

Policy on Research Involving Coded or De-identified Information or Biological Specimens
Effective Date November 1, 2004

Policy

Research involving coded or de-identified data or specimens must be reviewed by the KUMC Human Subjects Committee (HSC) prior to implementation, to ensure compliance with federal regulations on human subjects protection and patient privacy. A streamlined system of review and oversight may be utilized if the source of the data/specimens has been registered with the HSC under a Master Plan agreement.

Background

Federal regulations at 45 CFR 46.102(f) specify that human subjects research occurs when an investigator obtains identifiable private information or identifiable specimens for research purposes. When identifiable information or specimens are used for a research purpose, the Human Subjects Committee must review and approve the activity prior to initiation. In the past, questions have arisen about whether human subjects research occurs if the investigator obtains only coded or de-identified information or specimens. On August 10, 2004, the federal Office for Human Research Protections (OHRP) issued guidance that discusses appropriate institutional oversight of such research. The guidance clarifies federal regulations by stating that research using coded data or specimens does not have to be classified as human subjects research, provided that: (1) the data/specimens were not collected for the current research purpose; and (2) there are documented and approved mechanisms to prevent the release of identifiers. The guidance further clarifies that the regulations apply not only to existing information and specimens but also to materials to be collected in the future.

This policy is being issued to clarify the federal regulations regarding research with coded or de-identified data or specimens and to establish a Master Plan process to streamline the oversight of internal data centers or specimen repositories. Prior to their use for research, the HSC must confirm that the data centers or repositories have implemented appropriate security measures and assurances so that investigators are not given identifiers or keys to decipher coding systems. A data center or specimen repository with an approved Master Plan may be accessed for multiple research projects with limited oversight by the HSC.

Definitions

Coded means that:

(1) identifying information (such as 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 pertain 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 the linkage of the identifying information to the private information or specimens.

In order to comply with the HIPAA Privacy Rule, the code must not contain elements that are derived from or related to information about the individual (such as initials or segments of the social security number). [OHRP Guidance August 10, 2004]

De-identified means that the information does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual. Information is considered de-identified under this policy if the eighteen identifiers outlined in the HIPAA Privacy Rule are removed from the health information and if no code exists enabling the linkage of the identifying information to private information or specimens. [45 CFR 164.514]

Human subject means a living individual about whom an investigator obtains data, through intervention or interaction with the individual, or identifiable private information. [45 CFR 46.102]

Investigator means anyone involved in conducting research. The act of solely providing coded private information or specimens does not constitute involvement in the conduct of research. [OHRP Guidance August 10, 2004]

Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. [45 CFR 46.102]

Procedures

1. A Master Plan application may be submitted by a faculty member who is responsible for the data center or specimen repository. The faculty member will be the principal investigator for the Master Plan. Principal investigators must demonstrate knowledge of human subjects protection by completing the institution's certification process.
2. An approvable submission must include an application form, a written project plan, a sample user request form, resource manager agreements, and verification of human research protection training.
 - a. The application form is available from the Human Subjects Office and from the HSC website.
 - b. The written project plan must contain:
 - i. A description of the original sources of the data and/or specimens that are available for use by researchers. Applicants must confirm that the identifiable data or specimens were collected for purposes other than the currently proposed research project.
 - ii. The purpose for developing the master plan, including a general description of anticipated projects and anticipated users.
 - iii. A description of the coding system that will be used, when warranted, to allow resource managers to generate follow-up information. If no follow-up information is required, the data/specimens given to researchers should be de-identified.

- iv. An outline of the operating procedures that prohibit the release of identifiers to researchers. The application should include a description of security practices for the data or specimens including, as applicable:
 1. Physical security such as locked files and limited physical access.
 2. Electronic measures such as log-in authentication and passwords. Electronic measures may include software programming that facilitates de-identification of records.
 3. Administrative oversight to ensure that only authorized users are given access to identifiers or keys to the coding system.
 - c. A sample research request form should be developed by the principal investigator or resource manager, as applicable to the resource. In the request form, the researcher should describe his/her project, delineate the data elements required, agree to request and use only coded or de-identified materials, justify the use of coded data (if applicable), and agree to notify the HSC if subject identities or keys to decipher the code are inadvertently discovered or if unforeseen circumstances warrant the release of identifiers.
 - d. Resource manager agreements are available from the Human Subjects Office and from the HSC website. They must be signed by individuals who have access to identifiable data and specimens. In the agreement, the manager agrees only to release coded or de-identified data or specimens and to immediately report any breach of confidentiality to the HSC.
 - e. The principal investigator must maintain current training in human subjects protection.
 3. Review of a proposed Master Plan is the responsibility of the Chair of the HSC. The Chair may designate another HSC member and/or an administrative staff member within the Human Research Protection Program to conduct the reviews. Master Plans will be reviewed on an individual basis. The Chair or designated reviewer will confirm that the project comes under the OHRP guidance described above and does not involve data or specimens regulated by the U.S. Food and Drug Administration.
 4. The Principal Investigator will administer an internal approval process for individual uses of the data/specimen resource. The Principal Investigator will report semi-annually to the Human Subjects Committee about approved projects

Groups covered

This policy applies to faculty, staff, and students at the University of Kansas Medical Center and to researchers at external organizations for which the KUMC Human Subjects Committee serves as the institutional review board.

Related documents

HHS regulations for the protection of human research subjects (45 CFR part 46)
HIPAA Privacy Rule (45 CFR part 160 and subparts A and E of part 164)
OHRP Guidance on Research Involving Coded Private Information of Biological Specimens,
August 10, 2004

Contact

Director, Human Research Protection Program
G004 Sudler
(913) 588-0942

Master Plan # _____

KUMC Human Subjects Committee
Master Plan Application for Data or Specimen Resources

Responsible Faculty: _____ Department: _____

Brief Description of Data or Specimen Resource:

Resource Manager(s)	Phone	Email
1. _____	_____	_____
2. _____	_____	_____
3. _____	_____	_____
4. _____	_____	_____

This application form must be accompanied with a detailed description of the proposed Master Plan. The submission must contain the following:

- A description of the original source of the data or specimens and the type of consent obtained for their collection
- A description of anticipated projects and anticipated users of the resource
- A description of the coding system that will be used to prevent identifiers from being disclosed to users. Information on approvable coding systems is found in the [KUMC Policy on Research Involving Coded Private Information or Biological Specimens](#)
 - If the research can be accomplished with de-identified data/specimens, the data/specimens must be provided to the researcher without a code attached.
 - When research goals necessitate a code that links data to identifiers, coded data may be released. The application should address the criteria for approving the use of coded data.
- A description of security practices for the data or specimens including, as applicable:
 - Physical security including, but not limited to locked files and limited physical access.
 - Electronic security measures such as log-in authentication and passwords. Electronic security measures may include software programming that facilitates de-identification of records.
 - Administrative oversight to ensure that only authorized users are given access to identifiers or keys to the coding system.
- A sample request form that users will submit to the responsible faculty
- Agreements signed by each of the resource managers listed above

As the faculty member responsible for the Master Plan, I agree that I will:

- Ensure that the administration of the Master Plan follows federal and university policies for coding and/or de-identification of data/specimens;
- Review individual applications for use of the data/specimen resource approved under the Master Plan;
- Maintain records of approved projects;
- Notify the Human Subjects Committee if identifiers are inadvertently released or if unforeseen circumstances warrant the release of identifiers; and
- Report approved projects semi-annually to the Human Subjects Committee.

Signature _____ Date _____

Department Chair Approval:

As Department Chair, I have reviewed this application for a Master Plan and approve submission to the HSC.

Signature _____ Date _____

Master Plan # _____

Manager Agreement for Data/Specimen Resources

This agreement ensures appropriate safeguards for identifiable data and specimens that are accessed for KUMC research purposes. Under a Master Plan approved by the KUMC Human Subjects Committee, the resource manager may code or de-identify data/specimens for research projects approved by the faculty supervisor.

Manager Name	Title	Department

Data or Specimen Resource(s)		

Responsible Faculty	Department	Phone

By signing this agreement, I agree to do the following:

- Read and comply with the KUMC Policy on Research Involving Coded Private Information or Biological Specimens
- Limit physical and electronic access to identifiers as described in the Master Plan protocol
- Release information associated with data/specimens for research purposes only as authorized by the responsible faculty
- Remove all identifiers listed as identifiable information in the HIPAA Privacy Rule (see Attachment)
- When the use of a tracking code has been approved, create a code that does not use patient-related information, in whole or in part
- Notify the responsible faculty immediately (within two business days) if identifiers are inadvertently released

Signature _____ Date _____

Manager Agreement for Data/Specimen Resources Attachment

At 45 CFR 164.514(b)(2)(i), the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule delineates eighteen identifiers for health information. If any of the following demographic characteristics are paired with information about past, present, or future physical or mental health, or information about the payment of health care, the resulting information is Protected Health Information under federal law.

- Names;
- 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:
 - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- 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;

- 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;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code

To qualify as de-identified data, each of the elements listed above must be removed.

Note: a de-identified data set may include a tracking code or other numbering system, provided that:

- a. the tracking code is not derived from or related to information about the individual
- b. the re-identification algorithm is not disclosed to the data recipient