MUSC
Medical University of South Carolina

I. Policy

A. Introduction

All organizations involved in conducting human subjects research must ensure procedures are in place to protect the privacy of subjects and maintain the confidentiality of data.

B. Federal Regulations

The IRB will review proposed research activities in accordance with HIPAA privacy and security regulations at 45 CFR Parts 160, 164.The IRB will determine whether adequate procedures are in place to protect the privacy of participants and to maintain the confidentiality of the data in accordance with federal regulations at 45 CFR 46, 21 CFR 56 and 38 CFR 16, as applicable, or the regulations of federal agencies and applicable state laws.

C. Guidance on Additional Requirements of Federal Funding Agencies

Please note that protocols conducted by MUSC and sponsored by any of the following federal agencies

- the Department of Defense (DOD),
- Department of Education,
- Department of Energy,
- Department of Justice (DOJ) / National Institute of Justice (NIJ) and Bureau of Prisons (BOP) or
- Environmental Protection Agency (EPA)

have additional operational and review requirements. In addition, protocols following the International Committee on Harmonisation – Good Clinical Practices (ICH-GHP) have additional requirements. Further information available on the MUSC IRB Resources & Guidance Webpage <http://research.musc.edu/ori/irb/resources.html>)

D. IRB Responsibilities

The IRB must review how investigators are obtaining information and the participant's expectations of privacy regarding the information obtained by the investigator. Investigators must have appropriate authorization to access the subject's or the participant's information.

The IRB must also determine if appropriate protections are in place to minimize the likelihood that confidential information will be divulged. The level of confidentiality should be commensurate with the potential harm from inappropriate disclosure

E. Pertinence of Data Collected

Only data pertinent to answering an IRB approved research question will be collected for human research purposes. When research involves the collection of personally identifiable, sensitive data, consideration should be given regarding the need for obtaining a Certificate of Confidentiality. As detailed on the US DHHS *Certificates of Confidentiality Kiosk* Website, "Certificates of Confidentiality are issued by the National Institutes of Health (NIH) to protect identifiable research information from forced disclosure." Further information may be obtained by reference to the website listed in the References section of this policy guide

F. Prohibition on Use of Subject Identifiers

Unless explicitly approved by the IRB, subject identifiers must not be used as a code to link protected health information to individual subjects. For example, use of consecutive numbers is acceptable.

The following are considered subject identifiers not to be used as a code to link information to a participant:

1. Names
2. Address - (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: a) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and b) 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 for years) related to an individual - including, admission dates, discharge dates, date of death, birth dates, ages >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 >90
4. Telephone Numbers
5. Fax Numbers
6. E-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
13. Device Identifiers and Serial Numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) Address Numbers
16. Biometric Identifiers (e.g. finger or voice prints)
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

G. Requirements for Appropriate Data Storage Techniques

Electronic research data that is individually identifiable should be, to the extent possible, only stored in appropriately protected repositories/ databases with formally established and authorized information systems. In exceptional circumstances, there may be an unavoidable requirement to store electronic research data on an end-user device (including but not limited to: desktop computers, laptops or tablets). In these circumstances, the Investigators shall meet the baseline data protection requirements outlined in the MUSC information security-data protection policy (http://www.musc.edu/security/policy/data-protection.shtml).

For example, if a database containing identifiers is stored anywhere other than an MUSC network drive, the database must be encrypted using the OCIO approved encryption technology.
http://www.musc.edu/infoservices/endpointsecurity/encryption.htm

Ideally, hardcopy documents with identifiers, such as consent forms and HIPAA authorizations should be stored in a physically separate and secure location from the research data files and associated through an approved linking code.

If data that includes participant identifiers must be transmitted over an untrusted network (including any public network), then the data must be encrypted during transmission, using for example SSL encryption, a secure file transfer protocol, or MUSC SecureMail. For more information on MUSC SecureMail, please see:
http://www.musc.edu/infoservices/exchange/securemail.html

Participant identifiers and contact information may only be distributed outside MUSC with mechanisms including, but not limited to: specific informed consent of the participants and IRB approval, via Business Associates Agreement and/or Data Use Agreement. *For more information please contact the IRB*

H. Study Monitor Access to Research Participant's Study and Medical Records

When site visits are conducted by study monitors, investigators are obligated to maintain the confidentiality of participants enrolled in the study. Access to confidential information must be controlled and managed in a way that does not permit unauthorized access. Access must be authorized by the IRB as part of an approved and authorized by the research participant. Unsupervised access to the complete medical record, access to databases, and access to any other electronic medical record source that contain Protected Health Information which is not related to the research is not allowed.

Study Monitors are not permitted to conduct their visits in an area where unrelated case report forms with subject identifiers and/or other privileged study information (e.g. study materials or trial data belonging to other sponsors) or patient information might be viewed.

II. Definitions

Definitions of the following terms used in this section may be found in Section 1.3 - Definitions of the MUSC HRPP Program

A. Privacy

B. Confidentiality

C. Sensitive information

D. Private information

E. Identifiable information

III. Procedures

A. The principal investigator will describe the nature of the data to be collected and the plan to protect participant privacy and maintain data confidentiality in the research protocol. This description will include identification of who will have access to data collected, how information will be disclosed, the methods of accessing, storing, and how data will be safeguarded to maintain confidentiality. Any risk to disclosure of identifiable private information of participants and provisions to protect the participant's identity during the course of the research must also be described.

B. When research involves activities or information of a particularly sensitive or potentially damaging nature, the IRB, in collaboration with the principal

investigator, will determine whether the investigator should seek a Certificate of Confidentiality.

C. The informed consent document and the HIPAA Authorization will specify what collected data will be shared with others, how these data will be shared, and with whom the data will be shared.

D. The IRB will determine if the data being collected are relevant to answering the research question and the adequacy of the confidentiality and privacy protection plan.

E. Clinical Databases - Requirements for IRB Approval & HIPAA Authorization

1. Clinical Databases

   a) Developed for clinical purposes of tracking and monitoring care (not subject to IRB review or approval).

   b) Allowed by the covered entity's HIPAA notice of privacy practices.

   c) If an individual wants to query the database for research:

      (1) IRB approval is required;

      (2) HIPAA de-identification certification or a HIPAA waiver* is required and;

      (3) research must present **minimal risk** to privacy of the individuals.

2. Clinical Databases with Possibility of Future Research

   a) Developed for clinical purposes of tracking and monitoring care but may be used for research purposes at a later time.

   b) Allowed by the covered entity's HIPAA notice of privacy practices.

   c) If an individual wants to query the database for research:

      (1) IRB approval is required;

      (2) HIPAA de-identification certification or a HIPAA waiver is required; and

      (3) research must present **minimal risk** to privacy of the individuals.

3. Clinical Databases for Research

a) Developed for the express purpose of research with specific research questions not identified as of yet.

b) Requires IRB approval **before** the database is initiated.

c) Requires informed consent and HIPAA authorization from patients/participants to be included in the research database.

d) When an individual wants to query the database for research:

(1) IRB approval is required relative to the specific protocol, and

(2) a HIPAA authorization or a waiver of authorization is required.

Federal guidance regarding the HIPAA regulations states:

"**When a (research) database is maintained, any use of the database for a particular research purpose will require a new, protocol-specific authorization or waiver of authorization as well as a research protocol specifically describing the new study which must be approved by the IRB**."

* A HIPAA waiver can only be approved if the IRB assesses the PHI to be used as presenting no more than minimal risk to the privacy of participants. A HIPAA waiver may limit use of the available data; the IRB decides which of the available data elements may be used.

F. Security Considerations in an Electronic Data Protection Plan. A research study using identifiable protected health information must specify an Electronic Data Protection Plan and contain the following elements.

1. Determination of where the data will be stored

a) Desktop Computer - computer- security issues must be addressed

b) Network Drive - Downloaded/downloadable data

(1) Frequency and timing of downloads

(2) Purpose for Downloads

c) Mobile Media - security issues for each type of mobile media must be addressed

(1) Laptop computer

(2) PDA

(3) Thumb Drive

(4) Portable hard drive

d) Permanent Media- security issues for each type of media must be addressed

(1) CD

(2) DVD

G. Memorandum of Understanding

In aspects where the MUSC IRB is being utilized by the Ralph H. Johnson VA Medical Center, both parties will abide by the agreements set forth in the current "Memorandum of Understanding Between The Ralph H. Johnson VA Medical Center And The Medical University of South Carolina Concerning Utilization of the Medical University of South Carolina's Institutional Review Boards".

VA investigators must follow the procedures established in VHA Handbook 1200.12 "Use of Data and Data Repositories in VHA Research" for the use of data for VHA research purposes, the storage of VHA research data and the development of VHA research data repositories.

H. National Institute of Justice (NIJ) Protocol

1. All projects are required to have a privacy certificate approved by the NIJ Human Subjects Protection Officer.

2. All researchers and research staff are required to sign employee confidentiality statements, which are maintained by the responsible researcher.

I. Bureau of Prisons Protocols

1. A non-employee of the Bureau may receive records in a form not individually identifiable when advance adequate written assurance that the record will be used solely as a statistical research or reporting record is provided to the agency.

2. Except as noted in the consent statement to the subject, the researcher must not provide research information that identifies a subject to any person without that subject's prior written consent to release the information. For example, research information identifiable to a particular individual cannot be admitted as evidence or used for any purpose in any action, suit, or other judicial, administrative, or legislative proceeding without the written consent of the individual to whom the data pertain.

3. Except for computerized data records maintained at an official Department of Justice site, records that contain non-disclosable information directly traceable to a specific person may not be stored in, or introduced into, an electronic retrieval system.

4. If the researcher is conducting a study of special interest to the Office of Research and Evaluation (ORE) but the study is not a joint project involving ORE, the researcher may be asked to provide ORE with the computerized research data, not identifiable to individual subjects, accompanied by detailed documentation. These arrangements must be negotiated prior to the beginning of the data collection phase of the project.

IV. References

A. U.S. DHHS Certificates of Confidentiality Kiosk

B. HIPAA - http://www.hhs.gov/ocr/privacy/

C. http://www.charleston.va.gov/research/Research.asp

D. MUSC OCIO - http://www.musc.edu/security/policy/data-protection.shtml