UMKC
Office of Research Services

16. Health Insurance Portability and Accountability Act

16.1. Historical Background

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, and DHHS regulations promulgated thereunder with respect to standards to protect patient Protected Health Information (PHI) known as the HIPAA Privacy Rule, impose obligations on the University to protect the privacy of and safeguard of such information. The HIPAA Privacy Rule went into effect on April 14, 2003. While the main impact of the HIPAA Privacy Rule is on the routine provision of and billing for health care, the HIPAA Privacy Rule also affects the conduct and oversight of research. Researchers, Institutional Review Board (IRB) staff and members as well as the Office of Research Services (ORS) must be aware of these requirements.

16.2. Health Care Component

Under the Privacy Rule, any entity that meets the definition of a covered entity, regardless of size or complexity, generally will be subject in its entirety to the Privacy Rule. However, the Privacy Rule provides a means by which many covered entities may avoid global application of the rule, through the hybrid entity designation provisions. This designation will establish which parts of the entity must comply with the Privacy Rule.

Any single legal entity may elect to be a hybrid entity if it performs both covered and non-covered functions as part of its business operations. A covered function is any function where the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse. To become a hybrid entity, the covered entity must designate the health care components (health care component) within its organization. Health care components *must* include any component that would meet the definition of covered entity if that component were a separate legal entity. A health care component *may* also include any component that conducts covered functions (i.e., non-covered health care provider) or performs activities that would make the component a business associate of the entity if it were legally separate. Within a hybrid entity, most of the requirements of the Privacy Rule apply only to the health care component(s), although the covered entity retains certain oversight, compliance, and enforcement obligations. Thus, research components of a hybrid entity that function as health care providers and engage in standard electronic transactions must be included in the hybrid entity's health care component(s), and be subject to the Privacy Rule.

A hybrid entity is not permitted, however, to include in its health care component, a research component that does not function as a health care provider or does not conduct business associate-like functions. For example, a research component that conducts purely records research is not performing covered or business associate-like functions and, thus, cannot be included in the hybrid entity’s health care component.

The University intends to fully comply with its obligations under the HIPAA Privacy Rule. For this reason, UMKC has designated itself as a hybrid entity [see 45 CFR. 164.504(a), 164.504(b), and 164.504(c)] for HIPAA privacy compliance purposes. Furthermore, for HIPAA compliance

purposes, the University has designated the following health care components as being subject to the HIPAA Privacy Rule:

- **University of Missouri Kansas City School of Dentistry (SOD)**, its participating clinicians, staff, and all University employees and departments that provide management, administrative, financial, legal and operational support services to or on behalf of the SOD to the extent that such employees and departments use and disclose PHI in order to provide administrative and support services to the SOD and would constitute a business associate of the SOD.

- **Student Health and Wellness Center**, its participating clinicians, staff and University employees and departments that provide management, administrative, financial, legal and operational support services to or on behalf of the Student Health and Wellness Center to the extent that such employees and departments use and disclose PHI in order to provide administrative and support services to the Student Health and Wellness Center and would constitute a business associate of the Student Health and Wellness Center.

All other departments, personnel, and employees of the University are excluded from the health care component (i.e., they are not subject to the HIPAA privacy requirements).

16.3. Policy

The HRPP/IRB/Privacy Board protects and safeguards PHI created, acquired, and maintained during the conduct of human participant research in accordance with the privacy regulations promulgated pursuant to the HIPAA Privacy Rule, applicable state laws, and the University HIPAA privacy policies.

Under HIPAA, a covered entity must establish a Privacy Board or delegate authority to the IRB to serve as a Privacy Board to review uses and disclosures of PHI in research. The University has designated the IRB to serve as the Privacy Board for research.

The University has designated a Privacy Official who assures the University remains compliant under the privacy regulations within the HIPAA Privacy Rule. The Privacy Official shall review all non-research privacy issues and provide Guidance on research-related privacy issues at the request of the IRB.

16.4. Definitions

Authorization (or "HIPAA authorization"): for HIPAA purposes, is a written document completed and signed by the Individual that allows use and disclosure of PHI for specified purposes, which are generally other than treatment, payment, or health care operations of a covered entity.[45 CFR 164.501 and 164.508].

Coded: means **(1)** Individually identifiable private information (e.g., name or social security number) that would enable the investigator to readily ascertain the identity of the Individual to whom the private information (or specimens) pertains has been replaced with a number, letter, symbol, or combination thereof (i.e., the code); and **(2)** a key to decipher the code exists, enabling linkage of the Individually identifiable private information (or specimens).

Common rule: is a rule of ethics regarding research involving human subjects in the United States. These regulations governing IRB oversight of human subjects research are incorporated into the US Department of Health and Human Services (DHHS) title 45 CFR 46 Subparts A, B, C and D.

Covered entity: for HIPAA privacy purposes, is the term applied to institutions that must comply with the HIPAA privacy and security rule. They include: health plans, health care clearinghouses; and health care providers. [DHHS 45 CFR 160.103; 45 CFR 164.504].

Data Use Agreement (DUA): an agreement between a covered entity and the limited data set (as defined below) recipient that states the limited data set recipient will only use or disclose the patients' PHI for limited purposes.

***De-identified information*:** for HIPAA privacy purposes, health information that does not identify an Individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an Individual. If information is de-identified, it no longer is subject to the Privacy Rule and is exempt from HIPAA. [45 CFR 164.514(a) and (b); 45 CFR 164.502(d)(permitted uses and disclosures of de-identified information)]. De-identified information does not contain any of the 18 identifiers listed in the HIPAA Privacy Rule.

***Disclosure (or "Disclosure of PHI")*:** for HIPAA privacy purposes, a disclosure is the release, transfer, provision of access to, or divulging in any other manner individually identifiable health information outside of the covered entity. [45 CFR 164.501].

***Health information*:** for HIPAA privacy purposes, it means any information, whether oral or recorded in any form or medium, that: **(1)** is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or University, or health care clearinghouse; and **(2)** relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual. [DHHS 45 CFR 160.103].

***Hybrid entity*:** for HIPAA privacy purposes, it is a single legal entity that **(a)** is a covered entity; **(b)** whose business activities include activities covered and not covered under the HIPAA privacy regulations; and (c) that designates health care components that will be subject to HIPAA. [45 CFR 164.103.]

***Individually Identifiable Health Information ("IIHI")*:** for HIPAA privacy purposes, this is information, including demographic information collected from an Individual, that: **(i)** is created or received by a health care provider, health plan, employer, or health care clearinghouse; **(ii)** relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and **(iii)** identifies the Individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. [45 CFR 160.103]. This term should not be confused with ―Individually Identifiable Private Information, which is not covered by HIPAA.

Individually Identifiable Private Information (IIPI): is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information but is not subject to HIPAA as its origination is not from a covered entity.

***Limited Data Set (LDS)*:** for HIPAA privacy purposes, is PHI that excludes specific direct identifiers of the Individual or of relatives, employees or household members of an Individual, but may include city, state, zip code, elements of date and other numbers, characteristics, or codes not listed as direct identifiers. A limited data set can only be used for the purposes of research, public health, or healthcare operations, and disclosed for the purpose of research pursuant to a data use agreement.

***Minimum necessary*:** for HIPAA privacy purposes, this refers to the principle that any access (i.e., obtaining or using PHI by any means or in any medium) to PHI should be limited to the minimum amount of PHI needed to accomplish the intended purpose of the use or disclosure. [DHHS 45 CFR 164.502(b) and .514(d)].

***Preparatory research*:** for HIPAA privacy purposes, preparatory research is the method applied to developing or designing a research study. [45 CFR 164.512(i)(1)(II)].

***Protected Health Information ("PHI")*:** for HIPAA privacy purposes, PHI means IIHI that is transmitted or maintained in any form or medium (i.e., electronic, paper or verbal). [45 CFR 164.501]. PHI does not include IIHI in:

- Education records covered by the family educational right and privacy act, as amended, 20 USC. 1232g;
- Records described at 20 USC. 1232g(a)(4)(b)(iv); and
- Employment records held by a covered entity in its role as an employer.

***Privacy*:** for research purposes, having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

Do not confuse this research term with HIPAA privacy requirements.

***Privacy Board*:** for HIPAA privacy purposes, Privacy Board is the term used to describe a group of members with varying backgrounds and appropriate professional competency as necessary, to review Individual's private rights and related interests for research.

***Use*:** means, with respect to IIHI, the sharing, employment, application, utilization, examination, or analysis of such information within the organization that maintains such information. [45 CFR 164.501].

***Waiver of authorization (or "waiver of HIPAA authorization")*:** for HIPAA privacy purposes, this is a means of requesting approval from an IRB or Privacy Board rather than asking each research subject for an authorization to access PHI. [45 CFR 164.512(i)(1)(i)].

16.5. Effects of HIPAA on Research

Before the Privacy Rule, protection of human subjects in research focused primarily on assuring that the research project was performed ethically and that the human subjects participated on the basis of consent. While the common rule acknowledges the importance of confidentiality, it does not have extensive requirements regarding the matter. Likewise, the FDA regulations governing clinical trials of new drugs and medical devices have some restrictions protecting the confidentiality of human subjects. The Privacy Rule does not make any changes to these research requirements. The HIPAA Privacy Rule supplements research regulations within UMKC's health care components; it does not replace them.

The Privacy Rule also contains several provisions that resemble Federal research provisions and does make reference to those provisions. For example, the common rule contains specific requirements for a composition of an IRB. Similarly, the Privacy Rule contains specific requirements for a Privacy Board. The composition of a Privacy Board is similar to that of an IRB and, effectively, the IRB can easily serve as the Privacy Board for a covered entity.

The HIPAA Privacy Rule includes a number of important requirements that apply to research. Helpful resources for more information on how HIPAA applies to research can be found at:

- NIH HIPAA Privacy Rule booklet for research [see http://privacyruleandresearch.NIH.gov];
- The NIH fact sheet on IRB and HIPAA [see http://privacyruleandresearch.NIH.gov/pdf/IRB_factsheet.pdf]; and
- Impact of the Privacy Rule on academic research, a white paper published by the American council on education [see http://www.nacua.org/documents/HIPAA_111802.pdf].

16.6. Privacy Board

UMKC designates its IRB as the Privacy Board for purposes of institutional determinations of whether PHI created, maintained or stored as a result of Human Subjects Research can be used, accessed, reviewed, or disclosed without subject authorization or pursuant to a waiver or

alteration of subject authorization. UMKC's IRB shall be established and operated consistent with 45 CFR 164.512(i) of the Privacy Rule, which states that:

- Members must have varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on Individuals' privacy rights and related interests;
- Each board must have at least one member who is not affiliated with the covered entity or with any entity conducting or sponsoring the research and who is not related to any person who is affiliated with such entities; and
- Members may not have a conflict of interest regarding the projects they review.

Do not confuse UMKCs IRB/Privacy Board with the Privacy Official. The role of the Privacy Board is solely to determine whether PHI related to Human Subjects Research can be used, accessed, reviewed, or disclosed without subject authorization or pursuant to an alteration of subject authorization. The Privacy Officer is responsible for overseeing and implementing all other HIPAA Privacy compliance requirements for the Institution with respect to the University's Health Care Components.

16.7. Permitted Uses and Disclosures of Research PHI

The Privacy Rule permits covered entities to use or disclose PHI for research purposes when the Individual who is the subject of the information authorizes the use or disclosure. For research, a HIPAA authorization must be sought in addition to consent. The HIPAA authorization also must be sought for other research uses or disclosures of PHI that do not qualify for a waiver of authorization (discussed below).

The Privacy Rule has several special provisions that apply to research authorizations for uses and disclosures of PHI for research purposes. These requirements for UMKC with respect to UMKC's health care components are as follows:

- A **HIPAA authorization** purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the end of the research study; and
- **HIPAA authorization** must be filled out completely and accurately by the investigator, to ensure that all parties who require access to PHI for the research (including sponsors, regulatory agencies, IRBs, etc.) are identified in the form and may receive the information. The **authorization** language may be included in the study consent document or as a stand-alone document and submitted to the IRB for review and approval.
    - **The default position for the UMKC IRB is to have stand-alone consent forms and HIPAA authorizations, although blended forms will be considered for review.**

16.8. Research Under HIPAA

HIPAA defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." [45 CFR 164.501].

16.8.1. Waiver of Authorization for Use or Disclosure of PHI in Research

16.8.1.1. Background

Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research with Individual authorization, or without Individual authorization under limited circumstances. A covered entity may use or disclose PHI for research when presented with documentation that a Privacy Board has granted a waiver of authorization. [See 45 CFR 164.512(i)(1)(i)]. This provision of the Privacy Rule might be used, for example, to conduct records research, epidemiological studies, or other research where de-identified data is unavailable or not suited to the research purpose.

16.8.1.2. Procedure for Uses & Disclosures with an authorization

Unless an exception exists below, researchers must obtain Individual HIPAA authorization to use and/or disclose PHI for research purposes. This HIPAA authorization must contain the core elements required for all HIPAA authorizations.

16.8.1.2.1. Uses and Disclosures of Research PHI without an Authorization

The health care component of UMKC may use and/or disclose PHI for research without obtaining a HIPAA authorization provided that it has obtained the following:

- Representations from the researcher that the use and/or disclosure is sought solely to prepare for research, no PHI will be removed from the organization, and the PHI sought is necessary for the research;
- To the extent that research pertains to a deceased patient, representations from the researcher that the PHI in fact belongs to a decedent, that the use or disclosure is solely for research, documentation of the patient's death, and that the PHI is necessary for research; and
- Approval of an alteration or waiver of the HIPAA authorization (in whole or in part) by the IRB.

16.8.1.2.2. Uses and Disclosures of Research PHI Under Waiver/Alteration of HIPAA Authorization

To use and/or disclose PHI under a waiver/alteration, certain statements must be documented. The following items must be included in the documentation:

- The identity of the approving IRB
- The date on which the waiver or alteration was approved
- A statement that the IRB has determined that all the specified criteria for a waiver or an alteration were met

16.8.1.2.2.1. Waiver/Alteration Criteria

Documentation must exist that contain IRB/Privacy Board assurances that the waiver/alteration of the HIPAA authorization meets certain criteria, including:

- The use or disclosure of PHI involves no more than a minimal risk to an subject's privacy, based on:
  - an adequate plan to protect identifiers from improper use and disclosure,
  - an adequate plan to destroy identifiers at the earliest opportunity consistent with the research and absent a health or research justification for retaining that information, and
  - adequate written assurances by the PI that the PHI will not be re-used or disclosed to anyone else, except as is required by law, for oversight of the research itself, or for other permitted research;
- The research could not practicably be conducted without the waiver/alteration; and
- The research could not practicably be conducted without access to the PHI.

16.8.1.2.2.2. Effect of Prior Authorizations: HIPAA authorizations obtained prior to April 14, 2003 will continue to be valid unless a specific expiration date is noted in the HIPAA authorization. Without an expiration date, the institution may continue to use and disclose that PHI for research purposes in perpetuity.

16.8.1.2.2.3. Retention Requirements: the institution must maintain documentation of the IRB's (acting as a Privacy Board) approval of the waiver/alteration of the HIPAA authorization for at least six (6) years from the date the waiver/alteration was obtained.

16.8.2. Review Preparatory to Research

The Privacy Rule permits a covered entity to use or disclose PHI to a researcher without authorization or waiver of authorization for the limited purpose of a review preparatory to research. [45 CFR 164.512(i)(1)(II)]. Such reviews may be used to prepare a research protocol, or to determine whether a research site has a sufficient population of potential research subjects. Prior to permitting the researcher to access the PHI, the covered entity must obtain representations from the researcher that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any PHI from the covered entity, and that PHI for which access is sought is necessary for the research purpose. Researchers should consult the covered entity regarding any forms or applications necessary to conduct a review preparatory to research.

Researchers conducting a review preparatory to research may not record information in identifiable form, nor may they use the information they receive to contact potential subjects. Because the Privacy Rule permits a covered entity to disclose PHI to the Individual who is the subject of the information, covered health care providers and patients may continue to discuss

the option of enrolling in a research study without patient authorization. Even when permitted by the Privacy Rule, however, any use of patient information for recruitment must comply with IRB recruitment policies.

Reviews preparatory to research that are permitted under HIPAA may or may not be human subjects research depending on the investigation being conducted.

Only those reviews of a database by an Individual entitled to access that database intended to enumerate an available data set without reviewing PHI and for which no PHI is recorded do not require review. For example: medical records may be queried for information such as: in the year XXXX how many patients had a discharge diagnosis of [indicate disease/diagnosis]. IRB review is required for all other uses of PHI as Indicated.

IRB/Privacy Board review and approval is required prior to initiating this research. Investigators are not authorized to contact potential research subjects identified in reviews preparatory to research without first securing the appropriate IRB Human Subjects Research determination or approval

16.8.2. Research on PHI of Decedents

The protections of the Common Rule apply to living human beings. By contrast, the Privacy Rule also protects the IIHI of deceased persons (decedents). [See 45 CFR 164.512(f)(4)]. The Privacy Rule contains an exception to the authorization requirement for research that involves the PHI of decedents. A covered entity may use or disclose decedents' PHI for research if the entity obtains representations from the PI that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the Individuals about whom information is being sought. Researchers should submit the applicable IRB form for IRB approval when they intend to conduct research involving decedents' PHI. The IRB (acting as the Privacy Board) must then document its approval of an alteration or waiver of the HIPAA authorization (in whole or in part).

16.8.3. Limited Data Sets with a Data Use Agreement

When a researcher does not need direct identifiers for a study but does require certain data elements that are not permitted in de-identified data, the Privacy Rule permits a covered entity to disclose a Limited Data Set (LDS) to the researcher without authorization or waiver of authorization, provided that the researcher has signed a Data Use Agreement (DUA). [See 45 CFR 164.514(e)(1)]. The LDS is still considered to be PHI, but it must exclude only specified direct identifiers of the Individual or of relatives, employers, or household members of the Individual.

ALDS is an exception to the Privacy Rule requirement for an authorization from the subject for research use of PHI. A LDS lacks 16 of the 18 identifiers itemized by the Privacy Rule. Specifically, a LDS does **not** include the following identifiers:

- Name
- Postal address information, other than town or city, state, and zip codes;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web universal resource locators (URLs);
- Internet protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

An LDS may contain, for example:

- Dates of birth
- Dates of death
- Dates of service
- Town or city
- State
- Zip code

The difference between a LDS and de-identified information is that a LDS may contain dates and certain geographic information associated with an Individual that are absent from de-identified information.

The Privacy Rule requires that the DUA used in conjunction with the LDS contain provisions that:

- Establish the permitted uses and disclosures of the LDS by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the rule if done by the covered entity;
- Limit who can Use or Receive the data; and
- Require the recipient to agree to the following:
    - Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the DUA;

- Report to the covered entity any use or disclosure of the information not provided for by the DUA of which the recipient becomes aware; ensure that any agents, including a subcontractor, to whom the recipient provides the LDS agrees to the same restrictions and conditions that apply to the recipient with respect to the LDS; and
- Not to identify the information or contact the Individual.

Researchers who will be receiving a LDS must submit a signed copy of the covered entity's DUA to the UMKC IRB, prior to initiating the research.

16.9. Transition Provisions

The Privacy Rule contains certain grandfathering provisions that permit a covered entity to use and disclose PHI for research after the rule's compliance date of April 14, 2003. [45 CFR 164.532]. If the researcher obtained any one of the following prior to the compliance date:

- An authorization or other express legal permission from an Individual to use or disclose PHI for the research;
- The consent of the Individual to participate in the research; or
- An IRB waiver of consent for the research.

Even if consent or other express legal permission was obtained prior to the compliance date, if new subjects are enrolled or existing subjects are re-consented after the compliance date, the covered entity must obtain the Individual's authorization. For example, if there was a temporary waiver of consent for emergency research under the FDA's human subject protection regulations, and consent was later sought after the compliance date, Individual authorization must be sought at the same time.

The transition provisions apply to both uses and disclosures of PHI for specific research protocols and uses or disclosures to databases or repositories maintained for future research.

16.10. Patient Rights and Research

Under HIPAA, patients have certain rights. Those that may affect research include the right to receive a notice of privacy practices, the right to access, inspect, and receive a copy of one's own PHI, the right to request an amendment to one's own PHI, and the right to an accounting of certain disclosures of PHI that occur outside the scope of treatment, payment and health care operations that have not been authorized.

16.11. HIPAA and Existing Studies

Any research subject enrolled in a study that uses PHI from a covered entity must sign a HIPAA-compliant **HIPAA authorization form**. This form is in addition to the existing consent document, and is Federally required.

Approved by: Lawrence Dreyfus, PhD

Name of University Institutional Official

_____

Signature of University Institutional Official Date