GUIDANCE FOR DATA HANDLING AND PROTECTION

DATA PROTECTION - WHY AND HOW

The HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule establishes the conditions under which protected health information (PHI) may be used or disclosed by covered entities for research purposes. Research is defined in the Privacy Rule as, “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.”

The U.S. Department of Health and Human Services issued new regulations in 2009 requiring health care providers, health plans and other entities covered by HIPAA to notify individuals when their PHI is breached. Recently, a Connecticut State Attorney General filed an action against a HIPAA "covered entity" that was charged with a serious data breach after a computer disk drive, containing personal information of over 500 individuals, was stolen and the company failed to take appropriate actions. The company was fined $250,000 and was required to develop and implement a “corrective action plan.” This legal action sends a strong message to all users of private health information about their profound responsibilities to protect health and medical records.

Thus, it is imperative that students engaged in an MUSC online or distance education program store research data in a secure location. The best option to protect against breaches is to collect and store data that is de-identified. However, this may not always be a feasible option due to the design of the research. If the study requires the collection and storage of identifiable PHI, please note the following:

1. The MUSC IRB prohibits the use of identifiable databases containing PHI. Information in databases must be stored in a de-identified format.
2. MUSC strictly prohibits the use of portable devices (e.g. thumb drives, flash drives, CDs, PDAs, laptops) for identifiable PHI.
3. Students can access MUSC servers from off-site locations via the MUSC virtual private network (VPN) for secure storage of PHI.
4. The REDCap database is an additional option for the storage of PHI on secure MUSC servers.

HOW DO I KNOW IF I AM COLLECTING “IDENTIFIABLE PHI”?  

- What is Protected health information (PHI)?
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium by a Covered Entity or its Business Associate
- What is “individually identifiable health information”?
  - Health information, including demographic information
  - Relates to an individual's physical or mental health or the provision of or payment for health care
  - Identifies the individual
- What is not PHI?
  - Employment records of Covered Entity
  - Family Educational Rights and Privacy Act (FERPA) records
De-identification of PHI

- Removal of certain identifiers so that the individual who is subject of the PHI may no longer be identified
- Application of statistical method or
- Stripping of listed identifiers such as:
  - Names
  - Geographic subdivisions < state
  - All elements of dates
  - SSNs, etc.

There are also additional standards and criteria to protect individual's privacy from re-identification. Subject identifiers must not be used as a code to link data to individual subjects. The code must be a random linking code. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual. For example, a participant’s initials cannot be used as a linking code nor can the unique code include the last four digits (in sequence) of the social security number. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable is there was a way to identify the individual even though all of the 18 identifiers were removed.

List of 18 Identifiers:

1. Names;
2. All geographical 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. Phone 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 (note this does not mean the unique code assigned by the investigator to code the data)
Minimum Human Research Protections Programs (HRPP) Standards for the Collection, Storage, and Use of Subject Identifiers for Human Subjects Research

IRB applications require investigators to address issues related to subject privacy and confidentiality, HIPAA, and information security. Before filling out IRB applications, please keep in mind the following HRPP minimum standards:

- Do not collect any subject identifiers you do not need.
- Remove/destroy subject identifiers as soon as they are no longer needed, subject to MUSC guidance on records retention. (MUSC IRB Policy 10.2: Record Retention Policy [http://research.musc.edu/ori/irb/policies.html](http://research.musc.edu/ori/irb/policies.html))
- Restrict physical access (i.e. locked office, locked file cabinet) to any area or computer system that contains subject identifiers.
- Restrict electronic access (i.e. password protected) to any computer system that contains subject identifiers.
- Do not transmit PHI by email unless using Ironport.
- Subject identifiers should never be stored on laptops, PDA’s, flash drives or other portable devices.

The MUSC IRB prohibits the use of identifiable databases containing PHI. Subject identifiers must be removed from data files, and must be encrypted if stored electronically. Identifiers must be stored in a physically separate and secure location from the data files, and associated with data files through a code that is also stored in a separate and secure location. Subject identifiers and contact information may not be distributed outside of MUSC without the specific informed consent of the subject and the approval of the IRB.

**Example description of de-identified data storage & protection plan for IRB application**

*Data Storage & Protection Plan.* The master list linking participant names to the study IDs will be maintained by the PI and kept in locked cabinets in a locked office (or on a password protected computer and/or server) that can only be accessed by the PI and approved study staff. Data entered into the study database will only identify a participant via the study ID code. All communications among study personnel relative to individual study participants will be via the de-identified study ID. The study database will meet MUSC requirements for data security and confidentiality, including use of anti-virus software and protection against unauthorized access.

See MUSC IRB Policy 4.13: Privacy and Confidentiality ([http://research.musc.edu/ori/irb/policies.html](http://research.musc.edu/ori/irb/policies.html))

For an overview of Principal Investigator Responsibilities, See MUSC IRB Policies 5.1 and 5.2 ([http://research.musc.edu/ori/irb/policies.html](http://research.musc.edu/ori/irb/policies.html))