Institutional Review Board (IRB)
Human Subjects Protection Office
Penn State College of Medicine | Penn State Milton S. Hershey Medical Center
Hershey | 717-531-5687 | hspo@hmc.psu.edu

STANDARD OPERATING PROCEDURE ADDENDUM

Security and Integrity of Human Research Data

A. Definitions

1. **Data Transfer Agreement:** An agreement used if the research project involves any transfer of human research data to and/or from any third party, whether an external sponsor or external investigator.
2. **External researcher**: If the research uses/discloses identifiable protected health information (PHI) as defined below, an external researcher is defined as any research investigator who is not an employee, faculty member, or student of the Penn State College of Medicine (COM) and/or The Milton S. Hershey Medical Center (HMC). If the research does not use/disclose identifiable protected health information (PHI) as defined below, an external researcher is defined as any research investigator who is not an employee, faculty member, or student of the Penn State University, the COM and/or HMC.
3. **HIPAA**: the Health Insurance Portability and Accountability Act of the United States.
4. **Human research data**: Information captured in the course of conducting human research as defined by federal regulations and IRB policies.
5. **Institutional Review Board (IRB):** A committee that reviews human research to ensure the protection of human subjects in research.
6. **Intellectual Property (IP) policy:** as defined in the Penn State Policy IP01 and referencing the intellectual property agreement implemented in 2013 by the College of Medicine and Hershey Medical Center
7. **Office of Research Affairs (ORA):** The office managing contracts in support of sponsored research, clinical trials, or grants.
8. **Office of Technology Development (OTD):** The office managing intellectual property generated at HMC or COM.
9. **Penn State Hershey researcher**: Employee, faculty member or student of the Penn State College of Medicine and/or The Milton S. Hershey Medical Center who are engaged in human research.
10. **Personally Identifiable Information (PII)**: Information that can be used to uniquely identify a single person or group of individuals. Examples include an individual's name and Social Security Number, Driver's license, non-Driver's license identification number or financial account information.
11. **Protected Health Information (PHI)**: As defined under the Health Insurance Portability and Accountability Act (HIPAA) and in Penn State Hershey Hospital Administrative Manual (HAM) Policy C-18, is PII concerning the health status, provision of care, or payment for care.

B. Policy

1. It is the policy of the Penn State University College of Medicine IRB to oversee the review the data security and integrity plans for all research studies involving human subjects to ensure the protection of confidential information of research subjects and to ensure the integrity of the data. It is the responsibility of the ORA and the OTD to oversee the adherence to applicable IP policies and standard operating procedures regarding data and data transfer agreements.
2. This policy defines the following 2-level categorization schedule for human research data and accompanying sets of security and integrity measures to protect the human research data.

Level 1 – De-identified research information about people.

Level 1 information is research information in which all information that could be used, directly or indirectly, to identify an individual has been removed. De-identified research information is described in federal IRB regulations as information "recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to subjects." The HIPAA Privacy Rule for protected health information specifies eighteen categories of information that must be removed in order to de-identify PHI. For purposes of this policy, whole genomic sequence data are included in the same category as HIPAA identifiers.

See Appendix D for the eighteen categories of information that must be removed in order to de-identify data.

There are no specific data security requirements for the protection of de-identified research information, but researchers may want to protect such information for their own reasons, i.e., keeping data private until a paper about the data is published. The data security recommendations for Level 1 information are listed in Appendix A and the data integrity measures for Level 1 information are defined in Appendix C.

Level 2 – Information about individually identifiable people

Level 2 information includes individually identifiable information. This level includes non-sensitive and sensitive data. Sensitive data, if disclosed, could reasonably be expected to be damaging to a person's reputation, present risk of civil or criminal liability, psychological harm or other significant injury, loss of insurability or employability or social harm to individuals or groups. Non-sensitive data, if disclosed, would not ordinarily be expected to result in material harm, but the subject has been promised confidentiality.

Data security requirements for Level 2 information are defined in Appendix B. The data integrity measures for Level 2 information are defined in Appendix C.

3. The data security and integrity plan for a proposed research study involving human subjects is evaluated by the IRB in order to determine that the plan fulfills the requirements for the applicable security category and provides adequate measures to protect the integrity of the human research data.

a. The data security and integrity plans for initial study submissions are reviewed by the expedited review process by an IRB Chair or designated, experienced IRB member.

b. In conducting the review the IRB relies on the investigators' information provided in the protocol and the research data plan supplement submitted with the IRB application. The IRB may seek the advice and recommendations of the IT Security Group and/or appropriate Penn State Hershey technical experts in assessing the adequacy of provisions to maintain confidentiality of data.

c. If the IRB Chair or designated reviewer determines that the data security and integrity plan does not meet the requirements defined in this policy, the plan is reviewed by the IT Security Group.

d. The IRB has the authority to approve variances from the data security and integrity requirements that would apply to a study given its security category(ies), so long as the resulting plan complies with any legal requirements and does not increase the risk to the subjects, or jeopardize the integrity of the research data. Variances are granted on the recommendations of the IT Security Group and/or appropriate Penn State Hershey technical experts who assess the adequacy of provisions to maintain confidentiality of data and in approving a security category level.

4. If human research data are subject to security requirements specified in an information use agreement (such as data use or business agreements), grant, contract, or research protocol, those requirements must be met. The IRB, however, may impose additional requirements appropriate to the level of sensitivity of the information. If there are no security requirements specified in a data use agreement, grant, contract, or research protocol, the appropriate level of security and protection is determined by these data security and integrity policies.

5. Compliance with data security and integrity plans is monitored by the Research Quality Assurance Office as part of routine or directed post-approval reviews according to the standard operating procedures of that office. Any variances from the approved data security and integrity plans are reported to the IRB according to the Research Quality Assurance Office's standard operating procedures.

6. Breaches in confidentiality of research data must be reported promptly to the IRB according to the IRB standard operating procedure for reportable new information. In addition, investigators must report incidents involving identifiable health information to the Penn State Hershey Privacy Officer at (717) 531-2081.

7. If the research project involves any transfer of PII or PHI to and/or from any third party, whether an external sponsor or external investigator, the method of data transfer must be approved by the Penn State Hershey IT Security Group.

8. Written data transfer agreements are required if the research project involves any transfer of human research data to and/or from any third party, whether an external sponsor or external investigator, University unless the external entity would not be able to enter into an agreement (e.g. National Institutes of Health specific policies associated with the 3D print Exchange or Genomic Data Sharing). If an investigator believes there is a situation where an external entity would not be able to enter into a data transfer or data use agreement the investigator should contact OTD for consideration and evaluation. Written data transfer agreements are also needed if an investigator is leaving Penn State College of Medicine and/or The Milton S. Hershey Medical Center and plans to transfer research data to a new location. For more information see HRP-103 Investigator Manual, Section "What happens if I leave PSU?".

a. Data transfer agreements are negotiated by the ORA or OTD in the Penn State College of Medicine.
b. These data transfer agreements do not need to be submitted to the IRB but must be stored with Penn State Hershey investigator's regulatory documents and must be available upon request.

C. Procedure

This procedure provides guidance for submission, review and approval of data security and integrity plans.

I. Investigator Responsibilities

A. Penn State Hershey investigators are responsible for: (1) disclosing the nature of the confidential data they collect so the IRB can assess the data security risk in the protocol and the research data plan supplement submitted with the IRB application; (2) preparing study data security and integrity plans and procedures in accordance with the appropriate security category requirements; and (3) contacting the ORA or the Office of OTD to establish the data transfer agreement if the data are shared with a third party. For all research involving human research data, a data security and integrity plan must be submitted to the IRB as part of the initial IRB application.

B. Upon confirmation by the IRB of the appropriate security level(s), Penn State Hershey investigators are responsible for implementing and monitoring the data security and integrity plans over the course of their projects. If human research data are stored electronically, investigators are responsible for ensuring that computers and other devices that are used to store human research information are set up correctly and operated in a manner that meets the requirements of that level. Researchers may consult with Information Technology (IT) to help them understand and meet the requirements.

C. Penn State Hershey investigators are responsible for ensuring that all external investigators involved in the research study with access to any human research data have signed a confidentiality agreement which is available in policy C-01 HAM and a data transfer agreement. Note: Penn State College of Medicine and Penn State Hershey Medical Center staff, faculty and students have a signed confidentiality agreement on file in their applicable Human Resource department.

D. Penn State Hershey investigators are responsible for ensuring that all research team members with access to human research data have completed training in the protection of human research subjects according to the IRB educational policy.

E. Penn State Hershey investigators are responsible for reporting breaches in confidentiality of research data (such as loss of or inappropriate access to Level 2 human research data) promptly to the IRB according to the IRB standard operating procedures for reportable new information. In addition, investigators must report incidents involving identifiable health information to the Penn State Hershey Privacy Officer at (717) 531-2081.

F. Penn State Hershey investigators are responsible for contacting ORA or OTD to negotiate a written data transfer agreements if the research project involves any transfer of human research data to and/or from any third party, whether an external sponsor or external investigator.

II. IRB Responsibilities

A. The IRB Chair or his/her designee review the data security and integrity plan for research studies during initial review.

B. The possible determinations the IRB can make regarding the data security and integrity plans include:

1. Data security and integrity plan meets requirements and may be approved as submitted;

2. Data security and integrity plan requires modification to secure approval; or

3. Data security and integrity plan requires review by Penn State Hershey IT Security Group or technical experts for consideration of a variance or recommended revisions.

C. The IRB Chair or designee, documents his/her initial determinations regarding the data security and integrity plan on the IRB reviewer checklist. If review by the IT Security Group is required, an ancillary review activity is set in the IRB database system and approval of the study is granted after the IT Security Group has approved the study's security and integrity plan.

D. The approval memo for the study confers the final approval of the data security and integrity plan by the IRB. For exempt research involving human research data, the exemption determination memo confers acceptance of the data security and integrity plan by the IRB.

III. HSPO Responsibilities

A. An experienced IRB Coordinator reviews the submission for completeness and assigns it to an IRB Chair or designee for review.

IV. Office of Research Affairs and Office of Technology Development Responsibilities

A. The ORA and the OTD negotiate data agreements in accordance with the Standard Operating Procedures of the applicable office.

Appendix A

Level 1 – De-identified research information about people and other non-confidential research information

Examples of Level 1 information

- De-identified data collected for a research study with no regulatory or contractual requirements
- Data consisting of publicly available information

Data security recommendations for hardcopy (paper) data storage

- Research data forms should be stored securely in a controlled environments, e.g., at a Penn State College of Medicine or Penn State Hershey Medical Center facility.

Data security recommendations for electronic data storage

- Good computer use practice that meets the following requirements should be used when storing Level 1 research information and access should be limited to those individuals who have a specific research need to access the information. These requirements include making use of complex passwords, not sharing accounts, and limiting system accounts to those with a specific need.
- All portable media are physically secured when not in use either in a locked office or using lock-down cables
- Servers should have access controls
- Electronic devices may be disposed of following deletion of files or disposal of documents in regular trash

Data transfer/sharing requirements and recommendations

- Any transfer of Level 1 human research data outside of PSCOM/PSHMC requires a written agreement between PSCOM/PSHMC and the external institution unless the external institution is another campus of The Pennsylvania State University or if the external entity would not be able to enter into an agreement (e.g. National Institutes of Health specific policies associated with the 3D print Exchange or Genomic Data Sharing). If an investigator believes there is a situation where an external entity would not be able to enter into a data transfer or data use agreement the investigator should contact OTD for consideration and evaluation. These agreements are negotiated by the ORA and/or the OTD. Investigators are responsible for contacting these offices for a data transfer agreement.
- Conveyance of hardcopy research data forms should be double-wrapped so that damage to the outer container alone does not expose data and the delivery should occur using a secure chain of possession, such as commercial carrier or hand-delivery by a member or agent of the research team.
- Data may be transferred by unprotected e-mail.

Appendix B

Level 2 – Information about individually identifiable people

Examples of Level 2 information

- Data that include identifiable health information (PHI) collected for a clinical trial
- Data that include identifiable sensitive non-health information (PII), such as test scores or student record information, collected as part of an educational research project
- Data that include identifiable non-sensitive research information linked to social security numbers
- Data that include identifiable non-health, non-sensitive information collected as part of non-health-related survey research, interview or focus group research or education research
- De-identified data collected for a research study with regulatory or contractual requirements for data security

Data security requirements for hardcopy (paper) data storage

- Hardcopy research data forms and/or linking code lists must be stored securely in a controlled environments, e.g., at a Penn State College of Medicine or Penn State Hershey Medical Center facility unless a variance is granted by the IRB based on the recommendations of the IT Security Group.
- Hardcopy research data forms and/or linking code lists must be stored in a locked file cabinet or limited access storage area (e.g., a locked room) when not in use.
- Records must be maintained identifying who has or had keys that allow access to the hardcopy Level 2 information.
- Paper and other non-electronic copies must be shredded when no longer needed

Data security requirements for electronic data storage

- Level 2 information must be stored on the following electronic devices unless a variance is granted by the IRB:
    - Secure file server operated, supported and maintained by the Information Technology (IT) department or the Department of Public Health Sciences (PHS).
    - A secure data base server operated, supported and maintained by IT or PHS, e.g., REDCap or Oncore.
- Any removable media that is tracked, inventoried and systematically managed may only be used for either long-term archival storage of Level 2 information or conveyance to another party.
- A device not explicitly listed above is not deemed acceptable for storage of Level 2 information unless a special exception is granted by the IRB based on the recommendations of the IT Security Group.
- Level 2 information may not be stored, temporarily cached or otherwise accessed in a way that creates a local copy of the data on so-called personal devices such as Personal Digital Assistants, USB-based portable devices (e.g., thumb drives, flash drives, or jump drives) or non-Penn State owned and managed devices of any kind (e.g., home computers, personal laptop computers, public computers).
- Remote displaying is permitted for remote access using applications, such as Citrix or Remote Desktop, where there are no persistent data copies when the programs are remotely displayed. Applications, such as most Email clients, which open an attachment by making a local copy of that

document are not acceptable because a local cached copy of the document can persist on the user's computer indefinitely.

- Desktops and devices must be physically secured, including locked offices and/or locked facilities with access restricted to study personnel and their guests.
- Electronic devices must be set to automatically log-off and lock after defined periods of inactivity.
- Access Controls/Authorizations
    - The principal investigator must maintain a list of the individuals or the categories of people who are permitted to have access to Level 2 information.
    - Users' access to Level 2 electronic data must be removed if they no longer have a reason under the access policy to access the information, e.g., they change jobs or leave the institution.
    - Access to Level 2 electronic information must be logged. The logs must include the identity of the user, the time and the function (login or logout).
- Level 2 information may be re-classified as Level 1 information if all of the following conditions are met:
    - All HIPAA-specified identifiers are removed;
    - It is reasonable to expect that individuals cannot be identified through deductive means (the advice of a biostatistician should be sought to ensure this requirement); and
    - There are no agreements, contracts, rules or laws that regulate the use, storage, transmission, handling or disclosure of the de-identified information.
- Data should be routinely backed up and the back-up copy physically secured.
- Devices must undergo secure deletion of the disc at the end of life of the device or prior to recycling.

<u>Data transfer/sharing requirements</u>

- Level 2 information must be de-identified before sharing the information with Penn State Hershey members of the research staff whenever the identifying information is not necessary. All 18 HIPAA-specified identifiers must be removed or date-shifted per Information Technology Standard for de-identification. *If all 18 HIPAA-specified identifiers are removed or date-shifted per Information Technology Standards the data will then be considered Level 1 information. Please refer to the Level 1 information in Appendix A.*
- Any transfer of Level 2 human research data to external researchers must have all 18 HIPAA identifiers removed or date-shifted per Information Technology Standards before being transferred unless subjects have given authorization to do so.
    - This data transfer requires a data transfer agreement as negotiated by ORA or OTD.
    - The mechanisms used for transfer must be approved by the IT Security Group.

- No PHI or PII may leave PSCOM/PSHMC unless subjects have given written authorization to disclose their PHI/PII to specific external entity(ies) or the data are a limited data set.
- Any transfer of Level 2 human research data to a third party (whether an external sponsor or external investigator) requires a written agreement between PSCOM/PSHMC and the external institution. These agreements are negotiated by the ORA and/or the OTD. Investigators are responsible for contacting these offices for a data transfer agreement and adhering to all policies.
- Conveyance of hardcopy research data forms should be double-wrapped so that damage to the outer container alone does not expose data and the delivery should occur using a secure chain of

possession, such as commercial carrier or hand-delivery by a member or agent of the research team.

- Electronic transmission of Level 2 information requires encryption with at least the same level necessary to transmit other HIPAA-regulated data as outlined in HMC policy C-37 HAM. Level 2 information may only be transferred electronically in an encrypted state according to the Penn State Hershey Information Technology standards and practices as of the time of data transfer. Conveyance of portable media must occur using a secure chain of possession, such as commercial carrier or hand-delivery by a member or agent of the research team.

Appendix C

Data Integrity for Human Research Data

The following are examples of measures that may be used in data security and integrity plans to ensure the integrity of the human research data.

- Data entry performed twice by two different individuals when transcription errors are possible.
- Edit checks (time-of-entry contextual and programmatic evaluation of entered data)
- Random, internal quality and assurance auditing by a person other than the individual who performed the original entry

If an institutionally-supported computer is being used to store human research data the principal investigator must ensure that backup copies of human research data are periodically created and stored in a safe and recoverable location. If the human research data is stored on an IT or PHS supported server, backups can be assumed.

- Backup copies if necessary should be maintained in a location that would not be affected if the primary location were destroyed by a catastrophic event.
- The frequency and storage location of backups should be commensurate with the value of the human research data.
- Backups for Level 2 information must be protected according to the requirements described for original Level 2 information.

Appendix D

18 Identifiers as specified by the HIPAA Privacy Rule

The following is a list of elements considered to be identifiers according to HIPAA regulations (45 CFR 164 Security and Privacy regulations, 164.514 b(2)). These elements may be identifiers of the research subject or of the relatives, employers or household members of the subject.

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images, and
18. Any other unique identifying number, characteristic, or code

* In addition to these 18 identifiers, whole genomic sequence data are treated in the same manner as HIPAA identifiers.

Version Date: 11/19/2014

Most recent changes:

- November 19, 2014 – Revisions to the use of a DUA for level 1 data
- November 06. 2014 – Revisions to entire document including collapsing data into two levels in place of three.

- December 12, 2011 - Revised definitions of Level 1, 2 and 3 data with regard to coded datasets and code lists.

Revision History:

- Revision November 19, 2014
- Revision November 6, 2014
- Revision December 12, 2011
- Original November 8, 2011