16 Health Insurance Portability and Accountability Act (HIPAA)

This section is under review in anticipation of moving it to the portfolio of the HIPAA Privacy Office.

Protected health information obtained by CMU may not be used internally or disclosed to any outside person or organization for research purposes without prior approval of the IRB or the privacy board or privacy office of the entity responsible for the records. CMU researchers must also abide by all corporate HIPAA policies regarding HIPAA privacy and security.

The following describe the procedures for conducting research at CMU in accordance with the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*.

16.1 Definitions

Access –The mechanism of obtaining or using information electronically, on paper, or other medium for the purpose of performing an official function.

Authorization – A detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

Covered entity –The term applied to institutions that must comply with the Privacy Rule. These include

1. Health plans.
2. Health care clearinghouses.
3. Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

Common Rule – A federal policy on human subject protection that provides for the primary source of regulation of research.

De-Identified Information – 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.

Deletion – The removal, erasing, or expunging of information or data from a record.

Disclosure –The release, transfer, provision of access to, or divulging in any other manner information outside of the covered entity.

Health Information –Any information created or received by a health care provider or health plan that 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 payment for the provision of health care to an individual.

Identifiable Health Information –A subset of health information including demographic information collected from an individual.

Limited Data Set –Protected health information that excludes specific direct identifiers of the individual or of relatives, employees, or household members of an individual. 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.

Minimum Necessary –The principle that any access should be limited to the minimum amount of information needed to accomplish the intended purpose of the use or disclosure.

Privacy Board – A board comprised of members of varying backgrounds and appropriate professional competencies, as necessary, to review individual's privacy rights. It is an alternative to an IRB for privacy issues only. It cannot replace the IRB for Common Rule purposes.

Privacy Act –An Act of Congress that provides for the confidentiality of individually-identified and retrieved information about living individuals that is maintained in a system of records and permits the disclosure of records only when specifically authorized by the statute. The Act provides that the collection of information about individuals is limited to that which is legally authorized, relevant, and necessary.

Privacy Rule –Provides guidance on the use of protected health information in the conduct of research. It imposes requirements on those involved in research, both individuals and institutions. "Privacy" refers to a person's desire to control the access of others to information about him/herself. The evaluation of privacy involves consideration of how the investigator will access information from or about participants. The IRB members should know strategies to protect privacy interests relating to contact with potential participants and access to private information.

Protected Health Information – Individually identifiable health information transmitted or maintained electronically or in any other form or medium, except for education records or employment records, as excluded in the Privacy Rule.

Preparatory Research – The method applied to developing or designing a research study.

Waiver of Authorization –A means of requesting approval from an IRB or Privacy Board rather than asking each research subject for an authorization to access protected health information.

16.2 Research Under HIPAA

HIPAA defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." This definition is

identical with the one used in the Common Rule. HIPAA describes privacy standards for protecting PHI and so only applies to research that involves humans' (not animals') health information.

16.2.1 Waiver of Authorization for Use or Disclosure of Protected Health Information in Research

Under the Privacy Rule, covered entities are permitted to use and disclose protected health information for research with individual authorization or without individual authorization under limited circumstances. A covered entity may use or disclose protected health information for research when presented with documentation that an IRB 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.

The waiver of documentation presented to the covered entity must include the following:

1. Identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
2. A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Rule;
3. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;
4. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
5. The signature of the Chair or other member, as designated by the Chair, of the IRB or the Privacy Board, as applicable.

The following criteria must be satisfied for the IRB to approve a waiver of authorization under the Privacy Rule:

The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

1. An adequate plan to protect the identifiers from improper use and disclosure; and
2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
3. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart; and
4. The research could not practicably be conducted without the waiver or alteration; and
5. The research could not practicably be conducted without access to and use of the protected health information.

16.2.2 Review Preparatory to Research

The Privacy Rule permits a covered entity to use or disclose protected health information to a researcher without authorization or waiver for the limited purpose of a "review preparatory to research." 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 protected health information, the covered entity must obtain representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information 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 that they receive to contact potential subjects, unless the investigator is also the subject's treating physician. Because the Privacy Rule permits a covered entity to disclose protected health information 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 clinical trial without patient authorization. Even when permitted by the Privacy Rule, however, any use of patient information for recruitment must comply with IRB recruitment policies (see discussion below).

1. All human subjects' research requires IRB review to determine either (i) exempt status or (ii) need for further review.

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

a. 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 Privacy Board Review is required for all other uses of PHI as indicated.

b. If the research involves a de-identified data set, defined as removing the following identifiers, then a de-identified data set certification form must be completed submitted for administrative review and certified prior to accessing the data set. This activity also requires an IRB-determined exemption from review:

    1. Names
    2. Geographic information (city, state, and zip)
    3. Elements of dates (except years)
    4. Telephone #s
    5. Fax #s
    6. E-mail address
    7. Social Security #

8. Medical record, prescription #s
9. Health plan beneficiary #s
10. Account #s
11. Certificate /license #s
12. VIN and Serial #s, license plate #s.
13. Device identifiers, serial #s
14. Web URLs
15. IP address #s
16. Biometric identifiers (finger prints)
17. Full face, comparable photo images
18. Unique identifying #s

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 unless they are directly responsible for care of the potential subject and entitled to PHI as a result of that duty.

Investigators who have previously obtained full consent and authorization to contact a research subject as a result of a previously approved research project, may contact his/her former research subjects provided that the subject agreed to be contacted for information on future research conducted by the same PI or co-investigator(s).

16.2.3 Research on Protected Health Information of Decedents

The protections of the Common Rule apply only to living human beings; by contrast, the Privacy Rule also protects the identifiable health information of deceased persons ("decedents"). 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 researcher 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.

16.2.4 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" to the researcher without authorization or waiver, provided that the researcher has signed a data-use agreement. The limited data set is still considered to be protected health information, but it must exclude only specified direct identifiers of the individual or of relatives, employers, or household members of the individual.

If the research involves a limited data set, it is defined as removing the following 16 identifiers:

1. Names
2. Postal address information (if other than city, state and zip)
3. Telephone and fax #s
4. Email addresses

5. Social Security #s
6. Medical record, prescription numbers
7. Health plan beneficiary #s
8. Account #s
9. Certificate/license #s
10. Vin and serial #s, license plate #s
11. Device identifiers, serial #s
12. Web URLs
13. IP address #s
14. Biometric identifiers (finger prints)
15. Full face, comparable photo images

The Privacy Rule requires that the data-use agreement used in conjunction with the limited data set contain provisions that

1. Establish the 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; and

Limit who can use or receive the data; and

Require the recipient to agree to the following:

a. Not to use or disclose the information other than as permitted by the data-use agreement or as otherwise required by law; and

b. Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement; and

c. 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; and

d. 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

e. Not to identify the information or contact the individual.

Researchers who will be receiving limited data sets must submit a signed copy of the covered entity's data use agreement to the CMU IRB for approval, prior to initiating the research. 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, if the researcher obtained any one of the following prior to the compliance date:

2. An authorization or other express legal permission from an individual to use or disclose protected health information for the research; or

The informed consent of the individual to participate in the research; or

An IRB waiver of informed consent for the research.

Even if informed 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 informed consent for emergency research under the FDA's human subject protection regulations, and informed 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.

16.3 HIPAA and Documentation Requirements

HIPAA documents include an authorization form, a waiver of authorization form, and a de-identification form. One of these documents must be used whenever PHI is utilized in the research.

16.4 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.

16.5 HIPAA and Existing Studies

Any research subject enrolled in a study that uses PHI from a covered entity must sign a HIPAA-compliant authorization form. This form is in addition to the existing Informed Consent document and is federally required. In a few cases, the Informed Consent document may be combined with a HIPAA authorization.

16.6 Waivers to HIPAA Authorization Form

In some cases, the CMU IRB may approve a waiver to use of the HIPAA authorization form. This may occur when the IRB finds that the research could not be practically done without the waiver, not without access to and use of the PHI, and that disclosure poses minimal risk to privacy.