Electronic Data Protection Requirements for Research Involving the Use of Protected Health Information (PHI)*

As part of the IRB review process federal regulations require that prior to approving a protocol, IRBs establish that “there are adequate provisions... 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 data 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 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 Support Providers/Security Liaisons, please visit the following link.

Requirements for Data Storage when research Involves use of Protected Health Information (PHI):

For all research protocols that involve the use of directly identifiable protected health information [PHI] by Penn-based researchers, the protected health information must be maintained using one of the following mechanisms, or a combination of these.

1. Institutionally secured & managed network drive
2. Institutionally secured & managed device
3. Institutionally- approved third-party computing environment

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 support provider/security liaison. For a description of key features of institutionally-approved options please visit the companion guide to this document.

Requirements for Transmission/Temporary Storage of PHI
The IRB understands that in the course of research conduct, researchers may need to transmit PHI. Acceptable mechanisms for transmitting PHI include:

1. Use of a Penn-approved encrypted portable drive
2. Via a Penn-approved secure encrypted file transfer solution

For assistance in selecting a Penn-approved portable drive or secure file transfer solution, please contact your Local Support Provider/Security Liaison. For key features of Penn-approved transfer solutions, including examples of approved options, please review the companion guide to this document.

Please Note: Email is not secure. Make all efforts to reduce the sensitivity of information shared via email.

Completing the HS-ERA application:
For research that involves the use of directly-identifiable protected health information, researchers must identify within the HS-ERA application which mechanism for secure storage will be utilized from the list above. A description of your plan must be incorporated into the “Subject Confidentiality” section of the HS-ERA application. Within this section, the following must be included:

- A description of how research data will be handled, managed, and transmitted in compliance with the requirements above, as well as 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.
- A description of any additional controls that will be implemented for the storage, handling, and sharing of data.
- The long-range plan for protecting the confidentiality of research data, including a schedule for destruction of identifiers associated with the data.

Please 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://www.upenn.edu/IRB/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.
Directly identifiable Protected Health Information:
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 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 contact the IRB for guidance when proposing the use of a third-party computing environment.**