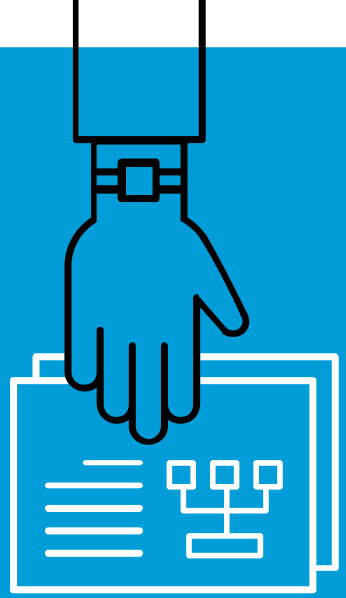
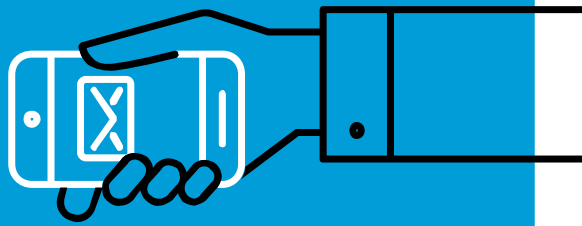
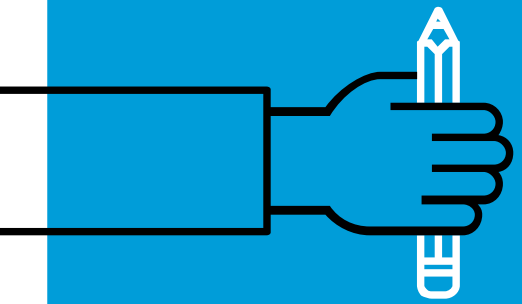
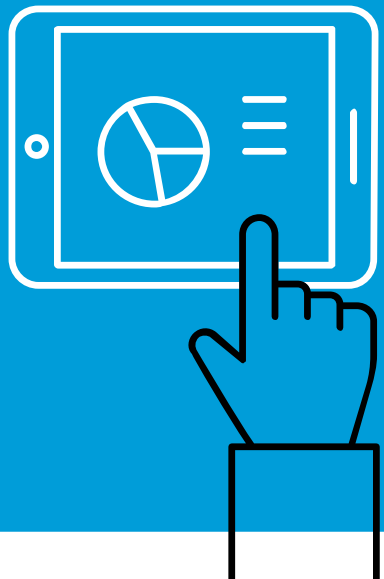




Research with Protected Health Information

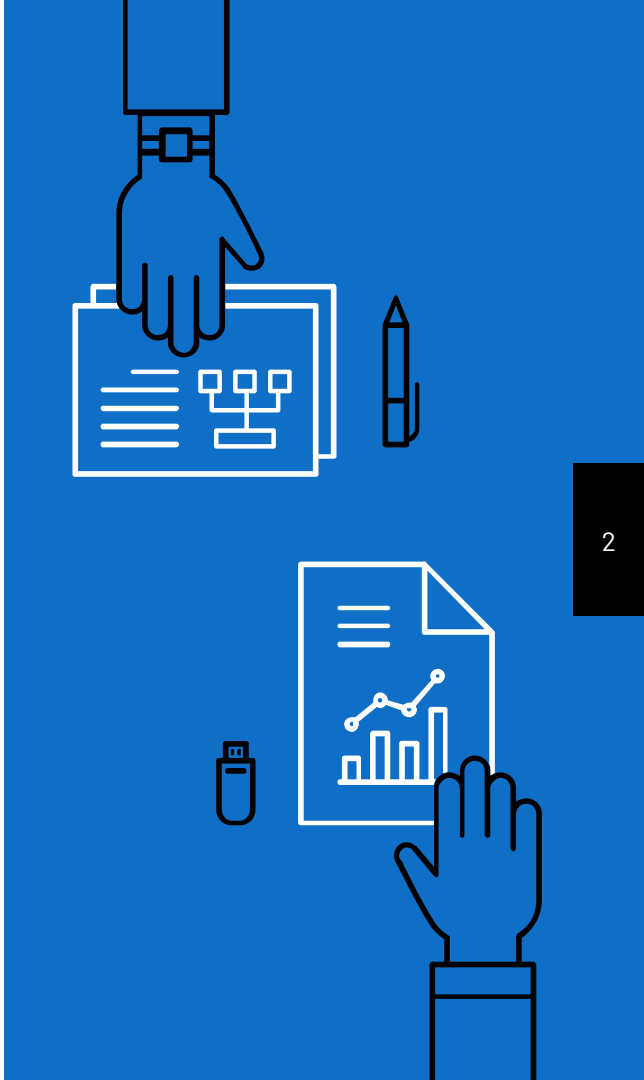
HIPAA and Associated Topics



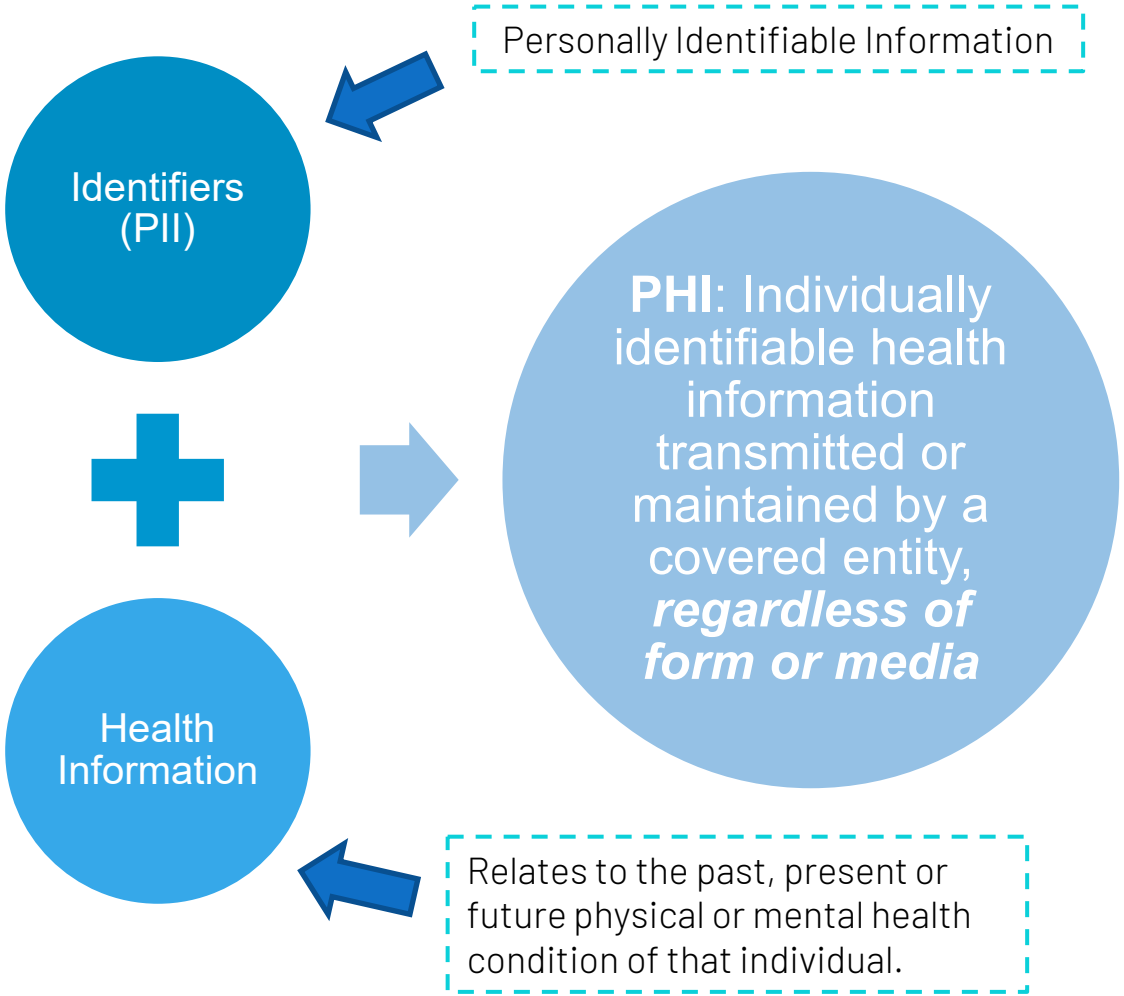


AGENDA

- HIPAA and Data Related Definitions
- Requirements for HIPAA in Research
  - Research with identifiable data
    - Authorization
    - Waiver
  - Research with limited data
  - Research with anonymous / de-identified data
- Special Topics
  - Preparatory to Research
  - Other Regulations & Institutional Policies
- Reporting Incidents and Breaches
- Resources



PROTECTED HEALTH INFORMATION



PHI IDENTIFIERS

INDIRECT

1. All elements of dates *related to an individual*
   - (e.g., DOB, date of admission, date of surgery, etc.)
   - Exact ages over 89
2. Address elements
   - City, County, State
   - Zip Code
3. Other codes not HIPAA-designated as direct

DIRECT

1. Names
2. Full address; street address
3. Electronic mail addresses
4. Telephone & Fax numbers
5. Social security numbers: *SENSITIVE, rationale needed for collection
6. Medical record numbers
7. Biometric identifiers, including fingerprints and voiceprints
8. Full-face photographic images and any comparable images
9. Device identifiers and serial numbers
10. Health plan beneficiary numbers
11. Internet protocol (IP) address numbers
12. Account numbers
13. Certificate/license numbers
14. Vehicle identifiers and serial numbers, including license plate numbers
15. Web universal resource locators (URLs)

LEVELS OF IDENTIFIABILITY

Anonymous

- The data/sample was collected without knowing the identity of the subject.
- There is no chance of re-identification because **no identifiers were collected**

De-identified

- The data/sample was collected knowing the identity of the subject, but identifiers were removed.
- There is no chance of re-identification because:
  - **All identifiers were removed;** OR
  - There is **no link** between identifiers and data/sample

Limited Dataset

- The data/samples **include indirect identifiers only**
- Re-identification is improbable

Identifiable

- **Coded**
  - Assigned a unique **random** ID code that is linked to identifiers. Link must be stored separately to be coded. Re-identification is possible.
- **Identified**
  - Identifiers (e.g., name, medical record number, etc.) is stored with the health information

REQUIREMENTS FOR HIPAA IN RESEARCH

Identifiable Data in Research

- 1+ of the 15 direct identifiers are being collected
  - Data may be coded (best practice) or not

- Authorization options
  - Full written with signature
  - Alteration of HIPAA (waiver of signature)*
  - Full waiver*
- Consent options
  - Full written with signature
  - Verbal / signature waived*
  - Waiver / alteration*

*With appropriate rationale

HIPAA AUTHORIZATION REQUIRED ELEMENTS

- The PHI collected as part of the study
- The purpose of the use/disclosure
- Who may use PHI (within the covered entity)
- Who may disclose and who may receive PHI
- The duration of the authorization (or statement that it does not expire)
- The right to revoke the authorization and how to do that
- A statement that once information is shared outside of the covered entity it may no longer be protected by HIPAA

HIPAA WAIVER CRITERA

- Use / disclosure involves **no more than minimal risk** to the participants
- **Adequate confidentiality plan** to protect PHI from improper use/ disclosure
- **Adequate plan to destroy** at least direct **identifiers at the earliest opportunity**
- Adequate written assurances that **PHI will not be reused/disclosed**
- **Rationale** as to why the research **could not be practicably conducted without the waiver**
- **Rationale** as to why the research **could not be practicably conducted without access to PHI** and the PHI to be collected **is the minimum necessary.**

When the disclosure of PHI could be considered greater than minimal risk given the potential identifiers included (certain direct identifiers), the waiver may require review by the convened board

What does an appropriate confidentiality plan consist of?

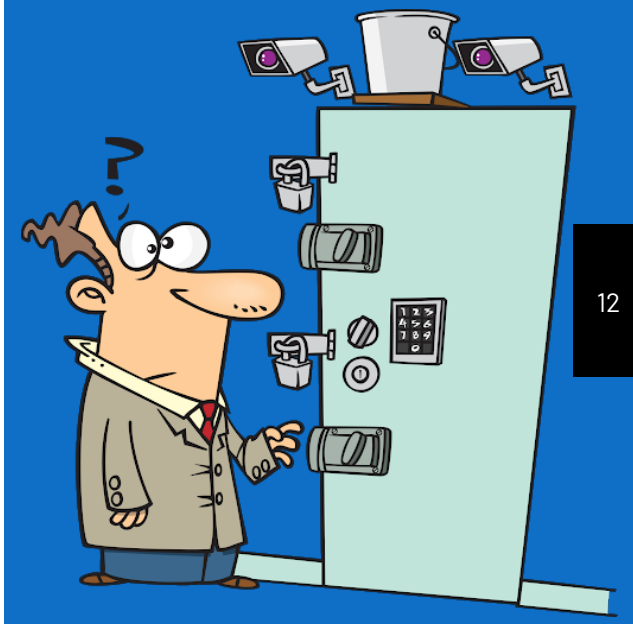
- How the data is stored (with identifiers, coded, de-identified)
- Where the data is stored electronically (as applicable)
  - How it will be secured, which must align with ePHI guidance
- Where the data is stored in hard copy (as applicable)
  - How it will be secured
- Whether data will be transmitted internally and/or externally
  - How it will be secured, which must align with the ePHI guidance
- Who will have access to the data
- Whether data will be disclosed to anyone outside of covered entity
  - How it will be secured, which must align with the ePHI guidance

Identifiable Data Storage

- Institutionally secured & managed network drive (e.g., Penn Medicine / Dental server)
- Device encrypted by ISC (hard drive or flash drive)
- Institutionally- approved third-party computing environment (RedCap, Penn Box, Way to Health, etc.)
- Strong passwords to protect against unauthorized access

Identifiable Data Physical Storage

- General location should be identified (e.g., PI's office or laboratory);
- Security required (e.g., locked filing cabinet/ office; locked freezer or fridge for coded or identifiable specimens)

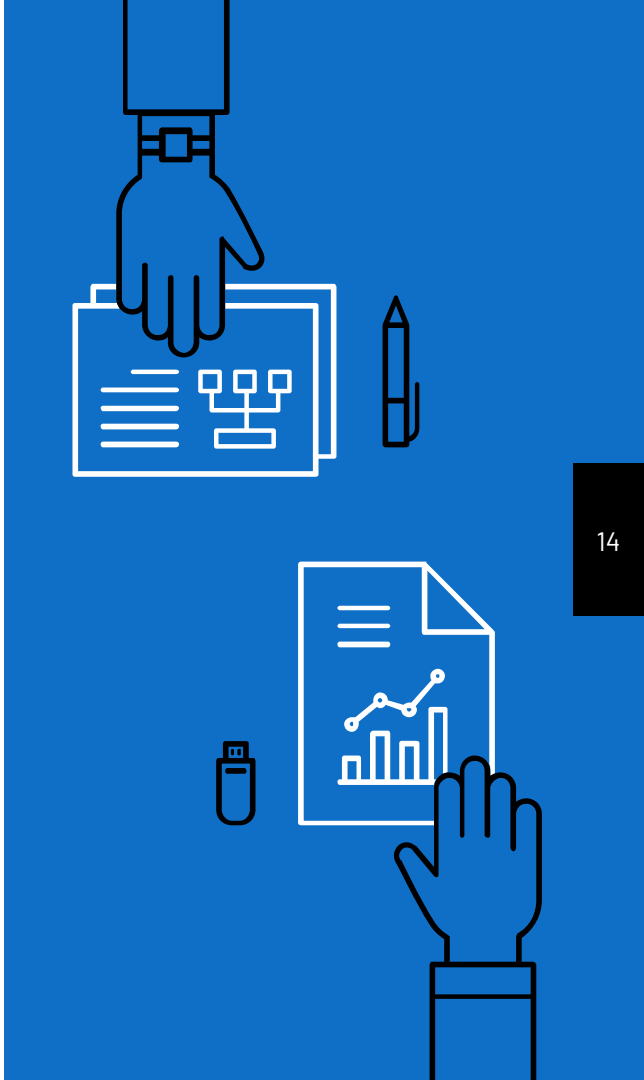


Identifiable Data Transmission

- Transmission of *data between co-investigators, collaborators, or sponsors* should be conducted via secure data transmission channels to protect against data interception
  - Penn Box, RedCap, Secure Share (internal only) are Penn-approved
  - Other Penn ISC approved transmission process.
  - Portable drive encrypted by ISC
- Transmission of data via email/ text is not considered secure
  - **Email is not HIPAA secured**, unless the study team is sending messages to a HIPAA secured encrypted mailbox where the recipient is required to log in to receive the message.
  - Data should be encrypted when "in- transit." Researcher should reach out to their ISC providers for guidance.

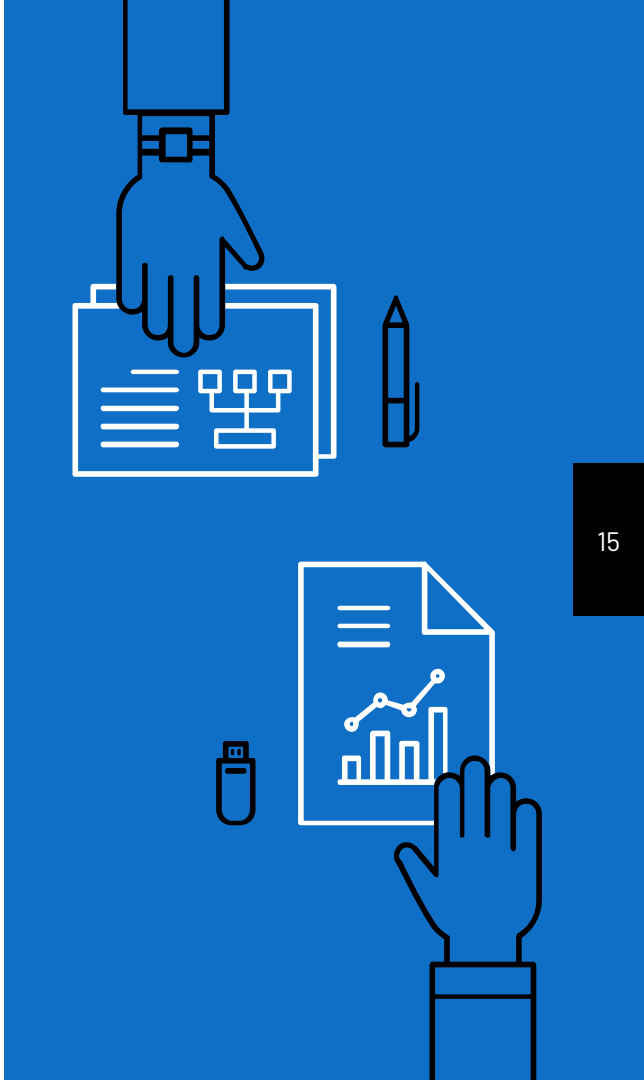
Identifiable Data Disclosures

- Access should be restricted to
  - IRB approved investigators
  - Any others described in the HIPAA authorization or HIPAA waiver form
- Business Associates Agreement (BAA) required **if authorization not obtained**
  - An agreement into which the covered entity enters with the intended recipient of **identifiable data** that establishes the ways in which the information may be used and how it will be protected.
- Business Associate
  - Any individual or entity that performs functions or services on behalf of a covered entity that requires the business associate to access PHI



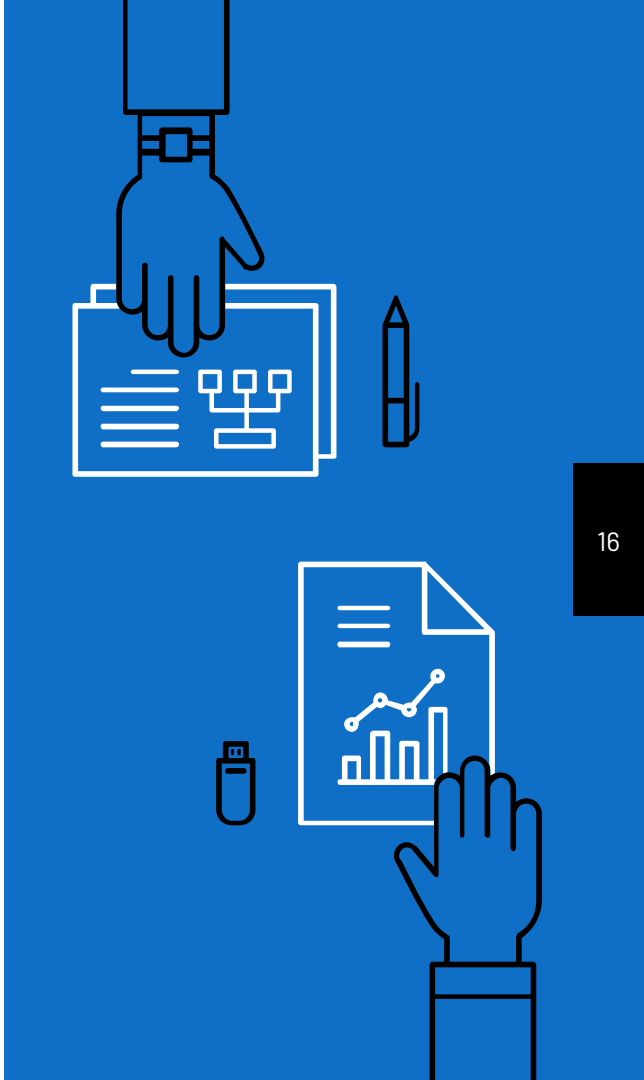
Limited Data in Research

- None of the **15 direct identifiers** are being collected
- Authorization requirements: None
- Consent still applies unless criteria for a waiver/alteration are met
  - Name cannot be collected on the IC



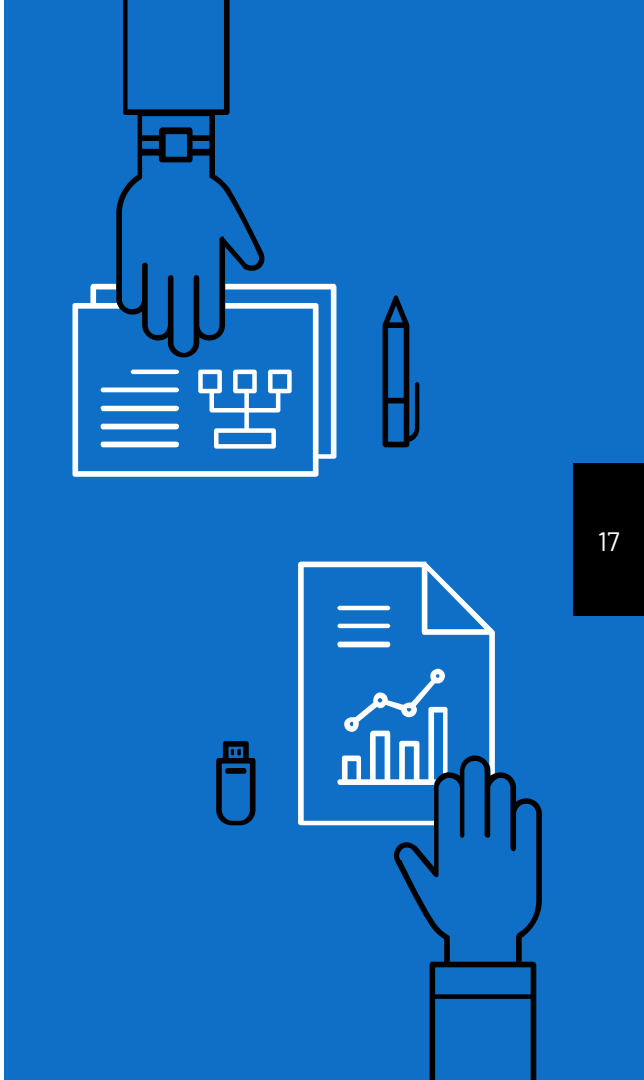
Limited Dataset Storage & Transmission

- Storage
  - Institutionally secured & managed network drive (Penn Medicine / Dental server)
  - Encrypted device (hard drive or flash drive)
  - Institutionally- approved third-party computing environment (RedCap, Penn Box, Way to Health, etc.)
- Transmission
  - Use of secure data transmission channels to protect against data interception, such as Penn Box, RedCap, Secure Share (internal only)



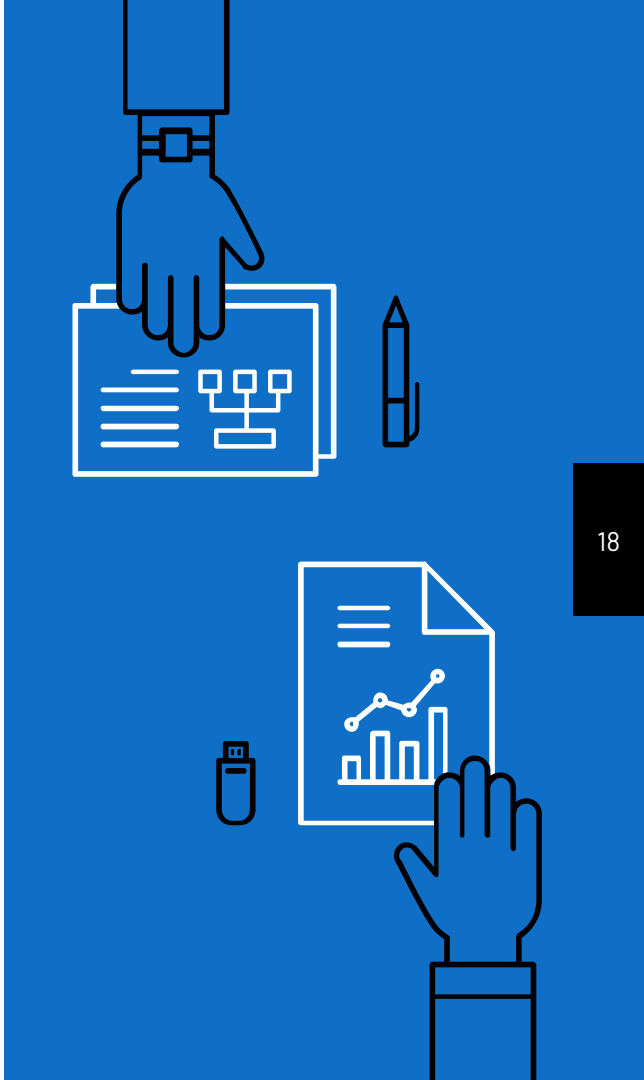
Limited Dataset Disclosures

- Access should be restricted to IRB approved investigators
- Data Use Agreement (DUA) required **if authorization not obtained**
  - An agreement into which the covered entity enters with the intended recipient of a **limited dataset** that establishes the ways in which the limited data may be used and how it will be protected.



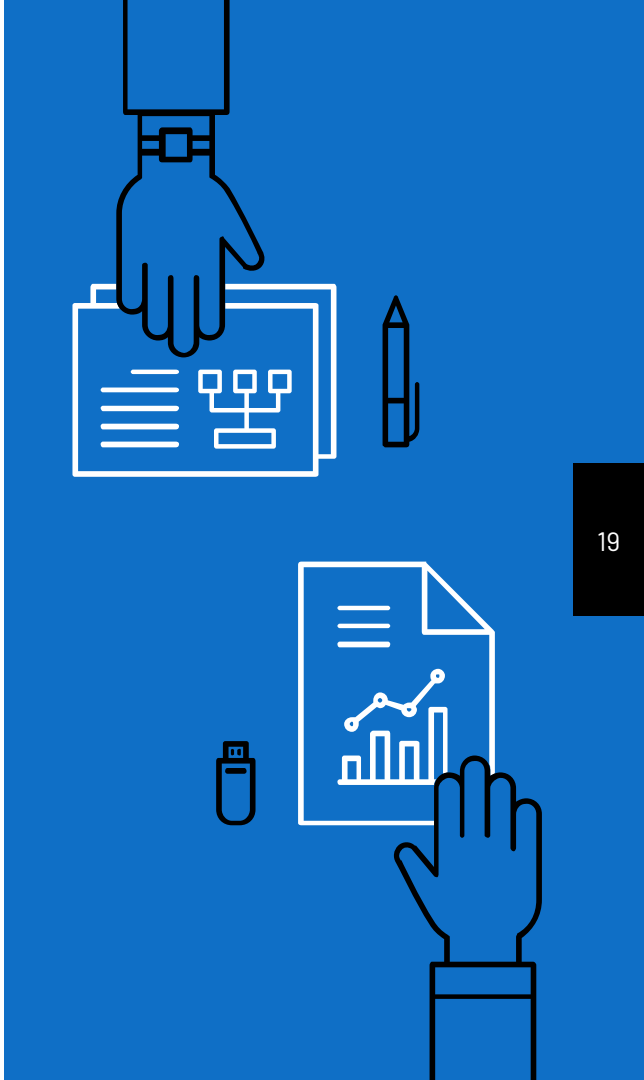
Anonymous/De-Identified Data in Research

- None of the **18 identifiers** are being collected
- Authorization requirements: None
- Consent still applies unless criteria for a waiver / alteration are met
  - Name cannot be collected on the IC

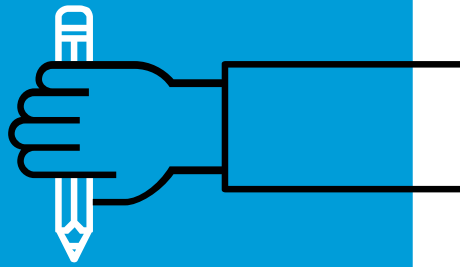


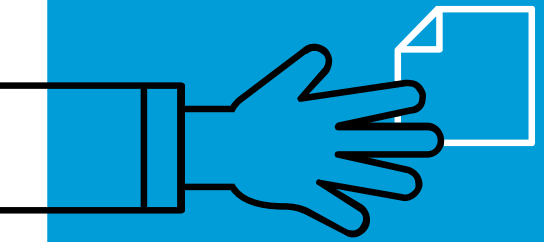
Anonymous/De-Identified Data Storage & Transmission

- Storage
  - No special requirements
  - To ensure data integrity recommend that data be stored on Penn server to mitigate potential for data loss.
- Transmission
  - Recommend using a secure transmission process such as Penn Box, RedCap, Secure Share (internal only)



SPECIAL TOPICS



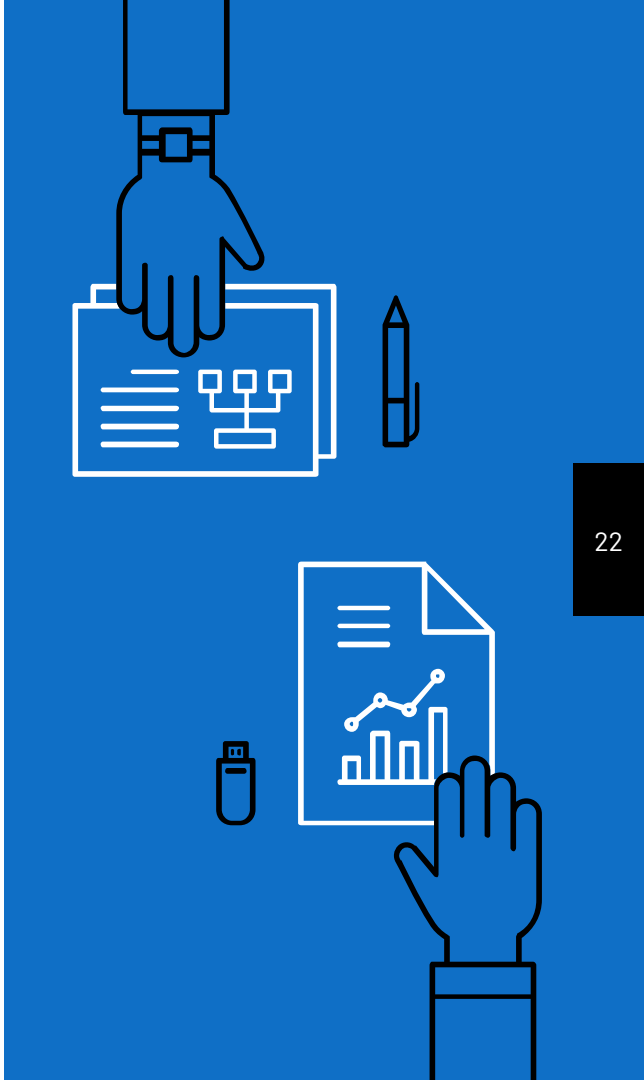


PREPARATORY TO RESEARCH ACTIVITIES

- Researchers may **access** PHI for planning or to determine feasibility of a study. Examples:
  - Searching charts to tally the number of cases of a certain condition for preparation of a protocol
    - PHI is not permitted to be collected
  - Reviewing charts to collect contact information for recruitment purposes
    - Study must be IRB approved
    - Only employees under the CE may contact potential participants
- For an activity to qualify under Preparatory to Research, the researcher must confirm the following:
  - The use is sought solely to prepare the research protocol or other similar preparatory purposes.
  - No PHI will be disclosed outside the CE
  - The PHI being accessed is necessary for the research purposes.

Requirements for the use of EMR Tools

- Slicer Dicer: Self-service tool
  - May be used for cohort identification or as a research tool
    - If utilizing to access PHI need to enter IRB number into query and should mention use of this tool in IRB application
- Care Everywhere: One of many health information exchanges detailed in the NPP
  - **Cannot be used to pull in research records from other hospitals for recruitment**
  - Can be used to obtain hospitalization information for tracking AEs on a trial.
  - Research information (e.g., results) may be sent out via Care Everywhere
- Contact OCR Operations with questions



LOCAL REGULATIONS: PENNSYLVANIA

Confidentiality of HIV-Related Information Act	• ***Identifiable*** HIV/AIDS related information may not be used for research purposes without prospective consent, unless the researcher is involved in a person's clinical care
Drug and Alcohol Abuse Control Act	• ***Identifiable*** patient records related to drug or alcohol use or dependence may not be used for research purposes without prospective consent
Mental Health Procedures Act	• Precludes a waiver of consent for use of ***any*** mental health data from the mental health records

LOCAL REGULATIONS: PENNSYLVANIA

- PA DOH Prescription Drug Monitoring Program [ABC-MAP Act 191]
  - Researchers may only query the PDMP database for research purposes if they are a prescriber or dispenser, and **only for their own existing patients**.
  - If information from PDMP is placed into any patient's medical record, it may be used in accordance with HIPAA.
  - Any publications resulting from the use of the PDMP system must contain the following disclaimer:
    - *"These data were obtained from the Pennsylvania Prescription Drug Monitoring Program (PDMP) system. The Pennsylvania Department of Health and Prescription Drug Monitoring Program Office specifically disclaims all responsibility for any analyses, interpretations, or conclusions."*

LOCAL REGULATIONS: NEW JERSEY

- Applicable to any research at or affiliated with Princeton Health

Genetic Privacy Act 126

- Precludes a waiver of consent for use and disclosure of **identifiable** "*genetic information* from an individual or an individual's DNA sample"
- Precludes a waiver of consent to "retain an individual's **identifiable** *genetic information*." If involves anonymous DNA sample and a waiver is granted for retention, the DNA sample must be "destroyed promptly upon completion of the project or withdrawal of the individual from the project, whichever occurs first."

OTHER RELATED REGULATIONS

21st Century Cures Act

- Requires healthcare institutions to allow patients increased access to the content in their electronic medical record.
- An exception can be made IF the research is blinded, and/or the protocol dictate that results must be withheld from a subject
  - The IC must inform participants of delays in information being available within their EMR (new consent language forthcoming)

European Union Privacy Laws

- If the research involves collecting personal information from individuals residing in Europe, refer researcher to the Privacy Office for direction.

REPORTING HIPAA INCIDENTS & BREACHES

- **All Penn staff are required by law and Penn policy to report incidents involving PHI** to Information Security Office, the applicable Entity Privacy Office/Officer, or OACP, including potential or confirmed loss, theft, or unauthorized access or disclosure
  - E.g., lost or stolen laptops, falling for a phishing scheme, losing papers that contain PHI, finding documents that have not been securely shredded or disposed of properly, knowledge of insider abuse of patient information, posts on social media and any other instance where sensitive patient data is exposed.
- The individuals working in these offices will help ensure an analysis is conducted and any necessary mitigation or reporting occurs.

RESOURCES

- Office of Civil Rights HIPAA Guidance
- Penn Medicine Privacy Office
  - 215-573-4992
  - privacy@uphs.upenn.edu
- Information Security
  - informationsecurity@pennmedicine.upenn.edu
- Penn Medicine Service Desk
  - 215-662-7474
- Penn Policies and Guidance
  - UPHS and SOM HIPAA Policy for Research
  - ePHI Guidance
- Methods of De-Identification:
  - www.imperva.com/learn/data-security/anonymization