Research Involving the Use or Disclosure of Protected Health Information

1. Definitions
   - 1.1. **Authorization** – signed permission to allow a covered entity to use or disclose protected health information.
   - 1.2. **Business Associate** - a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information.
   - 1.3. **Coded** - Direct personal identifiers have been removed (e.g., from data or specimens) and replaced with words, letters, figures, symbols, or a combination of these for purposes of protecting the identity of the source, but the original identifiers are retained in such a way that they can still be traced back to the source. Note: Sometimes also referred to as a "key" "link", or "map".
   - 1.4. **Covered Entity** - A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard. Covered entities can be institutions, organizations, or persons.
   - 1.5. **Data Use Agreement** – a contractual document used for the transfer of non-public or restricted use data. Examples include records from governmental agencies or corporations, student records information, existing human research subjects data, and limited data sets.
   - 1.6. **Disclosure** - The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.
   - 1.7. **Health information** - 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.
   - 1.8. **Health Insurance Portability and Accountability Act (HIPAA)** - HIPAA has three components, all of which are enforced by the federal Office for Civil Rights:
     - HIPAA Privacy Rule: protects the privacy of individually identifiable health information
     - HIPAA Security Rule: sets standards for the security of electronic protected health information
     - HIPAA Breach Notification Rule: requires covered entities and business associates to provide notification following a breach of unsecured protected health information
   - 1.9. **Hybrid entity** - A single legal entity that is a covered entity, performs business activities that include both covered and non-covered functions, and designates its health care components as provided in the Privacy Rule.

1.10. **Protected Health Information (PHI)** - Individually identifiable health information held or transmitted by a covered entity or its business associates, in any form or media, whether electronic, paper, or oral.

1.11. **Use** - With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity or health care component (for hybrid entities) that maintains such information.

1.12. **Workforce** – employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

2. Overview

2.1. The HIPAA privacy rule affects research and researchers when:

- Research requires access to and/or use of PHI that is created or maintained by covered entities, or
- A covered entity component of KSU performs research that creates or generates PHI

2.2. KSU researchers that obtain, use, or disclose PHI for research purposes are required to comply with the research-related requirements of the HIPAA regulations as described in this document. This policy applies to all research involving PHI, regardless of funding.

2.3. All KSU research activities involving human subjects and the access, use and/or disclosure of PHI must be reviewed and approved in advance by the KSU IRB or an IRB with which the KSU IRB has a written cooperative agreement, except in limited circumstances involving specific types of case reports or case studies. Research activities may not begin until the IRB has granted final approval of the research protocol.

2.4. The basic regulations published by the Department of Health and Human services (HHS) at 45 CFR part 46 and the Food and Drug Administration (FDA) at 21 CFR part 50 govern the protection of human subjects in research and include protections to help ensure the privacy of research subjects and the confidentiality of information collected during research. HIPAA supplements these protections by requiring covered entities to implement specific measures to safeguard the privacy of PHI.

2.5. Activities in which an investigator obtains or records individually identifiable health information for purposes of identifying potential human subjects to aid in study recruitment, among other things, would involve human subjects research under the HHS regulations at 45 CFR part 46.

2.6. Some research activities do not meet the definition of "human subjects research" yet they may require the use of a HIPAA authorization or a waiver from the IRB. Common examples include case studies, and activities that consist entirely of the use of decedent PHI. In these cases, investigators should submit a completed Exempt from Annual review application and Appendix N to the ORC for review.

2.7. Kent State University is a hybrid entity, an organization whose primary business is not the delivery of healthcare. Hybrid entities have both healthcare and non-healthcare components and thereby is directly or indirectly regulated by HIPAA and the Privacy Rule.

2.8. Components of KSU that are considered covered entities include:

- University Health Services
- Speech and Hearing Clinic

- KSU Medical Mutual and Anthem benefit plans

2.9. The IRB can consider, and act upon, requests for a waiver or alteration of the Privacy Rule's Authorization requirement for uses and disclosures of PHI for research when specific criteria have been satisfied. Among these criteria, an IRB must determine that, when appropriate, the research protocol includes "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data".

2.10. The KSU Privacy Officer and the Office of Security and IT Management help to ensure that PHI accessed or retained by KSU researchers meets HIPAA regulations.

2.11. Researchers may be required to complete HIPAA training prior to gaining IRB approval for a protocol involving the use or disclosure of PHI for research.

2.12. The Privacy Rule requires that an Authorization for disclosure of PHI pertain only to a specific research study, not to future, unspecified projects. As such, in general, broad-based statements about uses and disclosures of PHI for research, for example, those contained in some notice of privacy practices, do not qualify as gaining patient authorization for use or disclosure of PHI. However, as described in this document, there are allowable exceptions and qualifications that may apply to the use or disclosure of PHI for research purposes.

3. Use of PHI in Research

3.1. Under the Privacy Rule, researchers can use or disclose PHI under the following provisions:

- Disclosure or Use of PHI for Research with written Authorization
- Disclosure of Use of PHI for Research with an approved Waiver from the IRB
- Research Use/Disclosure without Authorization – in the following limited circumstances, researchers may access or use PHI obtained from a covered entity without an individual's authorization, provided that certain provisions are met.
    - Activities Preparatory to Research (when meeting specific requirements)
    - Research on decedent's information (when meeting specific requirements)
    - Use of Limited data set with a data use agreement
    - De-identified PHI

3.2. Disclosure or Use of PHI for Research with Authorization

3.2.1. Researchers must obtain individual authorization for use or disclose of PHI unless a regulatory permission applies.

3.2.2. An authorization is different from informed consent. The purpose of a HIPAA authorization is to provide the custodian of PHI (i.e., the covered entity) with written permission from an individual to release specific PHI to the researcher. The purpose of a consent form for research is to provide the researcher with written documentation that an individual has agreed to participate in a research study. At KSU, the HIPAA authorization and informed consent forms are stand alone documents that must be provided separately to prospective subjects. /

3.2.3. When individual authorization is obtained for research purposes, the Privacy Rule requires that it pertain only to a specific research study, not to nonspecific research or to future, unspecified projects.

3.2.4. The creation and maintenance of a research repository or database is considered a specific research activity, however the subsequent use of disclosure of information from the database for a specific research study requires a separate authorization

unless the use or disclosure of PHI is permitted without authorization (see sections below).

3.2.5. A HIPPA authorization must include the following core elements:

- A description of the PHI to be used or disclosed (identifying the information in a specific and meaningful way)
- The name(s) or other specific identification of person(s) or class of persons authorized to make the requested use or disclosure.
- The name(s) of other specific identification of the person(s) or class of persons who may use the PHI or to whom the covered entity may make the requested disclosure.
- Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.
- Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure (the terms "end of the research study" or "none" may be used for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the authorization is signed by an individual's personal representative, a description of the representative's authority to act for the individual.
- A statement of the individual's right to revoke his or her authorization in writing and any exceptions to that right (e.g., "except to the extent the authorization already has been relied on to make a disclosure," "to preserve the integrity of the other information collected during the study," "as part of a research dataset," "to individuals and organizations responsible for research oversight," "as required by federal or state law")
- Whether or not participation in the research is conditioned upon granting the authorization.
- The potential for the PHI to be re-disclosed by the recipient and no longer protected by HIPAA.

3.3. Disclosure of Use of PHI for Research with an approved Waiver from the IRB

3.3.1. In limited cases, the KSU IRB may waive the requirement for individual authorization for the release of PHI. A waiver of authorization permits, but does not require the covered entity to disclose PHI. The IRB may also approve a request that removes some, but not all, required elements of an authorization (a partial waiver). For example, the IRB may grant a partial waiver allowing the covered entity to disclose only the PHI necessary to a researcher to identify possible subjects. When subjects enroll into the study, they sign an Authorization so that the researcher can obtain additional data from the medical record to use as research data.

3.3.2. The following three criteria must be satisfied for the KSU IRB to approve a waiver or alteration of individual authorization:

1. The PHI use or disclosure involves no more than minimal risk to the privacy of individuals based on at least the presence of:

a. an adequate plan presented to the IRB to protect PHI identifiers from improper use and disclosure;
b. an adequate plan to destroy those identifiers at the earliest opportunity, consistent with the research, absent a health or research justification for retaining the identifiers or if retention is otherwise required by law; and
c. adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as 1.) required by law, 2.) for authorized oversight of the research study, or 3.) for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule.

2. The research could not practicably be conducted without the requested waiver or alteration, and
3. The research could not practicably be conducted without access to and use of the PHI.

3.3.3. While KSU IRB may review and approve a waiver/alteration of the HIPAA authorization process for a KSU researcher requesting to use or disclose PHI from any covered entity, a covered entity may have institutional policies that additionally require their own IRB or Privacy Board to approve a waiver/alternation. It is the researcher's responsibility to ensure that institutional requirements are met prior to access or use of PHI.

3.3.4. The KSU IRB may accept waivers or alterations of authorization that are granted by a privacy board or another IRB that have entered into an Institutional Authorization Agreement with the KSU IRB. A waiver of authorization permits, but does not require the covered entity to disclose PHI. Documentation of the approved waiver or alteration must be included with the IRB application and shall include:

- The identity of the approving IRB (IRB federal registration number) or Privacy Board
- The date on which the waiver or alteration was approved
- A statement that the IRB/Privacy Board has determined that all the specified criteria for a waiver or an alteration were met
- A brief description of the PHI for which use or access has been determined by the IRB to be necessary in connection with the specific research activity
- A statement that the waiver or alteration was reviewed and approved under either normal or expedited review procedures
- Signature of the IRB/Privacy Board chair, or the chair's designee.

3.4. Research Use/Disclosure without Authorization

3.4.1. **Preparatory to Research** – Under this provision, a covered entity can provide researchers with access or use of PHI without authorization, a waiver or alteration of authorization, or a data use agreement, provided that certain requirements are met. This provision is typically used for feasibility assessments (e.g., to determine whether a sufficient population exists to conduct research), or to aid in study recruitment.

3.4.1.1. A researcher who is an employee or a member of the covered entity's workforce (either directly or indirectly through an executed business associate agreement) can use PHI to for purposes preparatory to research purposes. However, this provision does not permit the researcher to remove PHI from the covered entity's site. Approval under this provision allows a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. To approve a study involving PHI under this provision, the IRB shall obtain representation from the researcher that:

1. The use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research,
2. A statement that no PHI will be removed from the covered entity by the researcher during the course of the review.
3. A statement that the PHI for which access is sought is necessary for research purposes.
4. Documentation from the covered entity that access to the PHI by the researcher is permissible with IRB approval.

3.4.1.2. A researcher who is not an employee or a member of the covered entity's workforce may access PHI from a covered entity for the purposes of contacting prospective research subjects, if they obtain IRB approval for a protocol that includes:

1. A request for a partial waiver of individual authorization by the IRB (Appendix N) for the purposes of obtaining PHI as necessary to recruit potential research subjects.
2. A statement that the use or disclosure of the PHI is solely for preparations of a research protocol.
3. A statement that the PHI for which access is sought is necessary for research purposes.
4. Documentation from the covered entity that access to the PHI by the researcher is permissible with IRB approval.

3.4.1.3. Under the HHS Protection of Human Subjects Regulations at 45 CFR 46 preparatory to research activities require that the informed consent of the subjects must be sought and documented, unless the IRB grants an alteration or waiver of consent.

3.4.2. **Research on PHI of Decedents** – under this provision, a covered entity can provide researchers with access or use of PHI of decedents without authorization, a waiver or alteration, or a data use agreement, provided that certain requirements are met.
.

3.4.2.1. To approve a study involving PHI under this provision, the IRB shall obtain representation from the researcher that:

1. The use or disclosure being sought is solely for research on the protected health information of decedents.
2. The PHI for which access is sought is necessary for the research.
3. Documentation will be provided regarding the death of the individuals about whom information is being sought (if requested by the covered entity).

3.4.2.2. Decedents are not considered "human subjects" under the federal human subjects regulations at 45 CFR 46, however, obtaining and using decedent PHI for research is subject to all HIPAA regulations for 50 years after the patient's death. If conducting research involving only the PHI of decedents, researchers must complete an Exempt from Annual review-Level I application, and Appendix N.

3.4.3. **Limited Data Sets with a Data Use Agreement** – Under this provision, a covered entity may disclose a limited data set to a researcher without individual authorization, or a waiver/alteration of authorization for research, public health, or health care operations with the execution of a data use agreement. A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Name
- Street address or box number
- Telephone or fax numbers
- Vehicle identification numbers and serial numbers
- URLs, IP addresses, and email addresses
- Full-face photographs
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers and other account numbers
- Device identifiers and serial numbers
- Biometric identifiers (fingerprints, handprints, iris scans)
- Certificate or license numbers

3.4.3.2. Information that may remain in a limited data set includes:

- Dates (i.e., admission, discharge, service, birth, death)
- City
- State
- Zip code
- Age (in years, months, days or hours)

3.4.3.3. The research use of a Limited Data Set may or may not be considered human subjects research, depending on whether the data are individually identifiable as defined by the human subjects regulations at 45 CFR 46. If conducting research

involving only data from a Limited Data Set, researchers should complete an Exempt from Annual review- Level I application, and Appendix N.

3.4.3.4. If it is the case that a researcher is provided with PHI that includes direct identifiers for the purposes of creating a limited data set for a covered entity, in addition to a data use agreement, a business associate agreement may be required.

3.4.3.5. Researchers must limit the protected health information disclosed or requested to that which is the minimum necessary for the research project. Per university policy, data use agreements and business associate agreements must be reviewed by the Office of General Counsel, the HIPAA privacy officer and the Office of Security and IT Management.

3.4.3.7. A data use agreement must contain the following provisions: :

1. Specific permitted uses and disclosures of the limited data set 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;
2. Identify who can use or receive the data; and
3. Require that the recipient:
    - Not 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 data use agreement;
    - Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
    - Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
    - Not to identify the information or contact the individual.

3.4.3.8. Researchers should consult with their department officials to determine who is authorized to sign the data use agreement on behalf of the university.

3.5. De-identified – health information that is de-identified can be used or disclosed without restriction under the Privacy Rule, and per the human subject regulations at 45 CFR 46 may meet the Exempt from Annual review – Level I requirements at KSU.

3.5.1. It is the responsibility of the covered entity granting access to PHI to determine that the information has been de-identified using either:

- Statistical verification of de-identification, or
- Removing the 18 elements that could be used to identify individuals, the individual's relatives, employers, or household members.

3.5.2. The following identifiers must be removed from PHI to consider the data un-identifiable:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, 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 unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
    b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 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 age 90 or older.
4. Telephone numbers
5. Facsimile numbers
6. Email 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. Web universal resource locators (URLs)
14. IP addresses
15. Device identifiers and serial numbers
16. Biometric identifiers (fingerprints, handprints, iris scans)
17. Full-face photographs
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

3.5.3. Coded data – Under the Privacy Rule, coded health information can be considered de-identified if both of the following standards are met:

1. The code is not derived from or related to the information about the individual, and the code could not be translated to identify the individual.
2. The researcher does not have the information to decode the data, and the key to the code is secure.

3.6. Online Resources

- Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule
- Frequently Asked Questions

- 45 CFR 164.501, 164.508, 164.512(i) (See also 45 CFR 164.514(e), 164.528, 164.532)
- Understanding HIPAA in Research
- Institutional Review Boards and the HIPAA Privacy Rule