Welcome to our HIPAA & The IRB session

• If you are joining via Zoom please make sure your microphones are muted
• There will be a Q&A session after this presentation
  o Please reserve your questions until then
    OR
  o Put any/all questions in the chat and we will address them after the presentation
• This session may be recorded
• Not registered? Please register now using the QR code.
HIPAA & The IRB
Understanding HIPAA and IRB Requirements

Jessica Ordax, MA, CIP, Sr. IRB Analyst, Human Research Protections
Lindsay Ropchock, JD, CIP, IRB Analyst, Human Research Protections
Christy O’Connor, Privacy Director, Compliance and Privacy Office

January 11, 2024
https://hrp.weill.cornell.edu/irb
Jessica Ordax, MA, CIP

8+ years of experience in human subjects research regulatory compliance.

My Masters is in Bioethics and Science Policy with a focus on the process of Informed Consent within the research context.

Joined WCM in March of 2022
Lindsay Ropchock, JD, CIP

5+ years in human subjects research regulatory compliance.

Former course director on medical ethics.

10+ years experience as an attorney.

Joined WCM in December of 2021
Christy O'Connor, BA, CIPP/US, CHC

- 15+ years of experience in health care privacy and compliance (hospital, physician, and health plan background)
- Certified as an Information Privacy Professional (CIPP/US) and in Health Care Compliance (CHC).
- Rejoined WCM in January 2022
Sarah Leon, BA, CIP

15+ years of experience in human research protections

Joined WCM in March of 2020
Yaritza Saavedra, BA, CIP

13+ years of experience in human research protections

Joined WCM in 2010
Rajvi Parmar

10+ years of experience in human research protections

Joined WCM in 2022
Lauren Odynocki

15+ years of experience in human research protections.

Joined WCM in 2007.
Today’s Topics

- Background: PHI, HIPAA & the IRB
- Obtaining Permissions

*Adapted from METS: Data Security in Research: PHI, Email, HIPAA, and You*
Background: PHI, HIPAA & the IRB
HIPAA (1996)

The three (3) main rules of HIPAA

- The Privacy Rule
- The Security Rule
- The Breach Notification Rule
The Privacy Rule

Defines the circumstances under which a person may disclose or use PHI. Everyone has a right to privacy, but as we all know, there are some situations in which the rule might be applied. Those who are covered by this policy must adhere to a set of rules.

The standards set by the privacy rule address subjects such as:

- Which organizations must follow the HIPAA standards
- What is protected health information (PHI)
- How organizations can share and use PHI
- Permitted usage and disclosure of PHI
- Patient’s rights over their health information
HIPAA Privacy Rule

Access

The right of individuals to request and obtain PHI from covered entities.

Use

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.

Disclose

The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.
What is a covered entity?

(1) Health plans

(2) Health care clearinghouses

(3) Health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards (i.e., billing and payment; insurance)
The Security Rule

The HIPAA Security Rule sets out the minimum standards for protecting electronic health information (ePHI).

- Types of Safeguards
  - Technical
  - Administrative
  - Physical
- Ensures the confidentiality, integrity, and availability of the PHI
- Protect against improper uses and disclosures of data
- Protects the ePHI against potential threats
- Trains employees so that they are aware of the compliance factors of the security rule
- Adapts the policies and procedures to meet the updated security rule
HIPAA Security Rule

Administrative Safeguards
- Policies & Procedures
- Training

Technical Safeguards
- Email/Data Encryption
- Authentication

Physical Safeguards
- Secure Rooms
- Workstation Security
Safeguard PHI and WCM Data

• Lock doors & file cabinets, and limit access to workspace where health information is used or stored
• Limit access to:
  o Printers and faxes where health information is printed
  o Health information to only those who need it for a specific task
• Shred/properly dispose of health information once retention is no longer required
• Encrypt emails to external recipients containing PHI by using #encrypt
• Utilize Adobe’s redaction feature for documents with PHI before sending
• Use Microsoft OneDrive for storing and appropriately sharing high risk research data (PHI/PII)
• For WCM work, use only WCM encrypted devices
• Use your WCM email address for correspondence and don’t use email rules to forward emails outside of WCM
• Take privacy and security refresher trainings
The Breach Notification Rule

Breach

- Compromised PHI
- Notification
- Fines
PHI (Protected Health Information)

Health information created, used, or disclosed by a covered entity

Pertaining to an individual’s past, present, or future:
- Physical or mental health
- Diagnosis and/or treatment
- Payment for health care
PHI = Individual Identifier + Health Information

1. Patient names
2. Geographical elements
3. Dates
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers
13. Device identifiers
14. URLs
15. IP Addresses
16. Biometric identifiers
17. Facial images
18. Any other unique identifiers

• Clinical data/Diagnosis data
• Patient’s health care provider
• Patient’s health care provider for sensitive conditions
• Patient’s location in facility
• Personal Health Condition or History
• Pregnancy
• Prescription drug usage or usage history
• Addiction
• Behavioral Health Information or History
• Family Health Condition or History
• Health Insurance Application, Claims History, or Appeals Records
• Interest in clinical trial research
## PHI Formats and Potential Privacy Incidents

<table>
<thead>
<tr>
<th>Electronic (ePHI)</th>
<th>Paper/Fax/Specimen</th>
</tr>
</thead>
<tbody>
<tr>
<td>A lost or stolen laptop or portable media device containing WCM data (encrypted and non-encrypted)</td>
<td>Health or research records sent to the wrong address</td>
</tr>
<tr>
<td>Patient or subject information being texted or emailed to the wrong external recipient</td>
<td>The wrong patient or subject label attached to a specimen</td>
</tr>
<tr>
<td>Using unauthorized platforms to communicate or exchange PHI</td>
<td>Bloodwork or specimens taken from an unlocked laboratory specimen box or room</td>
</tr>
<tr>
<td>2 or more WCM employees sharing a password</td>
<td></td>
</tr>
<tr>
<td>Patient or subject's data posted to, or leaked to, social media</td>
<td></td>
</tr>
<tr>
<td>Suspicious emails requesting your password or personal information to update your account.</td>
<td></td>
</tr>
</tbody>
</table>

### Oral

- Clinicians or research staff discussing a patient’s care in an elevator
- PHI verbally shared with another person who has no need to know (gossip)
- Any WCM staff discussing a patient’s or subject's case over dinner with friends
## PHI Formats and Potential Privacy Incidents

<table>
<thead>
<tr>
<th>Electronic (ePHI)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A lost or stolen laptop/portable media device containing WCM data (encrypted or not)</td>
<td>Suspicious emails requesting your password or personal information to update your account.</td>
</tr>
<tr>
<td>Patient or subject information being texted or emailed to the wrong external recipient</td>
<td>Patient or subject's data posted to, or leaked to, social media</td>
</tr>
<tr>
<td>Using unauthorized platforms to communicate or exchange PHI</td>
<td>2 or more WCM employees sharing a password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper/Fax/Specimen</th>
<th>Oral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health or research records sent to the wrong address</td>
<td>Clinicians or research staff discussing a patient’s care in an elevator</td>
</tr>
<tr>
<td>The wrong patient or subject label attached to a specimen</td>
<td>PHI verbally shared with another person who has no need to know (gossip)</td>
</tr>
<tr>
<td>Bloodwork or specimens taken from an unlocked laboratory specimen box or room.</td>
<td>Any WCM staff discussing a patient’s or subject’s case over dinner with friends</td>
</tr>
</tbody>
</table>
WCM's IRB Privacy Board and Privacy Office

**Privacy Office**
The Privacy Office is responsible for ensuring WCM's compliance with the HIPAA Rule and other federal, state, and international privacy requirements. The Privacy Office investigates all potential allegations of unauthorized use, access or disclosure of PHI, including IRB Reportable events involving HIPAA compliance. The Privacy Office is responsible for conducting Institutional risk assessments and reporting breaches to the Office of Civil Rights (OCR) and other regulators.

**IRB Privacy Board**
The Privacy Board is part of WCM's IRB and is a review body that is established to act upon requests for a waiver or an alteration of the Authorization requirement under the Privacy Rule for uses and disclosures of PHI for a particular research study. At WCM there is a Privacy Board constituted as part of the IRB.
WCM's Privacy Office

Effective Privacy Compliance Program

Wait...there is more to Privacy

- Incident Management
- Privacy Agreements & Vendor Management
- Research Data Privacy
- Tripartite Collaborations (i.e., NYP and Columbia)
- Notice of Privacy Practices (NPP) & Individual Rights
- Release of Information (ROI) and Access to PHI

IRB Incidents
Informed Consent
Research Study Protocol
Data flow
DUAs
DHI – mobile apps; wearables

Vendors, including AI

Research Data Privacy

Chief Privacy Officer & ISPAC
WCM Policies and Procedures
WCM Education and Training
Effective Lines of Communication
Internal Audit & Monitoring
Mitigation/CAPs

Enforcement through publicized disciplinary standards
Privacy Board and the IRB

• When access, use, or disclosure of PHI is Human Subjects Research, then and only then does the IRB serve as the Privacy Board.
• In order for the IRB to address its Privacy Board responsibilities the required HIPAA Authorization Language is embedded into all the consent form templates.
• In our capacity as a Privacy Board we are also authorized to grant HIPAA Authorization Waivers.
When does HIPAA apply?

- HIPAA permits covered entities to use and disclose PHI for research purposes under certain conditions.
  - Researchers must obtain either individual authorization from the subjects or a waiver of authorization from the IRB, if certain criteria are met.
- HIPAA requires that researchers obtain approval from an IRB before using or disclosing PHI for research purposes.
- The IRB ensures that the research protocol meets ethical standards and provides adequate privacy protections.
Adhere to HIPAA’s “Minimum necessary” standard

*Minimum Necessary:* Accessing, using or disclosing the least amount of patient data that is required for your WCM duties; only what you “need to know” for your role.

**EXAMPLES:**

Data exchange: Sharing only the minimum amount of information needed to accomplish an authorized task

Role-Based Access: System access that is based on a user’s role at WCM
Use strong computer passwords and do not share them
Obtaining Permissions

What avenues permit PHI to be accessed for research purposes?
Avenues To PHI Access for Research

1. Prospective HIPAA Authorization from Research Participants
2. HIPAA for Decedents
3. Alteration, Complete, or Partial Waiver of HIPAA Authorization
# Prospective HIPAA Authorization from Research Participants

<table>
<thead>
<tr>
<th>What is it?</th>
<th>• Written permission from an individual (either by standalone authorization or incorporated into the informed consent form) that allows a covered entity to use or disclose PHI for research purposes.</th>
</tr>
</thead>
</table>
| When is it required?                                                        | • When the requirements of a HIPAA waiver or alteration don’t apply  
• When obtaining written documentation of informed consent. |
| How is it obtained?                                                         | • With your initial application within WRG-HS, upload the appropriate WCM IRB Research Consent template. |

Continued on next slide
Prospective HIPAA Authorization from Research Participants

What are the elements?

• The core elements of a valid authorization include:

  • A meaningful description of the information to be disclosed
  • The name of the individual or the name of the person authorized to make the requested disclosure
  • The name or other identification of the recipient of the information
  • A description of each purpose of the disclosure (the statement "at the request of the individual" is sufficient when the individual initiates the authorization and does not, or elects not to, provide a statement of the purpose)
  • An expiration date or an expiration event that relates to the individual
  • A signature of the individual or their personal representative (someone authorized to make health care decisions on behalf of the individual) and the date.

Note: A copy of the signed HIPAA Authorization must be provided to the research participant and the researcher must retain the original.

HIPAA Authorization for Use and Disclosure of Your Protected Health Information

As part of this study, we will be collecting health information about you and sharing it with others. This information is "protected" because it identifies you.

Protected Health Information (PHI)

By signing this Consent Document, you are allowing the following people to use or release your protected health information for this study: [list all people or class of people (i.e. researchers and their staff) that will access PHI or you can also create a document to give participants that list these people].

This information may include: [list PHI, e.g. results of physical exams, medical history, body mass index, sensitive diagnoses if applicable, etc.]. We will use this information to: [include the purpose and describe each use of the requested information]. The researcher may use with and/or release the health information listed above to: [name or class of persons involved].

In addition to the people listed in this form, there is a chance that your health information may be shared outside of the research study and no longer be protected by federal privacy laws. Examples of this include releases to law enforcement, legal proceedings, health oversight activities and public health measures.

Right to Withdraw Your Authorization

Your permission for the use and disclosure of your health information for this project shall not expire unless you cancel it. Your health information will be used or disclosed as long as it is needed for this project. However, you may stop your permission at any time by notifying the WCM Privacy Office in writing. To do this, please send a letter to:

  Privacy Office
  1300 York Avenue, Box 303
  New York, NY 10065
  Email: privacy@med.cornell.edu

If you have questions about this and would like to discuss them, please call (646) 962-6930. Please note that the research team does not have to destroy or retrieve any of your health information that has already been used or shared before your withdrawal is received.

If you have questions about the privacy practices of the institution, you can request a Notice of Privacy Practices from your provider.
HIPAA for Decedents

The Privacy Rule also provides protection to deceased individuals for up to 50 years following death. To use decedents’ PHI for research purposes, a researcher must provide all of the following:

- Representation that the use or disclosure is solely for research involving the PHI of decedents (e.g., and not also the living relatives of decedents)
- Representation that the PHI is necessary for the research
- Documentation (at the request of the covered entity holding the PHI) of the death of the individuals whose PHI is sought
### Waivers of HIPAA Authorization

<table>
<thead>
<tr>
<th>What are they?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A waiver is a request to forgo the HIPAA authorization requirement based on</td>
</tr>
<tr>
<td>the fact that the disclosure of PHI involves minimal risk to the participant</td>
</tr>
<tr>
<td>and the research cannot practically be done without access to/use of PHI.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When is it required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When de-identification is not possible and obtaining HIPAA authorization</td>
</tr>
<tr>
<td>presents challenges.</td>
</tr>
<tr>
<td>• <strong>Full Waiver:</strong> This is a request to waive the HIPAA authorization</td>
</tr>
<tr>
<td>requirements for the conduct of the entire study. Typically used to</td>
</tr>
<tr>
<td>conduct records research (retrospective chart review).</td>
</tr>
<tr>
<td>• <strong>Partial Waiver:</strong> This is a request to waive the HIPAA authorization</td>
</tr>
<tr>
<td>requirements just for the screening and ascertainment portion of the</td>
</tr>
<tr>
<td>study.</td>
</tr>
<tr>
<td>• <strong>Alteration:</strong> This is a request to waive any of the elements of HIPAA</td>
</tr>
<tr>
<td>authorization. These are not typical at WCM—but may occur with studies</td>
</tr>
<tr>
<td>that involve deception.</td>
</tr>
</tbody>
</table>

Continued on next slide
## Waiver or Alteration of HIPAA Authorization Criteria

<table>
<thead>
<tr>
<th>How are they obtained?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Use/disclosure of PHI involves no more than a minimal risk to the privacy of individuals:</td>
</tr>
<tr>
<td>• An adequate plan to protect the identifiers from improper use and disclosure;</td>
</tr>
<tr>
<td>• 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</td>
</tr>
<tr>
<td>• 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;</td>
</tr>
<tr>
<td><strong>2.</strong> The research could not practicably be conducted without the waiver or alteration; <strong>AND</strong></td>
</tr>
<tr>
<td><strong>3.</strong> The research could not practicably be conducted without access to and use of the protected health information.</td>
</tr>
</tbody>
</table>
Criteria and Examples

**Criterion:** A.1) An adequate plan to protect the identifiers from improper use and disclosure;

**Example Language: Partial HIPAA Waiver (Recruitment/Screening) and Full HIPAA Waiver**

To protect PHI from improper use and disclosure, each participant will be given a randomly generated 3-digit code at the start of the study. Only listed study team investigators will have access to the original key code, which will be kept on a separate, password-protected file, stored on a secure NYP-WCM computer, in a locked office.
Criteria and Examples

**Criterion:** A.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

---

**Example Language: Partial HIPAA Waiver (Recruitment/Screening)**

For all patients who do not choose to participate in the study or who do not qualify, all identifiers and PHI will be destroyed and removed from all study records immediately.

---

**Example Language: Full HIPAA Waiver**

All materials containing subject identifiers will be discarded and shredded *two years after data analysis is completed*. Analysis is scheduled to be completed 1 year after study is closed to enrollment.
Criteria and Examples

Criterion: A.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;

Example Language: Partial HIPAA Waiver (Recruitment/Screening) and Full HIPAA Waiver

There will be no protected health information disclosed to individuals other than IRB approved investigators who have completed required institutional training. 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.
Criteria and Examples

Criterion: B) The research could not practicably be conducted **without the waiver or alteration**; and

**Example Language: Partial HIPAA Waiver (Recruitment/Screening)**

Access to PHI via a waiver is required to spare ineligible subjects from unnecessary contact.
Moreover, contacting all potential patients, including those who may not meet eligibility, presents a large burden to the research team.

**Example Language: Full HIPAA Waiver**

The research team no longer has access to this subject population.
All of these patients are lost to follow-up and there is no available updated contact information.
**Criteria and Examples**

**Criterion:** C) The research could not practicably be conducted without access to and use of the protected health information.

**Example Language: Partial HIPAA Waiver (Recruitment/Screening)**

Due to the nature of the eligibility criteria many patients will not qualify. Contacting such patients could cause them anxiety regarding their condition. Risks such as these can be mitigated by only reaching out to subjects who qualify based on inclusion criteria.

**Example Language: Full HIPAA Waiver**

Study team will not be able to conduct this retrospective chart review without access to the PHI as these data points are necessary for the proposed analysis.
Helpful Resources

- **Monthly Education and Training Series:**
  - [https://hrp.weill.cornell.edu/educational-resources/monthly-education-training-series-mets](https://hrp.weill.cornell.edu/educational-resources/monthly-education-training-series-mets)

- **NIH resource:**
  - [HIPAA Privacy Rule and Its Impacts on Research](https://nih.gov)

- **DHHS "Summary of the HIPAA Privacy Rule"**
  - [https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)

- **DHHS Frequently Asked Questions regarding HIPAA Authorization:**
  - Authorizations | HHS.gov
Questions?

For IRB assistance email: irb@med.cornell.edu

For Compliance & Privacy Office assistance email: privacy@med.cornell.edu
Contact Us

Scan the QR code to request a consult during our on-site Tuesday, 1/9 through Thursday 1/11

Weill Cornell Medicine Human Research Protections
575 Lexington Avenue
New York, NY 10022
Phone: (646) 962-8200
irb@med.cornell.edu