Ensuring Confidentiality with Data Sharing
Objectives

• To describe Protected Health Information (PHI)/Private Identifiable Information (PII)
• Discuss the importance of protecting PHI/PII
• Describe ways to properly share PHI/PII
What is PHI/PII?

Ellie Mendiola, CPC
Office of Regulatory Affairs and Compliance

**SEE HIPAA AND HIPAA COMPLIANCE WITH PHI/PII IN RESEARCH PRESENTATION**
## HIPAA Violation Penalties

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know that he/she violated HIPAA and by exercising reasonable diligence, would not have known.</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations. Note: This is the maximum penalty that can be imposed by the State Attorney General regardless of the violation.</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million.</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect.</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations.</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million.</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period.</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations.</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million.</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect and is not corrected.</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million.</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million.</td>
</tr>
</tbody>
</table>
Importance of protecting PHI/PII: An IRB perspective
Belmont Report Principles

• **Respect for persons**
  • Research participants should be treated as autonomous agents with the ability to exercise their autonomy, including the right to privacy and the right to have their private information remain confidential.

• **Beneficence**
  • Maintaining privacy and confidentiality helps to protect research participants from potential harms including psychological harm such as embarrassment or distress; social harms such as loss of employment or damage to one’s financial standing; and criminal or civil liability.
The Institutional Core Facilities are resources of the Office of the Vice President for Research

Regulation Requirements

- Department of Health and Human Services (DHHS), 45 CFR 46.111(a) (7)
- Food and Drug Administration (FDA) 21 CFR 56.111(a)(7)

- The IRB must ensure “there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.”
How to properly share PHI/PII.

A case-study approach
Scenario 1

A PI who recorded and stored research data in REDCap leaves the institution without transferring or closing an IRB approved study with the intention of keeping the study open as sub-investigators are continuing to work on the study and there are plans for the investigator to continue working on the study at the new location—an unapproved location. While at the new location, the PI requests access to REDCap to obtain a copy of the research data. A REDCap account is created. An IRB approved research team member from UTHSA grants the investigator access to all data, including PHI/PII.
Issues Identified in Scenario 1

• PI left institution without transferring the study to a new PI
• Access was granted to the RedCap data
• A potential disclosure was made outside of the covered entity
• The institution recipient does not have IRB approval to be engaged in research.
Preventative Actions for Scenario 1

• Ensure Investigators follow institutional policies for leaving the institution
• Ensure the IRB approved application includes plan for data sharing data
• Determine whether permission to share is required
  • Signed HIPAA Authorization
  • Data Use Agreement (DUA)
Studies with HIPAA Authorization

HIPAA Authorization* → De-Identified Data → Should list entity in the HIPAA Authorization
HIPAA Authorization* → Limited Data Set
HIPAA Authorization* → Identifiable Data → Must list entity in HIPAA Authorization

* HIPAA Authorization may be a combo Consent/Authorization or a Stand-Alone Authorization
Studies with Waived HIPPA Authorization

Waived HIPAA Authorization

- De-Identified Data
  - No DUA
  - Disclosure tracking is not required

- Limited Data Set
  - Must have DUA
  - Disclosure tracking is required

- Identifiable Data*
  - Sharing identifiable data under a Waiver is uncommon. Research should aim to use the minimum necessary

*Sharing identifiable data under a Waiver is uncommon. Research should aim to use the minimum necessary
The Institutional Core Facilities are resources of the Office of the Vice President for Research

### REDCap

- Allows for data to be stored in the tool (including the key)
- Project managers may grant access to the data based on the individual’s level of engagement in the protocol
- Will need to ensure access is updated as changes to study personnel occurs
- Compliance audits will now include the review of REDCap tools
Scenario 2

The IRB approved application notes that participant study eligibility confirmation will be shared with the Sponsor; however, will be shared in a de-identified fashion. A study coordinator sends an email to a Sponsor confirming study participant eligibility. The email contains an un-redacted Enrollment Note, X-Ray results, and CBC Results. Unbeknownst to the coordinator, the X-Ray and CBC Results belong to another subject who was determined to be ineligible. The email was sent using “+++” to ensure encryption. The Sponsor is listed as an entity which may receive PHI/PII.
Scenario 2

The Institutional Core Facilities are resources of the Office of the Vice President for Research.
Issues Identified in Scenario 2

• Identifiable data was sent to the Sponsor
• The X-ray and CBC Results belonged to another participant
Preventative Actions for Scenario 2

• Use sponsor's Case Report Forms (CRF) or electronic CRFs
• Upload only necessary data
• Ensure PHI/PII is redacted
• If emails must be used, create checklist study team members may utilize to draft sponsor correspondence
  • Consider creating an email template and include color coding that may help study team members remember requirements
Preventative Actions for Scenario 2

Dear Sponsor,

The subject identified below met study inclusion criteria. Please continue with randomization.

<table>
<thead>
<tr>
<th>Subject ID</th>
<th>Date of Eligibility Confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Inclusion

<table>
<thead>
<tr>
<th>Inclusion</th>
<th>Inclusion Criteria Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Lab Value A</td>
<td>Yes – Lab Value A:</td>
</tr>
<tr>
<td>2. Lab Value B</td>
<td>Yes – Lab Value B:</td>
</tr>
</tbody>
</table>

### Exclusion

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Exclusion Criteria Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Exclusion Criteria A</td>
<td>No, as evidenced by:</td>
</tr>
<tr>
<td>2. Exclusion Criteria B</td>
<td>No, as evidenced by:</td>
</tr>
</tbody>
</table>

Eligibility Confirmed by:
Scenario 3

An IRB approved protocol in which the IRB approved a waiver of consent and a HIPAA Waiver for a chart review study includes a plan to store collected data on a secure HSC server; however data will be stored separate from the key to coded data. In addition, the approved protocol states that de-identified data will be shared with a collaborator from another research site. A sub-investigator who is planning to share the research data with the collaborator at another entity makes a copy of the data and places on a personal laptop, from the secure HSC folder, which unbeknownst to the sub-investigator includes PHI/PII. While meeting the collaborator, the data is transmitted via personal email account to the collaborator. The sub-investigator goes home for the evening and forgets the laptop in the front seat of the car. Upon return, finds that the laptop is missing from the car. The sub-investigator reports a stolen laptop to the PI. Upon further explanation, it is learned that the laptop was a personal laptop and did not require a password once the computer is turned on.
Issues with Scenario 3

• Data was stored with PHI/PII
• Data was copied included PHI/PII instead of de-identified data
• Data was placed on a unencrypted laptop
• PHI/PII was shared with a collaborator
Preventative Actions for Scenario 3

- Storing data in a coded fashion in a shared drive – separate from key to code
- If using RedCap, data will be stored together; however, permissions and export functionality can be set to limit what may be seen or downloaded
- Use of secure emails
- Double checking data to ensure correct data is being sent and that data is sent consistent with approved method
- Encrypting personal laptops/use of Virtual Private Network (VPN)
Summary

- PHI/PII is individually identifiable health information/protected identifiable information
- Important to protect PHI/PII
  - Violation of federal laws, institutional policies and possible IRB noncompliance
- Developing tools to aid in the appropriate sharing of data
  - Sponsor CRFs/eCRFs
  - REDCap
  - Email templates