

<table>
<thead>
<tr>
<th>Data Element</th>
<th>De-Identified Data Set</th>
<th>Limited Data Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Address, city and other geographic information smaller than state. 3-digit zip code may be included in a de-identified data set for an area where more than 20,000 people live; use “000” if fewer than 20,000 people live there.</td>
<td>Remove</td>
<td>Remove postal address information other than city, town, state or zip code.</td>
</tr>
<tr>
<td>All elements of dates (except year); plus age and any date (including year) if age is over 89. Examples: date of birth, date of death, date of admission, date of discharge, date of service.</td>
<td>Remove</td>
<td>May be included.</td>
</tr>
<tr>
<td>Telephone, fax numbers; e-mail addresses, web URL addresses, IP addresses.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Social security number, medical record number, health plan beneficiary number, any account number, certificate or license number.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Vehicle identifiers and serial numbers, including license plate numbers.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Device identifiers and serial numbers.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Biometric identifiers (e.g., fingerprints; voice prints). DNA is not considered a biometric identifier for purposes of HIPAA.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Full-face photographs and any comparable images.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Any other unique identifying number, characteristic or code.</td>
<td>Remove*</td>
<td>Remove</td>
</tr>
</tbody>
</table>

Michigan Medicine
Limited Data Sets
Policy 01-04-342

De-Identified Data Sets and Limited Data Sets Chart
The Privacy Rule permits access to PHI in the form of a Limited Data Set (LDS) if the covered entity and the limited data set recipient enter into a data use agreement (DUA).

Even if the researchers requesting an LDS are members of the covered entity's workforce, a written data use agreement must be in place between the covered entity and the LDS recipient.

Michigan Medicine Compliance Policy 01-04-342 (level-2 login required) on Limited Data Sets describes the implementation of these requirements for internal and external sharing.

- Sharing an LDS within U-M, outside the MM Covered Entity: Use the internal template linked from the policy
  - “Responsible Data Use & Disclosure Attestation”
- Sharing an LDS outside U-M: Use the external template
  - Limited Data Use Agreement for External Use
Research involving a de-identified set (data/specimens) that cannot be "re-identified" by any known entity.

Research Involving De-identified Biological Specimens or Information

PHI excludes health information that is de-identified according to specific standards. De-identified health information can be used and disclosed by a covered entity, including a researcher, without Authorization or any other permission specified in the Privacy Rule.

1. De-identified by removal of all 18 elements, and no knowledge that the remaining information could be used alone or in combination with other information to identify the individual, OR

2. Certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable".

INSTUTIONAL REVIEW BOARD MEDICAL SCHOOL OFFICE OF RESEARCH
Referenced MM Web guidance:
Michigan Medicine Use of Protected Health Information (PHI) in Research Policy, 01-04-360,
Michigan Medicine Tracking & Accounting of Disclosures of PHI Policy, 01-04-335
Michigan Medicine De-identification and Re-identification of Protected Health Information (PHI) Policy, 01-04-340
Michigan Medicine Limited Data Sets Policy, 01-04-342

From IRBMED:
HIPAA
Protected Health Information (PHI)
Uses & Disclosures of Protected Health Information (PHI)
  Limited Data Sets - Research A to Z - University of Michigan
  De-identified Data Sets | Research A to Z
  Decedents - Research A to Z - University of Michigan
  Certification Preparatory to Research | Research A to Z
  Quality Assurance and Quality Improvement (QA/QI) Projects
Frequently Asked Questions (FAQ) - Office of Research

NIH’s guidance on PHI, de-identifying data sets, decedents, activities preparatory to research, LDS, etc.:
How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?
Data Use Agreements

15 November 2022

The HIPAA Privacy Rule and Research Involving Human Participants

Eric S. Ward  Assistant Managing Project Representative
Eric S. Ward

- Assistant Managing Project Representative for DUA team
- 4 years working at ORSP
- escottw@umich.edu
- (734) 764-4905
- Works 100% Remote (Cleveland area)
Office of Research and Sponsored projects

- Central Office located in Wolverine Tower (most work remote)
- A part of UMOR
- We support the research (funded and unfunded) at UofM (all campuses)

ORSP.UMICH.EDU
ORSP

PROJECT LIFECYCLE

- Find Funding
- Develop Proposal
- Route & Submit Proposal
- Set Up Project
- Manage Project
- Close Out Project

Research Ethics & Compliance
ORSP DUA Team

- Eric Ward (Asst. Manager)
- Michael Hudson (PR)
- Gabrielle Hammoud (APR)
- Michele Quick (APR)
1044

Average DUA (and amendments) processed per year
Do we need a DUA?
Start from the belief that you WILL need a DUA for the transfer or receipt of any/all data.
When is a DUA required?

- **MUST:**
  - Patient Medical Record PHI, LDS, De-IDentified Data*.
  - Research Data PII, Coded, Anonymized (individual level data)

- **May:**
  - Prefer to have contractual terms to cover use or other terms not required by law or policy

- **Not required:**
  - When data terms are covered in another agreement (MTA, clinical trial agreement, etc)
DUA Responsibilities

- ORSP DUA Team
  - Review UFA
  - Request clarification
  - Compliance concerns
  - Draft/Review DUA
  - Negotiate Agreements
  - Delegated signature authority
  - Consulting
  - Data Detective
DUA Responsibilities

- UofM Project Team
  - Initiate process
  - Create record in eRPM
  - Input information essential for ORSP to work on the project
  - Work with ORSP to finalize DUA
  - Understand their contractual responsibilities
  - Delete, destroy, or return data
  - Required submissions
    - IRBMED
    - Data and Biospecimen Release Committee
Resources to assist

ORSP has resources online to assist you with the creation of your project in eRPM
Understanding your project

- Is your project funded or unfunded?
- Is this DUA related to any other UFA or PAF?
- What direction is the data flowing: IN or OUT or BOTH?!
- Is your project a multisite project? Repository? Consortium?
- Is the data transfer contemplated in the HUM? Performance sites too?
Helping ORSP understand your project

Be as **specific** and clear as possible when completing UFA or PAF.

Leave lots of [BREADCRUMBS](#)
DUA essentials

- Sending or receiving *specific* DATA for a *specific* PURPOSE, and potentially for a **LIMITED TIME** and only to limited **RESEARCHERS**.
What should I name the UFA?

- If a **MULTISITE** project, with UofM acting as the **Data Control Center** (DCC) use the following;
  - “Project Name; Site Name” ex. “**STEPS; E. Michigan**”
  - Outgoing only!
- Same title as HUM is fine.
- Keep it simple yet accurate!
Description of the Data

- Where is the Data derived from?
  - **EMR**: PHI, LDS, De-identified
  - **Research Project**: PII, Coded, Anonymized
  - Other?

- The description of the Data should be succinct, clear, and note the source of the data
Bad description of the Data

“We are sending them data”
GOOD description of the Data

“We will be sending out de-identified data and MRI Images from patient medical records”
Description of the Purpose

- What will the Data be used for?
  - Analysis (be specific)
  - Research Project (specific part?)
  - Repository
  - Consortium

- The description of the Purpose is succinct, clear, and specific; especially when sending Data OUT.
BAD example of the Purpose

“They will analyze and publish the results of the data”
GOOD example of the Purpose

“The Data will be used for the purposes of the Friends Never Investigate Raspberries’ (FNIRs) project (HUM008675309)”
How are UFA/PAF for DUA processed

- UofM Project Team creates the UFA/PAF.
- Once approved by PI (sometimes the UNIT as well) it’s routed to ORSP for review.
  - DUA Team member is assigned the project and will review (initial review should occur within a few days).
How are UFA/PAF for DUA processed

- If **HIPAA data** is being sent out (any); routed for **HIPAA Review**
- If **HUM** not fully determined; Project will be returned to the Project Team
- ORSP Project Representative assigned to your project will reach out to the Research Administrator listed (possibly the PI as well) with any questions.
- If the Project is **Actionable**, the DUA will be **drafted** or **reviewed** and moved to “**Negotiations in Progress**”.
How are UFA/PAF for DUA processed

- Once **terms** of Agreement are **accepted by both entities**; ORSP will **sign** Agreement and route to PI for signature if needed.
- **Fully executed** Agreement will be entered into eRPM and the project will move to the state of **ACTIVE**.
- Data may be sent or received at this point.
Thank you!

Eric S. Ward
escottw@umich.edu
(734) 764-4905
Questions & Answers

U-M DOCTR Office Website: [https://research.medicine.umich.edu/our-units/data-office-clinical-translational-research](https://research.medicine.umich.edu/our-units/data-office-clinical-translational-research)