Title: HIPAA and Research with Human Subjects
Latest Approval Date: 7/28/2023
Previous Approval Dates: 6/1/2020
Standard Operating Practice: 19

19.1. Executive Summary

This unit standard provides information regarding the Health Insurance Portability and Accountability Act (HIPAA) and its application to medical records involving human subjects research. NC State University faculty and staff should review this unit standard to assist with making informed decisions when utilizing or generating medical records for research with human subjects.

HIPAA is a federal law that sets a standard for the protection of medical records and personal health information. The HIPAA Privacy Rule establishes a category of health information, defined as protected health information (PHI), which a covered entity may only use or disclose to others in certain circumstances and under certain conditions.

19.2. Standard Operating Practice (SOP)

Investigators are responsible for complying with HIPAA (opens in a new window), human subject protection regulations at 45 CFR 46 (opens in a new window), and applicable NC State University policies, regulations, and rules, including REG 01.25.09 (opens in a new window) when accessing medical records for research purposes. If a covered entity (or NC State department or administrator) denies an investigator access to information in a medical record, the NC State IRB cannot overrule the decision.

19.3. Operational Procedures

The Privacy Rule establishes a category of health information, called “protected health information” referred to as PHI, which may be used or disclosed to others only in certain circumstances or under certain conditions.

19.3.a. Definition of Terms

19.3.a.i. Covered Entities

1. A covered entity is a health plan, health care clearinghouse, or health care provider that engages in certain electronic transactions as specified by HIPAA.
2. A covered entity may be a hybrid entity, which is a single legal entity that is a covered entity but performs business activities that include both covered and noncovered functions, and designates certain units as its health care components as provided in the Privacy Rule.
3. NC State University is a hybrid entity.
4. Many organizations that use, collect, access, and disclose individually identifiable health information are not covered entities but their use of PHI may still be governed by HIPAA.
5. Researchers are not covered entities that must comply with HIPAA privacy policies and procedures unless they:
    a. are also health care providers who electronically transmit health information in connection with any transaction for which the Department of Health and Human Services (HHS) has adopted a standard OR
    b. are employees or other workforce members of a covered entity (e.g., a hospital or health insurer), they must comply with that entity’s HIPAA privacy policies and procedures

6. The Privacy Rule protects all “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. The Privacy Rule calls this information “protected health information” (PHI).

19.3.a.ii. Health Information

1. Health information is any information, including genetic information, whether oral or recorded in any form or medium, that:
   a. 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
   b. relates to the past, present, or future physical or mental health or condition of an individual or the past, present, or future payment for the provision of health care to an individual

19.3.a.iii. Protected Health Information (PHI)

1. The term “protected” means the information is shielded under the HIPAA Privacy Rule
2. PHI is individually identifiable health information that is:
   a. transmitted by electronic media;
   b. maintained in electronic media; or
   c. transmitted or maintained in any other form or medium
3. PHI includes all individually identifiable information used to identify a patient or provide healthcare services or coverage, such as:
   a. demographic data
   b. medical histories
   c. test results
   d. insurance information
4. PHI excludes individually identifiable health information that is:
   a. in education records covered by the Family Educational Rights and Privacy Act (FERPA);
   b. records of students aged 18 years old or older attending a post-secondary institution of education that are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in their professional capacity and the records are made, maintained, or used only in connection with the provision of treatment to the student and are not available to anyone other than persons providing such treatment or a physician or other appropriate professional of the student’s choice;
   c. employment records held by a covered entity in its role as employer; and
   d. regarding a person who has been deceased for more than 50 years
5. PHI does not include de-identified data, which is data where:
   a. a person’s identity is removed and cannot be reasonably ascertained either through the data itself or with contextual clues; and
   b. specific identifiers (described in HIPAA law (opens in a new window) have been removed with respect to the individual, their relatives, employers, and household members
6. De-identified PHI:
   a. can be used or disclosed without consent or authorization as long as no means of re-identification are applied

b. where it is not possible to re-identify an individual from the data, is not subject to IRB approval

19.3.a.iv. Individually Identifiable Health Information

1. Individually identifiable health information is data used by a HIPAA-covered entity or business associate within the context of healthcare services or payment.
2. Individually identifiable health information is classed as protected health information.
3. Individually identifiable health information contains one or more of the following identifiers that can be used to identify, contact, or locate a person:
   a. Name (full name or last name with first initial)
   b. All geographic identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. 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 for all geographic units containing 20,000 or fewer people is changed to “000”
   c. Dates (other than year) directly related to an individual
   d. Phone numbers
   e. Fax numbers
   f. Email addresses
   g. Social security numbers
   h. Medical record numbers
   i. Health insurance beneficiary numbers
   j. Account numbers
   k. Certificate/license numbers
   l. Vehicle identifiers (including serial numbers and license plate numbers)
   m. Device identifiers and serial numbers
   n. Web Uniform Resource Locators (URLs)
   o. Internet Protocol (IP) address numbers
   p. Biometric identifiers, including finger, retinal, and voice prints
   q. Full-face photographic images and any comparable images
   r. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

19.3.a.v. Hybrid Entities

1. Hybrid entities are institutions that perform both HIPAA-covered and non-covered functions as part of their business operations.
   a. A covered function is any function that makes the performer a health plan, a health care provider, or a health care clearinghouse

19.3.a.vi. NC State University as a Hybrid Entity

1. NC State University is a hybrid entity
2. The University has designated the following units as healthcare components:
   a. Student Health Services
   b. Counseling Center
   c. Sports Medicine
   d. All functional units that provide support services for health care functions (e.g., billing, payment, PHI management, etc.) to (a) through

(c) including their contact and subcontract employees not otherwise defined as “business associates”:

i. Office of Information Technology (OIT)
ii. Enterprise Application Systems (EAS)
iii. ComTech network services
iv. Technology Support Services (TSS)
v. Infrastructure, Systems & Operations (ISO)
vi. Security and Compliance Unit (S&C)
vii. Internal Audit
viii. General Counsel
ix. Risk Management
x. University Cashier
xi. Accounts Receivable
xii. Human Resources
xiii. Registration and Records
xiv. Environmental Health and Safety
xv. College of Veterinary Medicine
xvi. Office of Disability Services
xvii. University Housing (Conference and Guest Services)
xviii. NC State Dining

19.3.b. HIPAA and Research

The Privacy Rule does not generally apply to research unless the research is conducted in a designated health care component but it does govern when and how researchers can use and obtain PHI.

19.3.b.i. Research Within Covered Entities

1. The determination of whether an individual researcher must comply with the Privacy Rule is a fact-sensitive, individualized determination.
2. To gain access to PHI for research purposes, the researcher may have to provide supporting documentation on which the covered entity may rely in meeting the requirements, conditions, and limitations of the Privacy Rule. The documentation may depend on how the entity with which the researcher has a relationship with is organized.
3. Questions on a researcher’s status under the Privacy Rule should be referred to the NC State University IRB office or the NC State University HIPAA Privacy Officer.
4. Researchers who are not themselves covered entities or who are not workforce members of covered entities may still be subject to the Privacy Rule if covered entities supply their data.

19.3.b.ii. Research Within Hybrid Entities

1. Research components of a hybrid entity that function as health care providers and conduct certain standard electronic transactions must be included in the hybrid entity’s health care component(s) and are subject to the HIPAA Privacy Rule.
2. If the business unit would be considered a covered entity if it were a separate legal entity, then it must be included as a healthcare component subject to the Privacy Rule even if it is solely a research unit.

19.3.b.iii. Use and Disclosure of PHI for Research Purposes

1. When using PHI for research purposes, the researcher must apply to the IRB for approval before accessing or generating PHI and the application must include:
    a. A data use agreement with external covered entities
    b. A completed data access and security plan (Word document)
    c. A HIPAA individual authorization (medical records release form) or Request for a Waiver of Individual Authorization for the Use of PHI in Research
2. The HIPAA Privacy Rule generally requires an individual's authorization or a waiver by an Institutional Review Board (IRB) or a special privacy board for the disclosure of PHI from covered healthcare components.
3. A HIPAA Authorization waiver can be granted by an IRB or privacy board for activities preparatory to research, research on PHI of deceased individuals, and disclosure of limited data sets to an employee of a covered entity (or in the case of a hybrid entity, its covered health care component) pursuant to a data use agreement
4. De-identified health information may be used or disclosed for research purposes without an authorization or IRB waiver.
5. When using PHI for research purposes, the researcher must apply to the IRB for approval before accessing or generating PHI

19.3.b.iv. Use and Disclosure of PHI for Activities Preparatory to Research

PHI may be used or disclosed without an individual's authorization or waiver for the preparation for or development of a research protocol provided that:

1. the researcher is an employee of a covered healthcare component and
2. the researcher documents that all of the following criteria are satisfied:
    a. The use or disclosure of PHI is solely to prepare a research protocol or to identify prospective research participants for the purposes of seeking an authorization;
    b. The research shall not record or remove the PHI from the covered healthcare component;
    c. The PHI sought is necessary for the purposes of the research;
    d. The head of the covered health care component or their designee shall review, approve, and maintain the above documentation; and
    e. Researchers who are not employees of a covered health care component must obtain an authorization or waiver of authorization prior to accessing PHI for activities that are preparatory to research.

19.3.b.v. Use and Disclosure of PHI for Participant Recruitment

1. Individuals responding to a research study advertisement should be given an explanation of the study including, but not limited to, the name of the principal investigator and a description of the study prior to granting authorization.
2. All other uses or disclosures of PHI by a covered health care component for the purposes of contacting and/or recruiting potential research participants require an authorization or waiver of authorization.

19.3.b.vi. Use and Disclosure of PHI of Deceased Individuals

1. HIPAA permits disclosure of PHI of deceased individuals to researchers if they provide documentation to the covered entity of the individual's death, that the

PHI is necessary for research purposes, and that the PHI will only be used for the research about the deceased individual.

19.3.b.vii. Use and Disclosure of Limited Data Sets

1. Under HIPAA, a researcher may use a limited data set for any research purpose without an authorization or waiver of authorization if the covered entity agrees to provide limited data sets.
2. A limited data set must exclude all of the following direct identifiers of the individual and the individual's relatives, employers, and household members of the individual:
    a. Names (full name or last name with first initial)
    b. Postal address information other than town/city, state, or zip code
    c. Telephone numbers
    d. Fax numbers
    e. Electronic mail addresses
    f. Social security numbers
    g. Medical record numbers
    h. Health plan beneficiary identifiers
    i. Account numbers
    j. Certificate/license numbers
    k. Vehicle identifiers and serial numbers, including license plate numbers
    l. Device identifiers and serial numbers
    m. Web universal resource locators (URLs)
    n. Internet protocol (IP) address numbers
    o. Biometric identifiers including finger, retinal, and voice prints
    p. Full-face photographic images and any comparable images
    q. Any other characteristic or code that could be used to identify the individual
3. A researcher must sign a HIPAA-compliant data use agreement, which includes:
    a. provisions limiting the use of the data only for the research for which it was received;
    b. agreement to use appropriate safeguards to prevent the use or disclosure of the data other than as permitted by the HIPAA Privacy Rule; and
    c. agreeing not to re-identify individuals from the data or contact the individual.
4. In requesting a limited data set, the requestor must specify the purposes of the limited data set and the categories of data elements requested to satisfy the minimum necessary standard of HIPAA.

19.3.b.viii. Use and Disclosure of De-identified Health Information

1. De-identified health information is exempt from HIPAA and may be used or disclosed for research purposes without an authorization or waiver of authorization.
2. Researchers must provide documentation to the IRB that the health information has been de-identified by one of the following methods:
    a. Statistical method
        i. The IRB may determine that health information is de-identified for the purposes of this regulation if an independent, qualified statistician who is not the principal investigator or a member of the research team:
            1. determines that the risk of re-identification of the data, alone, or in combination with other data, is very small;

2. documents the methods and results by which the health information is de-identified;
3. makes a risk determination

b. Removal of all identifiers
    i. All identifiers concerning the individual and their employers, relatives, and household members are removed.
        1. Name (full name or last name with first initial)
        2. All geographic identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. 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 for all geographic units containing 20,000 or fewer people is changed to “000”
        3. Dates (other than year) directly related to an individual
        4. Phone numbers
        5. Fax numbers
        6. Email addresses
        7. Social security numbers
        8. Medical record numbers
        9. Health insurance beneficiary numbers
        10. Account numbers
        11. Certificate/license numbers
        12. Vehicle identifiers (including serial numbers and license plate numbers)
        13. Device identifiers and serial numbers
        14. Web Uniform Resource Locators (URLs)
        15. Internet Protocol (IP) address numbers
        16. Biometric identifiers, including finger, retinal, and voice prints
        17. Full-face photographic images and any comparable images
        18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

3. The de-identified information may be assigned a code affixed to the research record that will permit the information to be re-identified if necessary, provided that the key to such a code is not accessible to the researcher requesting to use or disclose the de-identified health information. NOTE: Other uses of code names to identify data are not considered de-identified under HIPAA.
4. Responsibility for provisions to protect the security and privacy of PHI used for research rests with the principal investigator of the research.

19.3.b.ix. Differences Between Informed Consent and Individual (HIPAA) Authorization

1. Informed consent is the individual’s permission to participate in research.
2. An informed consent provides research subjects with a description of the study, its anticipated risks and/or benefits, and how the confidentiality of records will be protected.
3. Informed consent must be sought, obtained, and documented in accordance with 45 CFR 46.116-117 (opens in a new window) and NC State IRB unit standard on informed consent, parental permission, and minor assent (Word

document) unless the IRB has determined a waiver of informed consent or a waiver of the documentation of informed consent is appropriate.
4. HIPAA authorization is not the same as obtaining informed consent for research.
5. HIPPA authorization differs from informed consent in that the authorization is an individual's permission to use or disclose PHI for a specified purpose, such as a research study
6. When seeking informed consent for research and an Individual HIPAA Authorization, researchers must use different forms though the processes can occur together.

19.3.b.x. Individual Authorization (HIPAA Authorization)

1. Obtaining individual authorization for the use of PHI can be a part of the informed consent process for research with human subjects.
2. When an authorization is obtained for research purposes, the Privacy Rule requires that it pertains only to a specific research study, not to future, unspecified projects.
3. If an authorization for research is obtained, a covered entity's use and disclosure of PHI must be consistent with what is stated in the authorization.
4. A valid HIPAA-compliance authorization must contain specific elements:
    a. A meaningful description of the PHI to be used or disclosed.
    b. The name of the individual or the name of the person authorized to make the requested disclosure.
    c. The name or other identification of the recipient(s) of the information.
    d. A description of each purpose of the disclosure (The statement "at the request of the individual is sufficient when the individual initiates the authorization and does not, or elects not to, provide a statement of the purpose).
    a. An expiration date or an expiration event that relates to the individual or to the purpose of the use or disclosure ("end of the research study" or "none" are permissible for research, including for the creation and maintenance of a research database or repository).
    e. A signature of the individual or their personal representative (someone authorized to make health care decisions on behalf of the individual) and the date.
    f. If the individual's legally authorized representative signs the authorization form, a description of the representative's authority to act for the individual must also be provided.
    g. A statement of the individual's right to revoke the authorization and how to do so and, if applicable, the exceptions to the right to revoke the authorization or reference to the corresponding section of the covered entity's notice of privacy practices.
    h. Information on whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on the authorization, including research-related treatment and consequences of refusing to sign the authorization if applicable.
    i. A statement of the potential risk that PHI will be re-disclosed by the recipient and no longer protected by the Privacy Rule, which can be a general statement in the authorization that the Privacy Rule may no longer protect disclosed health information.

5. The requested PHI must be limited to the information necessary to carry out the applicable research protocol consistent with HIPAA's 'minimum necessary' standard.
6. An individual who participates in research has the right to access their own PHI.
7. A copy of the authorization must be provided to the individual.
8. An individual may revoke their authorization in writing to the principal investigator at any time but the researcher may continue to use and disclose, for research integrity purposes only, any PHI collected from the individual pursuant to such authorization before it was revoked.

19.3.b.xi. Waiver of Individual Authorization (i.e., Waiver of Authorization)

1. A covered entity is permitted to disclose PHI for research purposes without an individual authorization if an IRB or a privacy board has waived the authorization requirement or has approved a modified authorization.
2. A request for a waiver of authorization must be completed by the researcher and submitted to the IRB along with an IRB submission for prior review and approval.
3. A request for a waiver of authorization is not the same as a request for a waiver of informed consent for research under 45 CFR 46 (opens in a new window).
4. A valid request for a waiver of authorization must contain the following:
   a. A plan to protect personal identifiers from improper use and disclosure;
   b. A plan to destroy the personal identifiers as soon as possible, consistent with the purposes of the research, unless there is a compelling health or research justification for retaining the identifiers or the retention is required by law; and
   c. Adequate written assurances that PHI will not be reused or re-disclosed to any other person or entity, except where required by law, for oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted under HIPAA.
5. To approve a waiver of authorization, an IRB must find that the disclosure poses a minimal risk to privacy based on the adequacy of plans submitted by the researcher and that the research could not be practicably done without the waiver of authorization and without access to and use of the PHI.
6. If a covered entity uses or discloses PHI based on an IRB's approval of a waiver of authorization or an alteration of the authorization requirement, the covered entity must retain the IRB's documentation on which is relied for at least six years from the date the waiver of authorization or alteration of authorization was obtained OR the date when it was last in effect, whichever is later.
7. Before a covered entity uses or discloses protected health information (PHI) for research based on a waiver of authorization or an alteration of authorization, a covered entity must receive documentation showing:
   a. The identity of the approving IRB or privacy board;
   b. The date when the waiver or alteration was approved;
   c. A statement that the IRB or privacy board has determined that all of the specified criteria for a waiver or alteration of authorization were met;
   d. A brief description of the PHI for which use or access has been determined by the IRB or privacy board to be necessary for the specified research;
   e. A statement that the waiver or alteration of authorization was reviewed and approved under full board or expedited review procedures; and

f. The signature of the IRB or privacy board chair or their designee.

8. The IRB shall maintain the following documentation regarding the waiver of authorization:
   a. A statement identifying the IRB and the date on which the waiver of authorization request was approved;
   b. A description of the PHI for which access has been determined to be necessary;
   c. A statement that the IRB determined that the waiver satisfied the criteria for a waiver of authorization;
   d. A statement that the waiver of authorization has been reviewed and approved under full board or expedited review procedures following the requirements of 45 CFR 46 (opens in a new window); and
   e. The documentation is signed by the IRB chair or their designee.

19.3.c. IRB Functions

19.3.c.i. IRB as a Privacy Board

1. A privacy board is a research review body that may be established to act upon requests for a waiver of authorization or a waiver of the authorization requirement under the HIPAA Privacy Rule for the uses and disclosures of PHI for a particular research study.
2. The NC State University IRB serves as a privacy board for NC State University.
3. When acting as a privacy board, the IRB may waive or alter all or part of the individual authorization requirement for a specified research project or protocol.
4. When acting as a privacy board, the IRB may act upon requests for waivers of authorization or alterations of the authorization requirement to permit covered entities to use and disclose PHI for research.
   a. Before a covered entity can use or disclose PHI for research under a waiver of authorization or an alteration of authorization requirement, it must obtain documentation of approval of the waiver or alteration of the authorization requirement from the privacy board, which at NC State University, is the NC State IRB.
   b. A covered entity may use and disclose PHI without an authorization or with an altered authorization if it received the proper documentation of approval of such alteration or waiver from a privacy board.
   c. A privacy board's review and actions on requests for approval of a waiver of authorization or an alteration of the Privacy Rule's authorization requirement may be conducted through review by the convened privacy board (e.g., convened IRB full board) or, in certain cases, through expedited review procedures.
   d. A waiver or alteration of authorization may be reviewed and approved under full board or expedited review procedures.

19.3.c.ii. Review of Research

1. Exempt Review

   a. Use of PHI may be exempted under the regulations governing human subjects as described in 45 CFR 46.104.d.4 (opens in a new window) discussing research with secondary data for which consent is not required.

b. Secondary data is data generated for a non-research purpose (such as a medical record) that a principal investigator now wishes to use for research purposes.
c. In order for a study using identifiable private information to be exempted, one of the following criteria must be met:
    i. The identifiable private information is publicly available
    ii. Information is recorded by the investigator in such a manner that the identity of the human subjects cannot be readily ascertained directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects
    iii. The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR part 160 (opens in a new window) and 45 CFR 164 subparts A and E (opens in a new window) for the purpose of "health care operations" or "research" as those terms are defined at 45 CFR 164.501 (opens in a new window) or for "public health activities and purposes" as described under 45 CFR 164.512(b) (opens in a new window)
d. Research that qualifies for exemption does not require a justification for a waiver of informed consent but does require individual authorization for the use of PHI or a request for a waiver of individual authorization.
e. Not all uses of PHI in research can be exempted.

2. Non-Exempt (i.e., Expedited or Convened Full Board) Review

a. In order for the IRB to review and approve research with human subjects including PHI, the IRB must find that that research meets the criteria for approval as defined in 45 CFR 46.111 (opens in a new window).

3. Granting Waivers of Individual Authorization

a. Under the HIPAA Privacy Rule, a privacy board or their designee may waive or alter, in whole or in part, the Privacy Rule's individual authorization requirements for the use and disclosure of PHI in connection with a specific research project
b. A waiver in whole occurs when the privacy board or their designee determines that no authorization will be required for a covered entity to use or disclose PHI for a particular research project because section 164.512(i) of the Privacy Rule (opens in a new window) has been met. For example, if a study involved the use of PHI of numerous individuals where contact information is unknown and it would be impracticable to conduct the research if individual authorizations were required, a privacy board could waive the authorization requirements for research participants if they determined that all the privacy rule waiver criteria had been satisfied.
c. If the privacy board or their designee approves a waiver of individual authorization, the receipt of the requisite documentation of approval permits a covered entity to use or disclose PHI for a particular research project without authorization.
d. For a covered entity to use or disclose PHI under a waiver of individual authorization, it must receive documentation of the privacy board's or their designee's determination that the PHI use or disclosure involves no more than minimal risk to the privacy of individuals based on:

i. adequate plan to protect PHI identifiers from improper use and disclosure;
ii. 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
iii. adequate written assurances that the PHI will not be reused or disclosed to any other person or entity except as required by law, for authorized oversight of the research study, or other research for which the use or disclosure of the PHI is permitted by the Privacy Rule.

4. **Granting Alterations of Individual Authorization**
   a. A researcher might request a partial waiver of the individual authorization requirements of the Privacy Rule to allow them to obtain necessary PHI to contact and recruit potential research subjects.
   b. Even if a privacy board does not waive the individual authorization requirement for the entire study, the privacy board may partially waive the authorization requirement to permit the covered entity to disclose PHI to a researcher for the purposes of contacting and recruiting individuals to a research study.
   c. A privacy board may also approve the request that removes some, but not all, required elements of an individual authorization, known as an alteration. For example, a privacy board may approve an alteration of the authorization to remove the element that describes each purpose of the requested use or disclosure where, for example, the identification of the specific research study would affect the results of the study.
   d. Before a covered entity could use or disclose PHI pursuant to an altered individual authorization, however, it would need to receive documentation that a privacy board determined that all the Privacy Rule waiver criteria at section 164.512(i)(2)(ii) (opens in a new window) had been satisfied.
   e. Any subsequent use or disclosure of PHI by a covered entity for a different research study would require an additional individual authorization except as permitted without authorization under section 164.512(i) (e.g., with a waiver of authorization) (opens in a new window) or 164.514(e) (i.e., as a limited data set with a data use agreement) (opens in a new window).
   f. For a covered entity to use or disclose PHI under a waiver of individual authorization, it must receive documentation of the privacy board's determination that the PHI use or disclosure involves no more than minimal risk to the privacy of individuals based on:
      i. adequate plan to protect PHI identifiers from improper use and disclosure;
      ii. 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
      iii. adequate written assurances that the PHI will not be reused or disclosed to any other person or entity except as required by law, for authorized oversight of the research study, or other research for

which the use or disclosure of the PHI is permitted by the Privacy Rule.