HIPAA COMPLIANCE

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) also known as the Privacy Rule specifies the conditions under which protected health information may be used or disclosed by entities that maintain the records containing the protected health information. Protected health information is defined in the regulation (45 CFR Parts 160 and 164) as individually identifiable health information. HIPAA defines health information as "…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."

Who must be compliant with HIPAA?

This regulation applies to: (1) health plans; (2) health care clearinghouses; and (3) health care providers who transmit any health information in electronic form in connection with a covered transaction. Typical examples of institutions that must comply with HIPAA would be: insurance companies, insurance services, health maintenance organizations, hospitals, large medical institutions, doctors and dental offices. Because the primary mission of ISU is education, only part of its activities include covered functions according to HIPAA. Based on the regulations, ISU is a "hybrid entity." The following ISU departments have been identified as part of the "hybrid entity" and must comply with HIPAA: Thielen Student Health Center and Pharmacy, ISU Student Counseling, Cyclone Sports Medicine/Physical Therapy, ISU Athletic Training Department, and the ISU Benefits Office that administers the ISU Health Plans covered by HIPAA. HIPAA also requires compliance from the following departments that provide support to the identified departments: Administrative Data Processing, Accounts Receivable, Internal Audit, University Counsel and Risk Management.

How does HIPAA affect ISU researchers?

All investigators, including faculty, staff or students, conducting human subject research that wish to access protected health information (PHI) for research purposes must comply with the HIPAA regulation. The regulation applies to clinical trials, behavior and social science studies, medical record reviews, epidemiological studies as well as basic science research. The Privacy Rule contains six provisions under which covered entities may use or disclose protected health information to investigators for research purposes.

How the Privacy Rule works?

In general, investigators wishing to obtain protected health information from a covered entity must have a signed authorization from the individual or patient giving permission for the release of his or her protected health information maintained by that covered entity. The regulations

allow covered entities to use or disclose protected health information without a signed authorization, but this may be done in only five circumstances.

RESEARCH USE AND DISCLOSURE WITH AN AUTHORIZATION

Investigators who will obtain PHI with an authorization must use an authorization document that contains core elements and required statements as specified by HIPAA. This authorization may be prepared by the researcher or provided by the entity that maintains the records needed to be accessed by the researcher. The core elements in an authorization for disclosure and use of PHI are different from the elements required for informed consent according to the Common Rule (45 CFR 46). The core elements and required statements are listed below.

Required Core Elements of an Authorization [45 CFR 164.508 (c)(1)]

A valid authorization must contain at least the following elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- Who may use or disclose the information.
- Who may receive the information.
- A description of each purpose of the requested use or disclosure.
- An expiration date or an expiration event that relates to the individual or the purposes of the use or disclosure. The regulation specifically allows for the expiration date to be "end of research study" or even "none".
- Signature of the individual and date the authorization is signed.

Required Statements of an Authorization [45 CFR 164.508 (c)(2)]

In addition to the core elements, the authorization must contain a statement to inform the individual of the following:

- The individual's right to revoke the authorization in writing, the exceptions to the right to revoke, and a description of how the individual may revoke the authorization.
- The right to refuse to sign the authorization and that the individual may be excluded from participation in the research.

If the authorization does not contain all of the key elements and required statements it is not in compliance with the federal regulations. Authorizations must be written in plain language. Investigators must provide the individual with a **copy of the signed authorization**. The informed consent document and the authorization document can be combined according to the regulation; however, at ISU the documents will be kept separate, as the authorization will be reviewed for completeness and accuracy by the covered entity office and not by the IRB. The IRB will continue to review informed consent documents. Prior to use of an authorization, investigators should either submit an authorization template to the covered entity that they wish to obtain information from for their review and approval or request that the covered entity provide a copy of the authorization form used by the covered entity.

RESEARCH USE AND DISCLOSURE WITHOUT AN AUTHORIZATION

As stated above, the Privacy Rule allows covered entities to release PHI to an investigator without a signed authorization in five cases.

1. Reviews Preparatory to Research [45 CFR 164.512 (i)(1)(ii)]

   In this case the investigator must assure the covered entity that:

   (A) Use or disclosure of the PHI is sought solely to review health information as necessary to prepare a research protocol or for similar purposes preparatory to research;
   (B) No protected health information will be removed from the covered entity by the researcher in the course of the review; and
   (C) The protected health information for which use or access is sought is necessary for the research purpose.

   An example for this provision might be to verify the feasibility of conducting a study.

2. Research on Decedent's Information [45 CFR 164.512 (i)(1)(iii)]

   A covered entity may use or disclose PHI for research, provided that the covered entity obtains from the researcher:

   (A) Representation that the use or disclosure is sought solely for research on the PHI of the decedents;
   (B) Documentation of the death of such individuals, if requested by the covered entity; and
   (C) Representation that the PHI is necessary for the research purposes.

3. De-identified Health Information [45 CFR 164.514 (a)(2)(i)]

   Health information is considered de-identified when it does not identify an individual and the covered entity has no reasonable basis to believe that the information can be used to identify an individual. The information is considered de-identified if the following 18 identifiers are removed and if the remaining health information could not be used alone, or in combination, to identify a subject of the information.

   1. Names;
   2. 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 Census: (a) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (b) the initial three

digits of a zip code for all such geographic units containing 20,000 or fewer people is 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. Fax 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 number, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of 45 CFR 164.514.

4. Limited Data Set [45 CFR 164(e)(1)]

A covered entity may enter into a data use agreement with an investigator. The agreement allows the covered entity to use or disclose a limited data set that excludes specific direct identifiers of the individual or individual's relatives, household members or employer. The data use agreement must:

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 Privacy Rule if done by the covered entity.
2. Establish who is permitted to use or receive the limited data set; and
3. Require the recipient to agree to the following:

   (a) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
   (b) Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;
   (c) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement that it becomes aware of;
   (d) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
   (e) Not identify the information or contact the individuals.

The following direct identifiers must also be removed from the information:

1. Names;
2. Postal address information, other than town or city, state and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers,
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

Waiver of Authorization [45 CFR 146.512 (i)(1)(ii)]

A covered entity may allow use and disclosure of protected health information if a privacy board or an Institutional Review Board waives the requirement for an authorization. The documentation of the waiver of authorization must be submitted to the covered entity from which the investigator wants to receive the PHI. The IRB at ISU will review requests for waiver of authorizations for covered entities at ISU. Investigators who wish to receive a waiver of authorization from a covered entity outside of ISU must contact that entity for information about applying for a waiver.

A privacy board or IRB may approve an alteration or waiver of authorization, in whole or in part, if the following criteria is satisfied and documented according to the Privacy Rule.

A) The use or disclosure of protected health information involves no more than 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.
    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 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 for other research for which the use or disclosure of PHI would be permitted by this subpart;

B) The research could not practicably be conducted without the waiver or alteration; and

C) The research could not practicably be conducted without access to and use of the protected health information.

Request for use of PHI for reviews preparatory to research, research on decedent information, de-identified health information and limited data sets will be reviewed by the covered entity from which the PHI will be obtained.