Penn
University of Pennsylvania
Human Research Protections Program

Table of Contents

Penn
University of Pennsylvania
Human Research Protections Program

Requirements for Research Involving the Use of Protected Health Information (PHI)

INTRODUCTION

As part of the IRB review process federal regulations require that prior to approving a protocol, IRBs establish that "there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data". [See 45 CFR 46 § 46.111 (7)]. Additionally, IRBs must establish that "risks to subjects are minimized" including potential informational risks associated with the use of data for research purposes. [See 45 CFR 46 § 46.111 (1)].

In addition to the regulatory requirements for human subjects' protections, researchers may be subject to specific requirements for data security and storage that stem from other state or federal regulations, requirements of funding agencies, contractual obligations, or data access agreements.

The purpose of this document is to outline the IRB's expectations for security and storage when research involves the use of directly identifiable protected health information subject to HIPAA requirements.

Please Note: Research studies may involve the use of data that does not qualify as protected health information but is otherwise considered to be sensitive. The IRB strongly encourages study teams planning to use sensitive data to consult with their local ISC support provider/security liaison to develop a plan for data security and storage prior to submitting their protocol for IRB review. For a list of local ISC support providers/security liaisons, please visit the following link.

REQUIREMENTS FOR RESEARCH INVOLVING ACCESS TO PHI

All research protocols that involve the viewing of directly identifiable PHI must outline this access.

REQUIREMENTS FOR RESEARCH INVOLVING COLLECTION OF PHI

All research protocols that involve the collection of directly or indirectly identifiable PHI must have an appropriate confidentiality plan that outlines the following:

1. How the PHI and/or (if applicable) specimens are stored
   - i.e., with identifiers, in a coded fashion (with a link stored separately from a de-identified or limited dataset, etc.);
2. Where the PHI is stored electronically (as applicable)
   - How it will be electronically secured;
3. Where (physical location of) the PHI is stored in hard copy (as applicable)
   - How it will be physically secured;
4. Who will have access to the PHI, including disclosures those external to the covered entity;

5. Whether PHI will be transmitted internally and/or outside of the covered entity
   - How it will be secured during transmission;
6. How long the PHI will be stored, and when destruction of direct identifiers may occur.
7. When applicable: any specific requirements for data security and storage that stem from other state or federal regulations, requirements of funding agencies, contractual obligations or data access agreements.

The confidentiality plan may be described in a standalone protocol or within the HSERA application. If the confidentiality plan is contained the standalone protocol, the HSERA sections *Subject Confidentiality* and *Data Disclosure* should refer to the section of the protocol where the confidentiality plan is located.

Guidelines for Physical Security (Paper files/ Biospecimens)
Research protocols that involve the collection and storage of files in paper format (including, if applicable, a master link for coded documents) AND/OR storage of biospecimens should outline appropriate security which includes:

1. Keeping any directly identifiable materials under lock and key (e.g., locked filing cabinet within the PI's office or locked freezer or fridge within the PI's lab)
2. If directly identifiable materials may be shipped to other locations, outlining how this will be securely shipped (e.g., Courier service; Fed Ex or UPS with tracking).

If physical files will not be collected or stored, the research team may note that in their confidentiality plan.

Guidelines for Electronic File and Data Security
Research protocols that involve the collection and storage of electronic files and data (including, if applicable, a master link for coded documents) should outline appropriate security which includes:

1. Secure storage on one of the following:
   - Institutionally-secured & managed network drive
   - Institutionally-secured & managed device encrypted by ISC
   - Institutionally-approved third-party computing environment.
2. Describe any additional security, as applicable (e.g., password protected document or folder)

<u>Guidelines for Electronic Transmission Security</u>
The IRB understands that in the course of research conduct, researchers may need to transmit PHI. Acceptable mechanisms for transmitting PHI include:

1. Institutionally-secured & managed device encrypted by ISC
2. Institutionally-approved secure encrypted file transfer solution

Please Note: Email is not considered a secure file transfer solution. Please refer to the following guidance documents in relation to the use of email, appended to this guidance:

1. Penn Medicine Privacy and Information Security Offices Guidance: **Avoiding & Minimizing PHI in Email**
2. Penn Medicine Office of Clinical Research (OCR) Guidance: **Use of Email During Conduct of Research**

Please see the definitions section below for a complete description of each of these mechanisms. To verify that you are using an institutionally-approved option, please consult with your local ISC support provider/security liaison. For a description of key features of institutionally-approved options please review the Companion Guide to this document.

For assistance in selecting an institutionally-approved portable drive or secure file transfer solution, please contact your local ISC support provider/security liaison.

NOTE: If you have any concerns about how to meet the requirements outlined in this document, please contact the IRB for assistance. The IRB's contact information is available at the following link http://irb.upenn.edu/directory.

DEFINITIONS

Protected Health Information (PHI)
PHI, as defined by HIPAA, means individually identifiable health information about an individual that is transmitted or maintained by electronic media or in any other form or medium. PHI includes demographic information that is created or received by a health care provider, health plan, employer, or health clearinghouse. PHI relates to the past, present, or future physical or mental health or condition of an individual; the provisions of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual or can reasonably be used as a basis to identify an individual.

Personally Identifiable Information (PII)
Information that can be used, alone or in combination with other available information, to identify an individual. HIPAA identifiers are PII.

Direct Identifiers
Research data that contains ANY of the following identifiers is considered to be directly identifiable and is subject to this policy:

- *Name*
- *Health plan beneficiary numbers*
- *Postal address information*
- *Account numbers*
- *Certificate/license numbers*

- *Telephone numbers*
- *Vehicle Identifiers and serial numbers including license plate numbers*
- *Fax numbers*
- *Device identifiers and serial numbers*
- *Electronic mail addresses*
- *Web Universal Resource Locators (URLs)*
- *Social security numbers*
- *Medical record numbers*
- *Internet Protocol (IP) address numbers*
- *Biometric identifiers – including finger and voice prints*
- *Full face photographic images and comparable images*

Please Note: If your research data only contains one or more of the following and qualifies as a limited data set, this policy does not apply, however, appropriate safeguards should still be undertaken for storage and maintenance of your study data:

- All elements of dates [e.g. birthdate, date of visit, date of sample collection]
- Certain limited geographic identifiers including city/town, state and/or zip code.
- Any other unique identifying number, characteristic or code

As a reminder: In the event that a limited data set will be shared outside of the covered entity, a data use agreement is required. Please note that a DUA can be executed through the Office of Research Services through use of their research inventory system. Look for the log-in to the research inventory system at the link in the left navigation bar at the following site: http://www.upenn.edu/researchservices/

Institutionally Secured & Managed Network Drive:
A network drive/departmental file share that is secured and managed by a regular, full-time University of Pennsylvania staff member with a designated IT position within a school's central IT organization.

Institutionally Secured & Managed Device:
A physical device including a laptop, desktop, tablet, phone, or other electronic device that is secured and managed by a School's central IT organization in accordance with applicable regulations and institutional requirements for storage of electronic protected health information. At a minimum, these devices must be encrypted.

Please Note: Penn Medicine devices and network drives are compliant with federal regulations for storage of PHI. For researchers who are not affiliated with Penn Medicine, additional review of your device/network drive may be required to ensure appropriate protections consistent with federal regulations. Consult your local ISC support provider/security liaison for guidance.

Institutionally-approved third-party computing environment:

A third-party computing environment that has been institutionally reviewed and approved. Such approval may be conditioned on the existence of contractual agreements and security review to ensure appropriate protections.

**Please consult with your local ISC support provider/ security liaison for guidance when proposing the use of a third-party computing environment.

Encryption
The process of converting information or data into a code, especially to prevent unauthorized access.

NOTE: Password protection is NOT encryption.

Penn
University of Pennsylvania
Human Research Protections Program

Key Features of IRB-Approved Mechanisms for Data Storage/Transmission when Research Involves the Use of Protected Health Information (PHI)

This document serves as a companion to the document titled *Requirements for Research Involving the Use of Protected Health Information (PHI)*. The purpose of this companion guide is to outline key features of IRB approved mechanisms for data storage/transmission when research involves the storage/ transmission of protected health information [PHI] containing direct identifiers. Please note, this guide is meant to assist you in working with your local ISC support provider/ security liaison to decide on the use of any of the approved options.

The IRB does not expect to see a description of these key features included in the data confidentiality plan described in your IRB application. It is presumed that if you have selected one of the IRB-approved options for data storage or transmission that you have verified with your local ISC support provider/security liaison that the option selected contains the key features described below.

IRB –APPROVED MECHANISMS FOR DATA STORAGE

Institutionally Secured & Managed Network Drive

In order to utilize this storage option, the information must be:

- Stored on a private institutionally-managed network
- Maintained on physically secure server in a secure data center
- Backed up on a regular basis
- Stored on a server that is monitored for unauthorized access and other security and operational events
- Stored on a server that is scanned on a regular basis for vulnerabilities
- Stored on a server that ensures unnecessary services and accounts are disabled

Institutionally Secured & Managed Device

Institutionally secured & managed devices will have the following key features:

- Devices are joined to a private institutionally-managed network.
- Devices have a theft and loss prevention software installed such as Computrace
- Devices have anti-virus installed that is set to update as new pattern files are released
- Devices have whole disk encryption
- Devices are supported by a School's central IT organization
- Devices are included in a patch management process to install security updates
- Devices have unnecessary services and accounts disabled

Institutionally- approved third-party computing environment

Each third party computing environment must be reviewed to determine the security provisions comply with Penn expectations for storage of directly-identifiable protected

health information. One avenue through which institutional review and approval may be secured is through the SPIA for Vendors process. More information about this process may be accessed here: http://www.upenn.edu/oacp/privacy/penndata/evaluating-third-parties.html.

IRB –APPROVED MECHANISMS FOR DATA TRANSMISSIONS

Use of a Penn-approved encrypted portable drive
Key features of acceptable portable drives include:
- Encryption technology is FIPS 140-2 compliant or stronger
- Biometric Encryption may be sufficient
- Utilizes a password/pin [Please note the password/key may not travel with the device]

Examples of acceptable options include:
- DataLocker: https://www.cdw.com/shop/products/DataLocker-Sentry-DLSF16-USB-flash-drive-16- GB/2844302.aspx?pfm=srh ($71.99)
- Kingston: https://www.cdw.com/shop/products/Kingston-DataTraveler-4000-G2-USB-flash-drive-16- GB/3613989.aspx?pfm=srh ($74.99)
- Kanguru: https://www.cdw.com/shop/products/Kanguru-Defender-3000-Secure-FIPS-Hardware- Encrypted-USB-flash-drive-16/3804547.aspx?pfm=srh ($126.99)
- Aegis: https://www.cdw.com/shop/products/Apricorn-Aegis-Secure-Key-3.0-USB-flash-drive-16- GB/3976334.aspx?pfm=srh ($131.99)

Use of a Penn-approved secure, encrypted file transfer solution:
Key features of a Penn-approved encrypted file transfer solution:
- Communication must be through a secure tunnel
- All data is encrypted prior to sharing with any third parties using an encryption mechanism that meets the FIPs 140-2 standard

Examples of acceptable file transfer solutions:
- Secure Share
- Secure FTP
- HTTPS

**Please note: Password protection does not afford sufficient protections for file-sharing.

Penn Medicine

Avoid and Minimize PHI in Email

GUIDANCE FROM THE PENN MEDICINE PRIVACY AND INFORMATION SECURITY OFFICES

Information we maintain related to a patient's health status that can be linked to the patient is considered protected health information (PHI) under HIPAA. **Whenever possible, you should avoid transmitting PHI or other sensitive information in email because there are many risks to using email**. For example, it is easy to make mistakes such as misdirecting email messages and inadvertently using "reply all" or "cc" instead of "bcc" features. Plus, there's the potential for an email to be intercepted and for email inboxes to be compromised by an external attack.

If email must be used to transmit PHI, use Penn's email system and limit PHI and identifiers to the minimum amount needed to achieve the purpose of the communication, without compromising patient safety. Publicly available email systems, like Gmail and Yahoo, must never be used for Penn business communications. Auto-forwarding of Penn email to external or personal mail accounts is also not permitted.

In all cases, **avoid** using email to send:

1. **Highly sensitive information** (such as social security numbers, intellectual property, diagnoses, treatment for certain specially-protected conditions such as mental health, substance abuse, and HIV information);
2. Documents containing **information about numerous individuals** (such as schedule lists for specific procedures or spreadsheets of data used in research or other analysis or business operations); and
3. Information that directly or indirectly reveals **patient PHI to groups of recipients**, such as listservs of patient names or names of research subjects.

Note that data loss prevention technology is being implemented to send alerts and may block Penn users who attempt to send sensitive patient data by email.

As **alternatives to email**, please use entity-approved file sharing systems, shared drives, as well as messaging within your patient portal and electronic medical records system. Your IT support can assist in identifying and supporting a solution to address your communication needs.

Created 11/19

Use of Email During the Conduct of Research

This guidance provides best practices for use of email in connection with clinical research in a way that appropriately safeguards Protected Health Information and Personally Identifiable Information as defined at the end of this guidance (PHI/PII). There are numerous risks associated with the use of email, including:

- Emails may be easily misdirected, including through auto populating and email forwarding
- "Reply all" can easily inadvertently used
- The carbon copy (cc) may inadvertently be used instead of the blind carbon copy (bcc)
- Email is often unencrypted or encrypted incorrectly

This document outlines situations within the course of a research study in which email communication may be considered by a research team such as: for recruiting subjects prior to obtaining consent, post- consent, and between and among the study teams. Each situation is outlined below along with best practices.

In all cases, and as described further below, the following practices should be followed:

- **Penn Medicine faculty and staff should not use email to transmit PHI and PII**
- **At a minimum, Penn Medicine faculty and staff must not use email to send (1) sensitive information[1] or (2) datasets / documents containing information about numerous individuals.**
- **When recruiting patients for trials, email must not be used without IRB approval**
- **Researchers must not send mass or group emails (emails to more than one recipient) because of the high risk of error in the copying process**

Please contact psom-ocrops@pobox.upenn.edu for assistance in tailoring an appropriate approach to email communication for the specific circumstances of the research.

COMMUNICATING WITH RESEARCH SUBJECTS VIA EMAIL

Recruiting Research Subjects via Email Pre-Consent

The IRB may grant approval to recruit subjects using email on a case-by-case basis.

1. IRB approval of recruitment communications must be obtained and documented
2. MyPennMedicine should be used to communicate with research subjects when feasible.
3. Whenever possible, patients should be notified that email will be used for communications, as well as the risks of using email[2]
4. PHI should not be included in the email beyond what is necessary for initial contact
5. The email should be encrypted when technologically feasible.

6. Researchers must not send mass email messages (messages to more than one recipient at a time), because of the high risk of error and implications for patient privacy and regulatory reporting.

Contact with Subject After Signing Consent:

1. MyPennMedicine should be used to communicate with research subjects when feasible.
2. If email is necessary, the risk of email should be clearly outlined to the subject in the consent and the subject must review and consent to the risks.

   Sample consent language:

   For this study we may need to contact you via email to provide you information about scheduling, appointments notes or to send you information about your participation in the study. Email communications are often not secure and may be seen by others as a result. By signing below, you accept this risk.

   If you wish for us to use a different means to communicate with you during the course of this trial please discuss this with the research team and alternative methods can be arranged.
3. If a research subject consents to the use of email for communication and it must be used to transmit PHI, always use Penn's email system and limit PHI and identifiers to the minimum amount needed to achieve the purpose of the communication, without compromising subject safety.
4. Researchers must not send mass email messages (messages to more than one recipient at a time), because of the high risk of error and implications for patient privacy and regulatory reporting.

COMMUNICATIONS AMONG THE RESEARCH TEAM IN A RESEARCH STUDY

During the course of a study, researchers may need to communicate with other members of the research team. The recommendations below apply:

1) Internal Sharing:

a) Establish parameters for sharing information internally at the start of the study.
b) Always use subject ID rather than MRN or other patient identifiers, whenever possible.
c) When possible, leverage Penn Chart InBasket, secure drives, and other secure communications.
d) If information must be sent internally by email:
   i. Limit PHI, including sensitive information, such as diagnosis and sensitive services.
   ii. Limit identifiers, provided this does not compromise patient care or safety.
   iii. Do not send mass emails to team members or include datasets on several

subjects data.

2) **External sharing**
Do not send PHI/PII externally by email. PHI may be shared externally using approved Penn Medicine secure file sharing solutions, such as Citrix ShareFile.[3] All other file sharing solutions used to transfer PHI to external recipients is prohibited. Always use subject ID rather than MRN or other patient identifiers whenever possible.

3) **Datasets**
Do not share datasets internally or externally.
Such datasets present a high risk from a privacy and breach reporting perspective.[i] Instead, leverage secure encrypted drives, authorized remote access methods, Electronic Data Capture Systems (EDCs) and approved Penn Medicine secure file sharing solutions. Always use subject ID rather than MRN or other patient identifiers whenever possible.

a) **NOTE:** Consider use of a Limited Data Set (LDS)- see note about LDS below if data must be transmitted internally or externally (see below for Covered Entity). In case of doubt, contact the Office of Clinical Research OR Office of Audit, Compliance and Privacy (OACP) to review the proposed dataset to be transmitted.

FOOT NOTES

[1] Examples of sensitive information are diagnosis information, a patient receiving mental health or substance abuse services, information about study participation that a subject could reasonably expect to be kept private, etc.

[2] (For example: a Facebook survey prescreen for a study should start with a brief description of the study, a note that email will be used for the initial communication aimed at identifying potential members of a volunteer registry and that email may be vulnerable to interception or misdirection)

[3] For more information or to obtain a temporary secure file sharing account, please submit a Penn Medicine IS Help Desk ticket and IS Security will assist you. Contact iassurance@pennmedicine.upenn.edu.

ADDITIONAL RESOURCES

Penn Medicine Data Protection Policy:
www.med.upenn.edu/policy/user_documents/PSOMElecDataPolicy-signedversion.pdf