Policy Name: **Privacy and Confidentiality**			
Approved			**Date: 11/01/08**
Effective Date: 12/01/09	**Page 1 of 6**	**Section: HRPP 4.13**	**Policy Number: N/A**
Replaces Policy: Effective 02/20/09			**Dated: N/A**

I. POLICY

A. Introduction

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

B. Federal Regulations

The IRB will determine whether adequate procedures are in place to protect the privacy of subjects 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. The IRB will also review proposed research activities in accordance with HIPAA privacy regulations at 45 CFR Parts 160, 164 and security.

C. IRB Responsibilities

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

D. 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.

E. Prohibition on Use of Subject Identifiers

Subject identifiers must not be used as a code to link data to individual subjects. The code must be a random linking code. If subject identifiers, such as date of birth, are included in the database, these identifiers 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

The following are considered subject identifiers:

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

F. Requirements for Appropriate Data Storage Techniques

Subject identifiers should not be stored on laptops, PDAs', flash drives, cell phones or other portable devices. If there is a necessity to use

portable devices for the initial collection of subject identifiers, the data files must be encrypted and the identifiers transferred to a secure system as soon as possible. Subject identifiers transmitted over public networks must be encrypted.

Subject identifiers and contact information may not be distributed outside of MUSC without the specific informed consent of the subjects and the approval of the IRB.

G. 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 subjects 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 study 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 subject 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 subjects and provisions to protect the

participant's identify 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
    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.
        (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 "maybe" will 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.
        (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/subjects 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 by the covered entity, 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 an 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 subjects. 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

1. Determination of where the data will be stored

    a) Desktop Computer – specific computer
    b) Network Drive - Downloaded/downloadable data
        (1) Frequency and timing of downloads
        (2) Purpose for Downloads
    c) Mobile Media – security issues must be addressed
        (1) Laptop computer
        (2) PDA
        (3) Thumb Drive
    d) Permanent Media
        (1) CD
        (2) DVD

2. Data Storage Scheme
    a) Data Elements separate from master list of linked codes recommended

III. REFERENCES

A. U.S. DHHS Certificates of Confidentiality Kiosk