

4.0 Privacy and Confidentiality

As required by federal regulation, the HSC reviews the investigator's plans to protect the privacy of subjects and maintain the confidentiality of data. Researchers proposing expedited or full-review research must provide information on these plans in the HSC application form.

The HSC considers privacy protections as those relating to ensuring a subject's right to protect access to his/her person or access to personal information. The HSC considers confidentiality provisions as those relating to appropriate controls on the disclosure of study information. Unless otherwise authorized, study information must be disclosed only to approved members of the research team, study sponsors, KUMC offices and committees that oversee research, and federal regulatory agencies.

The HSC reviews the investigator's plans to ensure privacy and confidentiality at the time of initial review. Proposed changes to the research also are evaluated for impact on the subjects' privacy and confidentiality. A privacy violation or a breach of confidentiality is considered an unanticipated problem and must be promptly reported to the HSC.

4.1 General privacy standards

- I. Privacy protections must be considered during the identification and approach of potential subjects and during the conduct of the research.
- II. When identifying potential subjects, KUMC researchers will comply with applicable standards in the HIPAA Privacy Rule, as described below.
- III. When approaching or contacting potential subjects, the first recruitment contact should come from an individual who has a treatment, professional or prior research relationship with the patient. Privacy is further respected by conducting the consent interview in a non-public setting, to protect the conversation from being overheard.
- IV. During the conduct of the study, the research team should continue to provide privacy protections to subjects. Examples of protections may include conducting study visits in a non-public setting, same-gender interviewers for questions on sexuality, and limiting the presence of accompanying friends or family members during study visits.

4.2 HIPAA Privacy Requirements

- I. KUMC is a covered entity under the HIPAA Privacy Rule. Therefore, KUMC researchers must fulfill HIPAA requirements for the use of protected health

- information in research. Protected health information (PHI) includes health information that is associated with at least one of eighteen identifiers that make the information “individually identifiable.” The eighteen identifiers include name, address, SSN, date of birth, dates of health care, medical record number and other elements specified in the Privacy Rule.
- II. In Kansas City, the HSC serves as the privacy board for KUMC. In Wichita, privacy board functions are administered by the community hospitals whose records are being used for the research, except for the MPA clinics.
 - III. The Privacy Rule allows PHI to be used for human subjects research under one of the following conditions:
 - A. Permission is granted by the patient, through a written authorization form;
 - B. The information is completely de-identified and no longer governed by the HIPAA Privacy Rule;
 - C. The information is compiled into a “limited data set” and a data use agreement is executed;
 - D. The activity qualifies as “preparatory to research”;
 - E. A waiver of privacy authorization is approved by the HSC.
 - IV. On the Kansas City campus, representatives of the KUMC HIPAA Compliance Office review each new application, each study amendment and each re-certification, to ensure compliance with the Privacy Rule. As needed, HIPAA personnel issue provisos that must be satisfied prior to HSC approval of the project. HIPAA provisos are sent to the investigator along with any HSC provisos. On the Wichita campus, HSC members provide the HIPAA review. As needed, Wichita HSC members or compliance staff consult with the Kansas City HIPAA Compliance Office.
 - V. When HSC requires written informed consent, the required elements of a HIPAA privacy authorization are incorporated into the informed consent document.
 - VI. Recruitment of subjects must comply with HIPAA standards. These requirements are further discussed in SOP 8.2-Use of Medical Records for Recruitment.

4.3 Certificates of Confidentiality

- I. The HSC advises investigators to obtain a Certificate of Confidentiality if the research involves sensitive topics such as illicit drug use, illegal activities, genetic data and HIV status.
- II. Information about the provision of the Certificate of Confidentiality, and the limits of its protection, are included in the informed consent document.

4.4 Physical Security for Research Data

- I. All KUMC researchers are required to ensure confidentiality by providing physical security for identifiable research information. Appropriate measures include limiting the extent of identifiers on data collection forms (when feasible) and providing locked file cabinets for storage.

4.5 Electronic Security for Research Data

- I. To comply with the HIPAA Privacy Rule and the HIPAA Security Rule, researchers must provide adequate electronic security for identifiable research data. In April 2005, KUMC adopted the HIPAA Policy on Research using Electronic Protected Health Information. The policy is found at: http://www.kumc.edu/hipaa/docs/HIPAA_Policy_on_Research_using_Electronic_Protected_Health_Information.pdf. The policy covers the creation, use and receipt of data, data access, data storage and data transmission.
- II. To maintain the confidentiality of electronic research data, investigators should store data preferentially on university network drives for firewall protection. When data are stored on a mobile device or storage media, data must be encrypted. Transmission of electronic data over the internet must employ a dedicated transmission line, virtual private network, encrypted website or secure file transfer protocols. When electronic storage media are used for data exchange, the media must be password-protected. Passwords must be sent to the data recipient in a separate secure communication.

References:

45 CFR 46.111

45 CFR Parts 160 and 164