IRB SOP 04.0 Privacy And Confidentiality, 2018 Requirements

Purpose:
As required by federal regulation, the IRB reviews the investigator's plans to protect the privacy of subjects and maintain the confidentiality of data.

Responsible Personnel:
The IRB reviews the investigator's plans to ensure privacy and confidentiality at the time of initial review in accordance with requirements of the Common Rule.

Background:

Regulation and Guideline Reference(s):
45 CFR 46.111
45 CFR Parts 160 and 164

KUMC References:
CR SOP 17.1 Confidentiality, Privacy and Security of Data
Data Classification Policy
Designation as a Hybrid Entity Under HIPAA
Mobile Device Security
Sensitive Information in Electronic and Paper-based Systems
4.0 Privacy and Confidentiality

As required by federal regulation, the IRB reviews the investigator's plans to protect the privacy of subjects and maintain the confidentiality of data. The IRB considers privacy protections to be those relating to ensuring a subject's right to protect access to his/her person or access to personal information. The IRB considers confidentiality provisions to be 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 IRB reviews the investigator's plans to ensure privacy and confidentiality at the time of initial review in accordance with requirements of the Common Rule and institutional policy. Proposed changes to the research also are evaluated for impact on the subjects' privacy and confidentiality. A privacy violation or a breach of confidentiality related to research data is considered an unanticipated problem and must be promptly reported to the IRB and other institutional authorities.

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 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.

III. 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.

IV. When using protected health information to identify potential subjects, KUMC researchers will comply with applicable standards in the HIPAA Privacy Rule, as described below.

4.2 HIPAA Privacy Requirements

I. KUMC has components that are covered under the HIPAA Privacy Rule. Therefore, KUMC researchers within those components must fulfill HIPAA requirements for the use or disclosure 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. The KUMC IRB may serve as the privacy board for both the Kansas City and Wichita campuses. Studies conducted on the Wichita campus may be under the purview of privacy boards at the community hospitals whose records are being used for the research.

III. The KUMC IRB may serve as the privacy board for external sites that are relying on the IRB. A written
request from the site is required and is obtained during the collection of local context information from the external site. Additional details about the evaluation of local context information is discussed in SOP 13 IRB Review when KUMC Conducts Multi-Site Research.

IV. The Privacy Rule allows PHI to be used or disclosed 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 IRB.

V. HIPAA provisos are sent to the investigator along with any IRB provisos, and they must be satisfied prior to IRB approval of the project.

VI. When the KUMC IRB requires written informed consent, the required elements of a HIPAA privacy authorization are incorporated into the informed consent document.

VII. When IRB determines that waiver of documentation of consent is appropriate, the information letter or verbal script will address HIPAA authorization elements as applicable. The HIPAA requirements for signature, receipt of a signed copy of the authorization, and written notification for revoking authorization are typically waived because minimal risk research is eligible for alteration of the authorization, as outlined in 45 CFR 164.512(i).

VIII. Research proposals involving only secondary research using information or biospecimens typically qualify for a waiver of privacy authorization. For each proposal, the IRB/Privacy Board confirms that use of PHI for secondary research satisfies the HIPAA standards for minimal risk by reviewing the investigator's plans for protecting identifiers from improper use and disclosure, plans to destroy identifiers at the earliest opportunity and assurances that PHI will not be reused or disclosed for another purpose. Because there is no interaction with research subjects, secondary research is automatically deemed to meet the waiver criteria that the (1) research cannot practicably be conducted without the waiver and that (2) the research cannot practicably be conducted without access to PHI because the information required for the research is located in the patients' medical record.

IX. For studies involving interaction with the participant, access to the participant's medical record must be authorized in writing to meet requirements of Kansas state law.

X. 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 National Institutes of Health (NIH) announced on September 7, 2017 that all NIH-funded research in which subjects can be identified will automatically be protected by a Certificate of Confidentiality. Upon request, certificates also may be issued for research from other federal agencies or non-federal sources.

II. Restrictions on the disclosure of the research information apply not only to the primary grant recipients but also to all subawardees and anyone who receives a copy of the identifiable information. NIH maintains a website that provides details about the requirements.

III. NIH expects subjects to be notified about these protections. Suggested language to describe these protections is included in the KUMC IRB's consent form templates.
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 posted in the KUMC online policy library. The policy covers the creation, use and receipt of data, data access, data storage and data transmission. Other university policies about computer security, sensitive information, and storage on mobile devices apply to all identifiable research data.

II. To maintain the confidentiality of electronic research data, investigators must store identifiable data on designated university network drives for firewall protection. When data are stored on a mobile device or storage media, data must be encrypted. Transmission of identifiable 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.

III. Additional requirements apply when study data will be stored on a mobile device. Investigators must describe how the data are secured and what information would be accessible if the device were lost or stolen. The informed consent document will describe risks related to electronic data as applicable.

IV. IRB application forms contain questions about provisions for data security. Representatives of the HRPP communicate regularly with staff from the KUMC Information Security Office to ensure appropriate security measures are utilized by researchers, use of new software meets institutional standards for security, and new security threats are identified. When advised by the Information Security Office, the HRPP holds final project approval until data security concerns are resolved.

References:

45 CFR 46.111
45 CFR Parts 160 and 164

Attachments:

Approval Signatures

<table>
<thead>
<tr>
<th>Approver</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steffani Webb: Vice Chancellor for Administration</td>
<td>12/10/2019</td>
</tr>
<tr>
<td>Lisa Hoebelheinrich: Chief Compliance Officer</td>
<td>12/10/2019</td>
</tr>
<tr>
<td>Annie Fors: QA Director</td>
<td>12/3/2019</td>
</tr>
<tr>
<td>Karen Blackwell: Director HRPP</td>
<td>11/26/2019</td>
</tr>
<tr>
<td>Kyle Stephens: Assistant Director</td>
<td>11/19/2019</td>
</tr>
</tbody>
</table>
Applicability

KU Medical Center, KU SoM Wichita