Reported to the Board of Trustees
May 19, 2016

UNIVERSITY OF ILLINOIS HIPAA PRIVACY AND SECURITY DIRECTIVE

UNIVERSITY OF ILLINOIS HIPAA PRIVACY AND SECURITY DIRECTIVE

Table of Contents

DIRECTIVE INFORMATION

Directive Owner: University Privacy and Security Official
Approved by: University Privacy and Security Official
Date Approved: 5/9/2016
Effective Date: 5/9/2016
Date Amended (most recent): N/A
Targeted Review Date: 5/9/2017
Contact: University Privacy and Security Official at hipaa@uillinois.edu

BACKGROUND

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its companion regulations (the Privacy, Security, Breach Notification and Enforcement Rules) is intended to assure the privacy and security of health information held or transmitted by Covered Entities and their Business Associates. A Covered Entity is a Health Plan, a Health Care Clearinghouse or a Health Provider that transmits health information in electronic form in connection with specific financial and administrative transactions identified by the U.S. Department of Health and Human Services.

The University of Illinois (UI) is a Covered Entity because certain UI units perform HIPAA-covered functions or activities. The majority of UI units, however, do not perform HIPAA-covered functions or activities. The Privacy Rule permits Covered Entities that perform both covered and non-covered functions to designate themselves Hybrid Entities so as to limit their HIPAA compliance efforts essentially to only those Health Care Components (each an "HCC") that perform HIPAA-covered functions or activities.

APPLICABILITY

This Directive implements the University of Illinois HIPAA Privacy & Security Compliance Policy approved by the Board of Trustees on November 13, 2013. This Directive applies to the Workforce of all HCCs of the UI Hybrid Entity in a manner consistent with the HCC's role as a Health Care Provider (HCC-PR), a Health Plan (HCC-PL) or a Business Associate (HCC-BA). The Privacy Official will identify and classify the role of each HCC and maintain and publish a current list of HCCs.

OBJECTIVE

The objective of this Directive is to ensure the privacy, security, Integrity, and Availability of Individuals' health information held or transmitted by UI's designated HCCs and UI's Business Associates.

DEFINITIONS

This Directive uses many defined terms with specific meanings. To assist with identifying defined terms throughout this Directive, defined terms always begin with capital letters wherever they appear. The Glossary (Appendix A) contains definitions of all defined terms used in this Directive.

DIRECTIVE

This Directive is intended to ensure that Protected Health Information (PHI) in the control of the Hybrid Entity is used and disclosed in a manner that protects privacy and is consistent with applicable state and federal law and industry best practices. This Directive also establishes the Hybrid Entity's security and Breach notification responsibilities, outlining the security measures and methods of implementing standards to adequately safeguard PHI, including electronic PHI (ePHI), and respond appropriately to incidents of Breach. The Privacy Official, in consultation

with the Security Official, may enter into memoranda of understanding with HCCs to delegate specific responsibilities or to grant Policy exceptions that are consistent with HIPAA and other relevant laws and UI policies. Any supplemental policies and procedures adopted by an HCC must be consistent with this Directive.

Situations involving certain types of PHI (such as that involving HIV, substance abuse, mental health, developmental disabilities and genetic information), certain patients (such as minors, students, and sexual assault victims) or certain legal representatives (such as court-appointed guardians or persons acting pursuant to health care powers of attorney), may require compliance with laws that offer greater privacy protections than HIPAA. If you are dealing with such a situation, contact the Privacy Official or the Office of University Counsel for guidance.

I. PRIVACY

A. HIPAA Privacy Official

1. UI has a Privacy Official, appointed by the President, whose responsibility is to ensure the Hybrid Entity's compliance with the HIPAA Privacy Rule and other applicable laws related to privacy of Health Information. The Privacy Official's responsibilities include, but are not limited to, the following:

    a. Developing and implementing the policies and procedures of the Hybrid Entity, as required by the Privacy Rule;

    b. Monitoring HCC compliance with the Privacy Rule;

    c. Regularly reviewing the activities of the University to ensure HCCs are properly identified and documented in writing;

    d. Serving as a compliance resource to the HCCs;

    e. Developing and maintaining HIPAA training and maintaining related records; and

    f. Receiving, investigating, and recommending resolution of complaints concerning the University's compliance with the Privacy Rule.

2. The Privacy Official may assign other persons (including but not limited to the HIPAA Liaisons) to assist with any of the above responsibilities. The name, location, e-mail, and telephone number of the Privacy Official is to be publicized throughout each HCC in the event that an Individual elects to file a complaint. This same information is to be provided, as appropriate, with correspondence from each HCC pertaining to PHI.

B. Permitted Uses and Disclosures of PHI

The HIPAA Privacy Rule regulates each HCC's use and disclosure of PHI. This section summarizes permitted uses and disclosures of PHI under the Privacy Rule. Other state or federal laws may impose more stringent restrictions on use or disclosure of PHI associated with certain health conditions or treatments (e.g., HIV status, substance abuse treatment, mental health and/or developmental disabilities, or genetic information). Before disclosing or using PHI in situations involving those health conditions or treatments, consult with the Privacy Official or the Office of University Counsel.

1. Uses and Disclosures Not Requiring Authorization or an Opportunity to Agree or Object. The Privacy Rule permits an HCC to use and disclose PHI about an Individual without obtaining the Individual's authorization and without providing the Individual with an opportunity to agree or object under the following specific circumstances.

    a. For Treatment. The HCC may use or disclose PHI about an Individual to facilitate medical treatment or services by the HCC-PR or other providers. The HCC may disclose PHI about an Individual to doctors, nurses, technicians, medical students, or other Health Care Providers who are involved in taking care of the Individual. For example, the HCC may disclose to a treating surgeon the name of an Individual's treating endocrinologist so that the surgeon may ask for the Individual's blood test results from the treating endocrinologist.

    b. For Payment. The HCC may use and disclose PHI about an Individual for its own Payment activities or for another Covered Entity's Payment activities. For example, the HCC may disclose PHI about an Individual to that Individual's insurance company in order to determine what portion of the HCC-PR's bill for treatment and services will be paid by that insurance company.

    c. For Health Care Operations. The HCC may use and disclose PHI about an Individual for its own Health Care Operations or certain Health Care Operations of another Health Care Provider if that other provider also has a relationship with the patient who is the subject of the PHI and certain other conditions apply. For example, the HCC may use PHI about its patients to review, assess, compare and improve the skills of individual staff members and the overall level of care provided by the HCC. The HCC also may use or disclose PHI to conduct training programs in which students, trainees or practitioners in health care learn under supervision to practice or improve their skills as health care providers.

    d. For Uses or Disclosures Required by Law. The HCC will disclose PHI about an Individual when required to do so by applicable law, provided that the use or disclosure complies with and is limited to the relevant requirements of such law. Examples of Illinois laws that may require disclosure of PHI include, but are not limited to, the following:

        (1) Abused and Neglected Child Reporting Act

        (2) Communicable Disease Report Act

        (3) Firearm Owners Identification Card Act

    e. For Uses and Disclosures Permitted by Law. The Privacy Rule permits, but does not require, an HCC to use and disclose PHI about an Individual under the following specific circumstances.

        (1) Uses and disclosures for public health activities;

        (2) Disclosures about victims of abuse, neglect or domestic violence;

        (3) Uses and disclosures for health oversight activities;

(4) Disclosures for judicial and administrative proceedings;

(5) Disclosures for law enforcement purposes;

(6) Uses and disclosures about decedents;

(7) Uses and disclosures for cadaveric organ, eye or tissue donation purposes;

(8) Uses and disclosures for research purposes (See Section I. K.);

(9) Uses and disclosures to avert a serious threat to health or safety;

(10) Uses and disclosures for specialized government functions;

(11) Disclosures for Workers' Compensation

2. Uses and Disclosures that Require Providing the Patient with an Opportunity to Agree or Object. Under the circumstances set forth in this section, the Privacy Rule permits an HCC to use and disclose PHI about an Individual after informing the Individual in advance of the use or disclosure and providing the Individual an opportunity to agree to or prohibit or restrict the use or disclosure. Disclosures made pursuant to this section are not required to be included in the accounting of disclosures to the Individual.

   a. Disclosure of PHI to Family and Friends Involved in the Care of the Patient. The HCC may use or disclose a patient's PHI to a family member, relative, or close personal friend of the patient or any other person identified by the patient. Such PHI shall be limited to that directly relevant to that person's involvement with the patient's care or Payment related to the patient's care.

      (1) Patient Present. If the patient is present or otherwise available prior to such disclosure and has the capacity to make health care decisions, the HCC must:

         (a) Obtain the patient's agreement;

         (b) Provide the patient with the opportunity to object to the disclosure; or,

         (c) Reasonably infer from the circumstances, based on the exercise of professional judgment, that the patient does not object to the disclosure.

      (2) Patient Absent. If the patient is not present, or the opportunity to agree or object cannot practicably be provided due to the patient's incapacity or emergency circumstances, the HCC should exercise professional judgment to determine whether disclosure is in the best interests of the patient.

   b. Disclosure for Notification Purposes. The HCC may use or disclose a patient's PHI to notify, or assist in the notification of (including identifying or locating) a family member, personal representative of the patient, or another person responsible for the care of the patient, of the patient's location, general condition, or death. The HCC must provide the patient an opportunity to agree or object as described in subsection (a) above.

   c. Disclosure in Disaster Relief Situations. The HCC may use or disclose a patient's PHI to a public or private organization authorized by law or by its charge to assist in disaster relief efforts, for the purpose of coordinating with such entities for the notification of, or to assist in the notification of (including identifying or locating), a

family member, a personal representative of the patient, or another person responsible for the care of the patient, of the patient's location, general condition, or death. The opportunities to agree or object as described in subsection (a) above must be provided to the patient.

d. Use and Disclosure for Facility Directories. The HCC may use the following PHI to maintain a directory of patients in the HCC facility and to disclose the information to members of the clergy or to disclose the information (other than religious affiliation) to other persons who ask about the Individual by name:

(1) Name;

(2) Individual's location in the facility;

(3) Individual's condition in general terms; and

(4) Individual's religious affiliation.

e. Disclosures Involving Deceased Individuals. The HCC may disclose the PHI of a deceased Individual to a family member or to other persons who were involved in the Individual's care or Payment for health care prior to death unless doing so is inconsistent with any prior preference expressed by the Individual to the HCC.

3. Uses and Disclosures Requiring an Authorization. As a general rule, an HCC may not use or disclose PHI without a "valid" authorization that complies with the Privacy Rule. When an HCC obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure must be consistent with the authorization.

a. Research. With a few exceptions, the use or disclosure of PHI for research purposes requires an authorization from the Individual whose PHI is to be used or disclosed. As more fully described in Section I.K., only in the following instances may PHI be used for research purposes without an authorization:

(1) An institutional review board ("IRB") or privacy board has granted a waiver or alteration of the authorization requirement;

(2) The research requires use of a Limited Data Set under a data use agreement entered into by UI and the data recipient;

(3) The information is needed for activities preparatory to research and the researcher has made certain representations;

(4) The research requires use of information about decedents only; or

(5) The information is de-identified in accordance with the Privacy Rule. See section I.F.

b. Disclosures at a patient's request (including to a patient's attorney) generally require an authorization.

c. Most disclosures for marketing purposes require an authorization. See Section I.I., below.

d. Most disclosures for fundraising purposes require an authorization. See Section I.J., below.

e. Disclosures to a patient's employer generally require an authorization, unless disclosure is for Worker's Compensation purposes.

f. Most uses or disclosures of psychotherapy notes require an authorization, except where necessary to carry out Treatment, Payment or Health Care Operations, or for an HCC's use in its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills.

4. Disclosures to an Individual: With limited exceptions, the HCC is required to disclose an Individual's PHI to the Individual or the Individual's Personal Representative when the Individual or his/her Personal Representative requests access to the PHI. The Privacy Rule treats the Personal Representative of an adult or of an emancipated minor as the Individual in health care matters that relate to the representation, including the right to access PHI. However, the authority and scope of a Personal Representative's access will depend on the authority and scope granted to the Personal Representative by state law.

   a. Verification. An HCC must verify the identity of a person requesting PHI, the authority of any such person to have access to PHI, and the scope of his or her access, if the identity or authority of the person is not known to the HCC. Verification may be done orally or in writing and, in many cases, the type of verification may depend on how the Individual is requesting or receiving access (e.g., written authorization or web portal access) or the basis of authority as a Personal Representative (e.g., court appointed guardian or health care power of attorney).

   b. Required Documentation. An HCC must obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the disclosure (e.g., a valid HIPAA authorization or valid health care power of attorney). An HCC may rely, if reliance is reasonable under the circumstances, on the provided documentation, statements, or representations that appear to meet the requirements.

5. Internal Disclosures: An internal disclosure is one made within an HCC provided the recipient has a need to know consistent with this Directive. Access to PHI may be provided only in accordance with this Directive. Workforce members requiring the use of PHI during the course of their jobs are responsible for maintaining the confidentiality of the PHI. Individuals engaged in the collection, handling, or dissemination of PHI shall be responsible for protecting that information. Violation of confidentiality of PHI may be cause for disciplinary action up to termination.

C. Prohibited Uses

HCCs are prohibited from selling or disclosing PHI in return for remuneration, regardless of who will receive the remuneration.

D. Authorizations

1. Standard University Authorization Form.

   a. HCCs should use UI's or the HCC's standard HIPAA Authorization Form whenever possible. HIPAA authorization forms submitted by third parties may be accepted provided they meet the requirements set forth in paragraphs 2 and 3, below, at a minimum.

   b. An authorization that includes all of the elements required by the Privacy Rule and set forth in paragraphs 2 and 3, below, may not be sufficient to disclose especially sensitive PHI, such as HIV status, substance abuse treatment, mental health and/or developmental disabilities, or genetic information.

2. Required Elements of a HIPAA Authorization: Except as otherwise permitted in this Directive or as specified by applicable state and federal law (e.g., see paragraph 1.b., above) a valid authorization containing all of the HIPAA-required elements below is required prior to using or disclosing PHI:

   a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

   b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

   c. The name or other specific identification of the person(s), or class of persons, to whom the HCC may make the requested use or disclosure;

   d. A description of each purpose of the requested use or disclosure. The statement "at the request of the Individual" is a sufficient description of the purpose when an Individual initiates the authorization and does not, or elects not to, provide a statement of purpose;

   e. An expiration date or an expiration event that relates to the Individual or the purpose of the use or disclosure;

   f. A statement regarding the patient's right to revoke the authorization in writing and the limitations on that right;

   g. A description of how the patient may revoke the authorization;

   h. A statement indicating that the PHI disclosed pursuant to the authorization may be re-disclosed by the recipient and no longer protected by the Privacy Rule;

   i. A statement of the HCC's ability or inability to condition treatment, Payment, enrollment, or eligibility for benefits on the authorization; and

   j. Signature of the Individual and date. If the authorization is signed by an authorized representative of the Individual, a description of such representative's authority to act for the Individual also must be provided.

3. Validity:

   a. An authorization must be in writing to be valid.

   b. An authorization is invalid if any of the elements required by section (D)(2) above are missing or appear to have been falsified or amended without indication that the patient is aware of the amendment.

   c. A photocopy of an authorization is acceptable.

   d. If there is any doubt about the validity of an authorization, the authorization must be rejected and the PHI sought may not be disclosed.

   e. The original or photocopied authorization must be filed in the patient's Record.

   f. An Individual may revoke an authorization in writing. Revocation will be effective only for future uses and disclosures of PHI. The revocation will not be effective for uses or disclosures of PHI that already have occurred in reliance on the authorization.

4. Authorization in Certain Special Situations. Use or disclosure determinations in the following special situations are fact-specific and require an understanding of applicable federal and state laws and regulations. In these situations, you should contact the Privacy Official or the Office of University Counsel for assistance.

   a. Emancipated, Pregnant or Married Minors – Consent and Authorizations.

      (1) Emancipated minors between 16 and 18 who have an emancipation order, pregnant married minors, and minors who are parents may consent for their own treatment. The consent of a parent is not required. Furthermore, the parent is not the minor's Personal Representative under the Privacy Rule and has no right to access an emancipated minor's PHI unless specifically allowed by law. Otherwise, the minor must authorize disclosure.

      (2) Other minors of various ages may consent for their own treatment based on the type of treatment sought (e.g., sexual assault and counseling, inpatient and outpatient mental health, HIV testing, drug and alcohol, sexually transmitted diseases, birth control, abortion, and blood donation). In most of these circumstances, parents have limited rights to access the minor's PHI. Contact the Privacy Official for assistance.

   b. Patient Not Physically Able To Sign: Have the patient sign with an "X" and have the mark witnessed by two staff members. If the patient is unable to make an "X", document that the request was fully explained to the patient and that the patient understands the nature of the request. Two individuals must witness this procedure and sign the authorization.

   c. Authorization by a Person Other than the Patient: If the patient cannot give authorization, persons authorized by the patient may give authorization under certain circumstances set forth below. In instances where documentation/proof of legal relationship is required, a copy of the proof shall be retained in the patient's medical Record.

(1) Minors: A "minor" means a person who is less than 18 years of age. In general, only a parent, guardian, or legal custodian may consent for medical treatment of a minor, and as a general rule, the parent, guardian, or legal custodian of a minor has access to the minor's PHI, as his or her Personal Representative. Generally, the parent, guardian, or legal custodian must authorize to the release of PHI for a minor. If there is any question as to the legitimacy of the authority of a parent, guardian, or legal custodian to release information, proof of legal relationship will be required.

(a) Divorced Parents: In the case of divorced parents, either parent can authorize release of information unless the parent's right to access medical, dental or psychological records has been terminated through court order or via the approved parenting plan pursuant to state law. If there is any question of the legitimacy of the authority of a divorced parent with respect to a child's PHI, proof of legal relationship will be required.

(2) Deceased Patient: Any authorization signed by the patient is invalid after death. Any of the following can authorize disclosure from records of deceased patients:

(a) A court-appointed personal representative, bearing appropriate documentation to prove this status;

(b) The surviving spouse, or of there is no surviving spouse, an adult child, a parent, a grandparent, an adult sibling, or an adult sibling's spouse; or,

(c) An executor or administrator or other person that has the authority to act on behalf of the deceased Individual or of the deceased's estate.

(3) Health Care Power of Attorney: Any individual who is authorized under a health care power of attorney to make health care decisions on behalf of the patient may give a valid authorization for the patient.

(4) Person Adjudged Incompetent: A legal guardian of the person appointed by the court may authorize release of the ward's PHI. Letters of Guardianship of the Person must be displayed by the guardian before an authorization signed by such individual will be honored to release PHI. A legal guardian of the estate, on the other hand, is not legally authorized to release medical Records of the ward.

(5) Other Incompetent Persons: Where there is reason to believe that a patient is not competent to authorize the release of PHI, but the patient has not been declared incompetent by a court, contact the Privacy Official.

5. Transmission of PHI by Phone or in Person:

a. If an inquiring individual contacts the HCC regarding another Individual's health status or other PHI, the HCC should, if required by applicable sections of this Directive, try to obtain oral agreement from the affected Individual that PHI may

be shared with the inquiring individual before communicating with the inquiring individual, the minimum necessary information may be disclosed.

b. If the affected Individual is not available at the time an inquiry is made, the HCC will:

(1) Verify the identity of the individual and his or her relationship to the affected Individual; and,

(2) Review the affected Individual's records to determine whether such individual is explicitly authorized to receive protected health information about the patient.

6. Oral Conversations. HCC Workforce members will ensure the privacy of all conversations or discussions involving PHI.

7. Documentation and Recordkeeping Requirements. The HCC must document and maintain each authorization for at least six years from the date of its creation or the date when it was last in effect, whichever is later. HCC's should consult UI and unit record retention policies in the event longer retention periods are prescribed.

E. Minimum Necessary Rule. When using or disclosing PHI or when requesting PHI from another Covered Entity, the HCC will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. However, the minimum necessary standard will not apply in the following situations:

1. Disclosures to or requests by a Health Care Provider for Treatment;
2. Disclosures made to comply with HIPAA (including to the Secretary of the U.S. Department of Health and Human Services);
3. Uses or disclosures that are required by law; and
4. Uses or disclosures made pursuant to an authorization signed by the Individual or his/her Personal Representative.

F. De-Identification.

1. An HCC may de-identify PHI in two ways:

a. By removing specific direct and indirect identifiers from the Record (known as the Safe Harbor); or,

b. Through statistical verification (known as the Expert Determination Method).

2. In order to satisfy the Safe Harbor, the HCC must strip the following 18 direct and indirect identifiers from the PHI:

a. Names;

b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and the equivalent geographical codes except for the first 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; or (b) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000;

c. All elements of dates (except year) for dates directly related to an Individual, including:

   (1) Birth date;

   (2) Admission date;

   (3) Discharge date;

   (4) Date of death; and,

   (5) All ages over 89 including the year, except it may be aggregated into a single category of 90 and over.

d. Telephone numbers;

e. Fax numbers;

f. E-mail address;

g. Social security numbers;

h. Medical record numbers;

i. Health plan beneficiary numbers;

j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; and

r. Any other unique identifying number, characteristic, or code, except as permitted to allow the organization the ability to re-identify the Individual upon the return of the information.

3. Under the Expert Determination Method, an HCC may use an expert with "appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" to determine that there is a "very small" risk that the information, alone or in combination

with other reasonably available information, could be used by the researcher to identify the Individual who is the subject of the information. The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination. The HCC must keep such certification, in written or electronic format, for at least six years from the date of its creation or the date when it was last in effect, whichever is later.

4. The HCC may, without patient authorization, either use PHI as permitted under the HIPAA Privacy Rule to create De-Identified Information, or disclose PHI to a Business Associate in order to create De-Identified Information, whether or not the De-Identified Information is to be used by the HCC or disclosed to another entity or individual.

5. The HCC may assign a code or other means of record identification to allow De-Identified Information to be re-identified by the HCC, provided that the code or other means of record identification is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient; and the HCC does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification. No member of the researcher's team may be given the code or other means that would allow re-identification of the data.

G. Limited Data Sets.

1. The HCC may use or disclose a Limited Data Set only for purposes of public health activities, research, or Health Care Operations and only after UI enters into a data use agreement with the person or entity sharing or disclosing the Limited Data Set that meets the following requirements of the HIPAA Privacy Rule. A Limited Data Set is not completely de-identified and is PHI. Unlike De-Identified Information, a Limited Data Set may contain the following indirect identifiers: dates (such as dates of birth, death, admission, discharge and service); geocodes (city, state, zip); and ages.

2. The data use agreement must:

   a. Establish the permitted uses and disclosures of such information by the Limited Data Set recipient, which may be for research, public health activities or Health Care Operations.

   b. Establish who is permitted to use or receive the Limited Data Set; and

   c. Provide that the Limited Data Set recipient will:

      (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

      (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

      (3) Report to the Privacy Official any use or disclosure of the information not provided for by the data use agreement of which it becomes aware;

      (4) Ensure that any agent to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient; and

(5) Not identify the information or contact the individual.

3. The responsible contracting office will make sure that a copy of each data use agreement entered into is retained for at least six years from the expiration or termination of the data use agreement. The responsible contracting office should also consult UI and unit record retention policies in the event longer retention periods are prescribed.

4. An HCC may create a Limited Data Set by removing the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:
   a. Name
   b. Postal address information other than town or city, state and zip code
   c. Phone numbers
   d. Fax numbers
   e. E-mail addresses
   f. Social security number
   g. Medical record number
   h. Health plan beneficiary number
   i. Account numbers
   j. Certificate/license numbers
   k. Vehicle identifiers and serial numbers
   l. Device identifiers and serial numbers
   m. URLs
   n. Internet protocol (IP) address numbers
   o. Biometric identifier
   p. Full face photographic and any comparable images
5. If an HCC Workforce member becomes aware of a pattern of activity or practice of a Limited Data Set recipient that constitutes a material breach of the data use agreement, that individual must report it to the Privacy Official, per Section III.C.

H. Responding to Certain Requests for Information

1. General. If authorization is not required for the release of PHI, determine if the disclosure needs to be included in any future accounting of disclosures. If so, Section I.L.3 applies. Every effort should be made to process requests for information within thirty (30) days of receipt.
2. Records of Other Health Care Providers. An individual generally has a right to access all of the information about the individual that an HCC-PR maintains in the individual's medical Record, including information the individual provided to the HCC-PR herself, as well as PHI about the individual contributed to the Record by other Health Care Providers and Covered Entities.
3. More Stringent Restrictions. Other state or federal laws may impose more stringent restrictions on use or disclosure of PHI associated with certain health conditions or

treatments. Before disclosing or using PHI in such situations, consult with the Privacy Official or the Office of University Counsel. Examples of health conditions or treatments giving rise to more stringent PHI use or disclosure restrictions include, but are not limited to (visit the HIPAA website for a more comprehensive list):

a. HIV test results
b. Substance abuse Records
c. Mental health, developmental disabilities.
d. Genetic information.

I. Use or Disclosure of PHI for Marketing Purposes: Any HCC must obtain patient authorization prior to using or disclosing PHI for Marketing purposes except if the communication is in the form of a face-to-face communication made by the HCC to an individual or a promotional gift of nominal value provided by the organization. If the Marketing involves direct or indirect remuneration to the HCC from a third party, the authorization must state that such remuneration is involved.

J. Use or Disclosure of PHI for Fundraising Activities

1. Any HCC must obtain patient authorization prior to using or disclosing PHI for fundraising activities, except the HCC may use or disclose to a Business Associate or to an institutionally related foundation the following PHI for the purpose of raising funds for its own benefit:

   a. Demographic information relating to an Individual, consisting of names, addresses, other contact information, age, gender and date of birth;
   b. Health insurance status;
   c. Department where treatment was provided;
   d. Treating physician;
   e. Outcome information, for purposes of excluding Individuals from a fundraising communication; and
   f. Dates of health care provided to an Individual.

2. The HCC must provide a recipient of a fundraising communication with a clear and conspicuous description of how the Individual may opt out of receiving any further fundraising communications and whether the opt-out pertains to all future fundraising or to a specific fundraising activity. The opt-out method may not impose an undue burden or more than nominal cost on the Individual. The HCC must treat opt-out requests as a revocation of authorization.

3. The HCC may provide a method for opting in to fundraising communications that is not targeted toward specific Individuals who have opted out of future fundraising communications.

4. The HCC may not condition treatment on receipt of fundraising communications.

5. The HCC shall maintain a list of all Individuals who have opted out from its fundraising communications and shall not send fundraising communications to the Individuals within the scope of the opt-out.

6. The HCC must identify and use or disclose only the minimum set of PHI necessary when using or disclosing PHI for fundraising.

K. Use or Disclosure of PHI for Research Purposes.

1. Conditions under which PHI may be used or disclosed for research purposes are:

   a. Authorization from the Individual research participant or his or her legally authorized representative (See Section I.D.).

   b. Waiver of Authorization approved by a duly constituted institutional review board (IRB) or privacy board based on the following criteria:

      (1) The use of PHI presents no more than a minimal risk to the privacy of the subject based on, at least, the presence of an adequate plan to protect identifiers from improper utilization; 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 adequate written assurance that the PHI won't 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 of PHI would be permitted by the Privacy Rule;

      (2) The research could not practicably be conducted without the waiver; and

      (3) The research could not practicably be conducted without access to and use of the PHI.

   c. Limited Data Set and Data Use Agreement (See Section I.G.).

   d. De-identified Data (See Section I.F.).

      Note: An HCC may assign a code or other means of record identification to allow De-Identified Information to be re-identified by the HCC, provided that the code or other means of identification is not derived from or related to information about the Individual and is not otherwise capable of being translated so as to identify the Individual; and the HCC does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification. No member of the researcher's team may have access to the code or other means that would allow re-identification of the data.

   e. Activities Preparatory to Research, provided that the researcher has made a written representation to the HCC that:

      (1) Use is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;

      (2) No PHI is to be removed from the HCC by the researcher in the course of the review; and

(3) The PHI for which access is sought is necessary for the research purposes.

The IRB will review all proposed screenings of Records for recruitment of research participants as part of the protocol approval process unless the research is exempt from the regulations protecting human subjects.

f. Research on Decedents, provided that the researcher represents in writing to the HCC that the use is solely for research that involves the PHI of decedents and the PHI is necessary for the research. The HCC may request documentation of the death of the Individuals about whom PHI is being sought.

2. As a general rule, HCCs may not condition a patient's Treatment, Payment, enrollment in a Health Plan, or eligibility for benefits on providing an authorization; however, one exception to this rule is that an HCC-PR may condition its provision of research-related treatment (e.g., a clinical trial), on the patient providing an authorization permitting uses and disclosures of PHI for the research.

L. Individual Rights Regarding PHI: Individuals have the following rights regarding PHI that the HCC maintains about them. Unless otherwise specified in the Business Associate Agreement (BAA) when a Business Associate receives a request from an Individual regarding his or her rights, the Business Associate should coordinate with the Health Care Provider and/or Health Plan, as applicable, to facilitate an appropriate and timely response.

1. Right of Access: Subject to certain exceptions, which are identified on the HIPAA website, Individuals have the right to inspect PHI about them that is maintained by the HCC in any Records within a Designated Record Set. If an Individual requests a copy of the information, the HCC may charge a fee for the costs of copying, mailing or other supplies associated with the request. If an Individual requests a copy of the information in electronic format and the HCC maintains the information electronically, the HCC will provide the Individual with access to the information in the requested electronic format, if it is readily producible in such format; or, if not, in a readable electronic format as agreed to by the HCC and the Individual.

a. Requests for Access: The HCC-PR or HCC-PL that maintains the PHI in question will be responsible for responding to all requests for patient access to PHI contained in the Designated Record Set. The HCC's personnel will not attempt to explain or interpret any part of the PHI. The patient or patient's Personal Representative will be referred to the physician or other responsible healthcare professional for any necessary assistance in understanding the PHI. A minor has the right to inspect or obtain copies of his/her Records maintained in a Designated Record Set in any situation where the minor consented to care. In these instances, the parent has no right or limited right to access the minor's PHI within a Designated Record Set.

b. Procedure: Patients must submit a written, signed authorization/request to the HCC and furnish sufficient identification. A patient may request to inspect Records or request copies of Records maintained in the Designated Record Set. If the patient wishes to have copies of any part of the Records, he/she must so indicate by describing that part of the Records in his/her written request.

(1) Prior to permitting an inspection or providing copies of Records, HCC Workforce members will review the Designated Record Set to ensure

completeness of all Records within the Designated Record Set. The HCC may consult the attending physician to ensure the Record is complete.

(2) When a Workforce member of an HCC reasonably believes that an Individual has been or may be subjected to domestic violence, abuse or neglect by a Personal Representative, or that treating a person as the Individual's Personal Representative could endanger the Individual, then the HCC may choose not to treat that person as the Personal Representative if, in the exercise of professional judgment, doing so would not be in the best interests of the Individual.

(3) Inspection of Records: An HCC must act on a request to inspect PHI in a Designated Records Set within 30 days following receipt of a written, signed request or valid authorization. If the HCC is unable to respond within 30 days, it may extend the deadline one time by no more than 30 days by notifying the Individual in writing of the new deadline with an explanation for the delay. Inspections of Records must be conducted at the HCC under the direct supervision of designated HCC Workforce member.

(4) Denial of Request. If an Individual's request for access to or a copy of the PHI in any Designated Records Set is denied, in whole or in part, the HCC will notify the Individual in writing and include the specific reason for the denial with information on the Individual's right, if any, to request a review of the denial. (Under certain circumstances, the Individual has the right to have the denial reviewed by a licensed health care professional, chosen by the Privacy Official, who did not participate in the original decision to deny.)

(5) Copies of Records: If copies are requested, they will be sent by mail within 30 days of receipt of the request or valid authorization unless other mutually agreeable arrangements are made (e.g., patient pick-up). If a request cannot be processed within 30 days, the HCC will notify the requestor that the deadline has been extended by no more than 30 days.

(6) Cost-Based Fee for Providing Copies: An HCC may impose a reasonable, cost-based fee for providing copies of PHI requested by an Individual entitled to receive them. All fees for providing copies will be explained to and collected from the requester prior to the HCC complying with the request. Fees may include the cost of labor for copying the PHI (but not any PHI search costs); supplies for creating the copy of the PHI; postage (if applicable); and the cost of preparing an explanation or summary of the PHI, if agreed to by the Individual.

(7) Documentation: All requests will be retained with documentation as to the disposition of the request, type of access, date and name of person processing the request.

2. Right to Request Amendment: If an Individual feels that the PHI or a Record that the HCC maintains about him/her in a Designated Record Set is incorrect or incomplete, the Individual may request that the HCC amend the PHI or Record. All requests to amend must be in writing and include a reason for the request. An Individual has the right to request an amendment for as long as the information is kept by the HCC.

a. The HCC must act on an Individual's request for amendment within 60 days after receipt of such a request. If the HCC is unable to act on the request within 60 days, the HCC may extend the time to respond for up to a maximum of 30 additional days, provided that the HCC gives the Individual a written statement for the reasons for the delay and the date by which the HCC will respond to the request.

b. If the HCC accepts the requested amendment, in whole or in part, it must make the appropriate amendment by, at a minimum, identifying the PHI or Records affected by the amendment and appending or otherwise providing a link to the amendment. The HCC must inform the Individual in a timely manner that the amendment is accepted and obtain the Individual's permission to notify the relevant persons with whom the amendment needs to be shared. The HCC will make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the Individual as having received the PHI and needing the amendment and to persons, including Business Associates, that the HCC knows have the PHI that has been amended and may have relied, or could foreseeably rely, on such information to the detriment of the Individual.

c. The HCC may deny an Individual's request for an amendment if it is not in writing or does not include a reason to support the request. In addition, the HCC may deny a request if the request is for the HCC to amend PHI that:

   (1) Is not part of a Designated Record Set maintained by or for the HCC;

   (2) Was not created by the HCC, unless the person or entity that created the information is no longer available to make the amendment;

   (3) Is not part of the information which the Individual would be permitted to inspect and copy; or

   (4) Is accurate and complete.

d. If the HCC denies a request for an amendment, in whole or in part, it must notify the Individual in writing in a timely manner, using plain language, and explain:

   (1) The basis for the denial;

   (2) The Individual's right to submit a written statement disagreeing with the denial and how the Individual may file such a statement;

   (3) That, if the Individual does not submit a statement of disagreement, he/she may request that the HCC provide the Individual's request for an amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

   (4) How the Individual may complain to the HCC, including the name, title, and telephone number of the designated contact person or office, or to the Secretary of the Department of Health and Human Services.

e. The HCC will permit the Individual to file a written statement disagreeing with the denial of all or part of a requested amendment and the basis for such disagreement, subject to a reasonable limit on length. The HCC may prepare a

written rebuttal to the Individual's statement of disagreement, which must be provided to the Individual.

f. The HCC will link or append the request for amendment, the HCC's denial, any statement of disagreement, and any rebuttal to the applicable Record. The HCC must include the request for amendment, the HCC's denial, any statement of disagreement, and any rebuttal, or an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.

g. If the HCC receives a notice from another Covered Entity that it has amended a Record that has been provided to the HCC, the HCC will amend such Records that it maintains.

3. Right to an Accounting of Disclosures: An Individual has the right to request an accounting of disclosures of PHI made by the HCC in the 6 years prior to the date of the request, with certain exceptions.

   a. Accountings do not include disclosures:

      (1) Made to carry out Treatment, Payment, or Health Care Operations;

      (2) To Individuals of PHI about them;

      (3) Incident to a use or disclosure otherwise permitted or required under the HIPAA Privacy Rule;

      (4) Pursuant to an Individual's authorization;

      (5) For the HCC-PR's facility directory or to persons involved in the Individual's care;

      (6) For national security or intelligence purposes;

      (7) To correctional institutions or law enforcement officials; or

      (8) That are part of a Limited Data Set.

   b. Temporary Suspension of Right to an Accounting: The HCC must suspend a patient's right to receive an accounting of disclosures of PHI that has been released to a health oversight agency or law enforcement official if the agency or official provides the HCC with a written statement that says that such accounting is likely to impede the agency's or official's activities and specifies the time period for the suspension. If the statement regarding suspension is provided to the HCC orally by the oversight agency or law enforcement official, the HCC shall document the statement made, including the name of the individual making the statement, and temporarily suspend the patient's right to the accounting. This suspension can be no longer than 30 days unless the HCC receives a written request for suspension.

   c. Procedure: An Individual's request for an accounting must state a time period that may not be longer than six years prior to the date of the request. In response to the request, the HCC will provide the requester with a written accounting unless the requester and the HCC agree upon a different media (e.g., electronic). The HCC must provide the first accounting to a requester in any 12-month period

without charge. For additional requests, the HCC may charge the requester for the costs of providing the accounting. The HCC will notify the requester of the cost involved and the requester may choose to withdraw or modify his/her request at that time before any costs are incurred.

d. Documentation: All disclosures required to be included in an accounting of disclosures pursuant to this Section shall be documented in the patient's Record. Such documentation must include, at a minimum, the following:

(1) The date of the disclosure;

(2) The name of the entity or person who received the PHI and, if known, the address of such entity or person;

(3) A brief description of the PHI disclosed; and

(4) A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for disclosure.

e. Documentation of disclosures and documentation of accountings of disclosures shall be maintained for a period of no less than six years from the date of disclosure or provision of the accounting.

f. Timing of Response. The HCC will act on each request for an accounting within 60 days after receiving the request. If the HCC cannot provide the accounting within that timeframe, it may extend the timeframe by no more than 30 days. In order to make an extension, the HCC must provide a written statement to the Individual within the original 60-day time period that explains the reasons for the delay and establishes the new deadline for the accounting.

4. Right to Request Restrictions: Individuals have the right to request that the HCC-PR restrict uses or disclosures of their PHI for Treatment, Payment, or Health Care Operations and disclosures to a family member, relative or friend who is involved with the health care or Payment of the patient's health care. With a limited exception (described below), the HCC-PR is not required to comply with an Individual's request.

a. The request must tell the HCC-PR:

(1) What information to limit;

(2) Whether to limit use, disclosure, or both; and,

(3) To whom the Individual wants the limits to apply (for example, disclosures to the Individual's spouse).

b. Procedure Relating to Requests for Restrictions: Upon receipt of an Individual's request for restrictions on the use or disclosure of his or her PHI, the HCC-PR will determine whether the requested restriction should be granted. If the HCC agrees to the requested restriction, the HCC-PR will document the restriction in the patient's Records and abide by the restriction until it is terminated.

c. Requests for Restrictions on Certain Disclosures to Individual's Health Plan. The HCC-PR must agree to restrict disclosure of a patient's PHI to the patient's Health Plan if:

(1) The disclosure is for the purpose of carrying out Payment or Health Care Operations and is not otherwise required by law; and,

(2) The patient's PHI pertains solely to a health care item or service for which the patient, or person other than the patient's Health Plan on behalf of the patient, has paid the HCC-PR in full.

d. Termination of Restrictions:

(1) The HCC-PR may terminate its agreement with a patient to restrict disclosure of that patient's PHI if the information is needed to provide emergency care or Treatment or if the Individual agrees or requests the termination in writing or orally if it is documented.

(2) In other circumstances, the HCC-PR may terminate a restriction after notifying the patient of the termination. Should the HCC-PR decide to terminate a restriction agreement with a patient without the patient's agreement, the HCC-PR must maintain the confidentiality of the information covered by the restriction agreement that was collected prior to the HCC-PR's notification to the patient of the termination. The HCC-PR is not bound by the agreement to restrict use or disclosure of PHI collected after the notification to terminate is provided to the patient.

(3) In general, the HCC-PR can terminate a restriction agreement except in the circumstance where an agreed-upon restriction pertains to disclosures of certain information to a patient's Health Plan as described in subsection (c) above.

5. Right to Request Confidential Communications: An Individual has the right to request that the HCC communicate with the Individual about medical matters in a certain way or at a certain location. For example, the Individual can ask that the HCC only contact him/her at work or by mail. The HCC will not ask an Individual the reason for his/her request. The HCC will accommodate all reasonable requests. The Individual's request must specify how or where (s)he wishes to be contacted.

6. Right to Receive a Paper Copy of the Notice of Privacy Practices: Each HCC that is required to have a Notice of Privacy Practices shall make it available on its website. An Individual also has the right to receive a paper copy of the HCC's Notice of Privacy Practices.

7. Right to Complain. Individuals may file a complaint with the Privacy Official and/or the Department of Health and Human Services Office for Civil Rights (OCR) regarding a violation of this Directive or the HIPAA Privacy, Security or Breach Notification rules. Complaints must be filed with OCR within 180 days of the alleged violation.

M. Business Associates:

1. Before a UI unit undertakes any Business Associate functions, activities or services (singly or collectively, "services") either for a UI HCC or for an outside covered entity, the unit must contact the Privacy Official and be designated an HCC (unless it has already been so designated).

2. The Workforce members who will be involved in performing the Business Associate services must complete HIPAA training, and the unit is responsible for satisfying all other relevant HIPAA compliance requirements set forth in this Directive before performing the Business Associate services.

3. Whenever an HCC performs or receives Business Associate services for or from an outside covered entity, UI and the outside entity must enter into a services contract describing the transaction and a companion BAA.
    a. UI's template BAA should be used whenever possible, and in particular when an HCC is engaging the services of a contractor to serve as a Business Associate.
    b. All BAAs must be reviewed by the relevant OBFS contracting office and signed by the authorized contract signatories.
    c. BAAs should have an appropriate expiration date.
    d. The University Contracts Records Office OBFS will maintain each BAA in a central repository for at least six years from the date the agreement expires or is terminated. UI record retention policies may prescribe a longer retention period.
    e. Procurement of vendor services must comply with state procurement laws and University policies.
4. Each HCC either performing or using Business Associate services is responsible for confirming at least annually that its active BAAs are necessary and proper, and for reporting completion of the annual review to the Privacy Official. Any concerns or changes should also be raised promptly to the attention of the OBFS contracting office that originally processed the agreement.
5. Each HCC-BA must train its employees on the use of any relevant software, systems or procedures for safeguarding, receiving and transmitting PHI to the external covered entity and shall comply with the terms of the BAA.
6. All requests, uses or disclosures of PHI in connection with the provision of Business Associate services must be limited to the minimum necessary to accomplish the services.
7. Any Workforce member who becomes aware of a possible or actual Breach or violation of a BAA must report the information as required by Section III.C, to the Privacy Official.

N. Complaints. The Privacy Official will publish a process for reporting privacy and security complaints. Individuals may make complaints anonymously. There will be no

retaliation against any person who makes a privacy or security complaint. HCCs shall immediately forward to the Privacy Official any privacy or security complaint received. After receiving a complaint, the Privacy Official will:

1. Investigate the Validity of the Complaint: Investigate the complaint and with the assistance of the Office of University Counsel if needed, determine if there is any validity to the complaint and assess its seriousness.

2. Take the Following Steps after Completing the Investigation:

    a. If the Privacy Official determines the complaint is not valid (meaning neither this Directive nor HIPAA has been violated), the Privacy Official will respond to the person who submitted the complaint.

    b. If the Privacy Official determines that the complaint is valid, the Privacy Official will:

        (1) If the complaint is that the HCC Notice of Privacy Practices does not comply with the HIPAA Privacy Rule, and the complaint does not allege any improper use or disclosure of PHI, then the Privacy Official will make sure that the Notice of Privacy Practices is amended appropriately.

        (2) If the complaint is that the HCC used or disclosed PHI in a way that violates this Directive or any related procedures, then the Privacy Official will:

            (a) Determine whether the violation constitutes a Breach of Unsecured PHI requiring notification to affected Individual(s), as set forth in Section III(C);

            (b) Determine whether there is any harm that should be mitigated;

            (c) Forward a written investigation report to the UA or campus official exercising disciplinary authority over the Workforce member responsible for the violation;

            (d) Consider, in light of the nature of the improper use or disclosure of PHI, if additional training should occur for one or more Workforce members; and

            (e) Consider, in light of the nature of the improper use or disclosure or PHI, whether this Directive or any related procedures need to be amended.

3. Documentation. All complaints and any response letters will be documented in the complaint log and retained for six years by the Privacy Official. Content of the documentation will include the nature of the complaint, the date, time and name of person making the complaint, and the resolution of the complaint.

4. Complaints Involving HCC's Business Associate:

    a. Any complaint alleging improper use or disclosure of PHI by the HCC's Business Associate shall be communicated to the Privacy Official. The Privacy Official shall investigate the allegation with the cooperation of other HCCs as necessary, and shall determine whether PHI was impermissibly used or disclosed by the Business Associate. As part of the determination, the Privacy Official will:

(1) Determine if the improper use or disclosure was serious;

(2) Determine if the improper use or disclosure was repeated.

b. The Privacy Official has authority to determine whether the University should or must terminate a BAA. A BAA must be terminated when a material violation of the agreement by the Business Associate cannot be cured or a violation cannot be ended.

c. If the HCC receives any complaint alleging a Breach of Unsecured PHI by a Business Associate, the HCC will comply with Section III.

II. SECURITY

A. Security Official.

1. UI has a Security Official, appointed by the President, whose responsibility is to oversee the Hybrid Entity's compliance with the HIPAA Security Rule. The Security Official's responsibilities include, but are not limited to, the following:

   a. Developing and implementing the policies and procedures of the Hybrid Entity, as required by the HIPAA Security Rule;

   b. Monitoring HCC compliance with the Security Rule;

   c. Assisting the Privacy Official in regularly reviewing the activities of UI units to ensure HCCs are properly identified and documented in writing;

   d. Serving as a compliance resource to the HCCs;

   e. In cooperation with the Privacy Official, developing and maintaining HIPAA training and maintaining related records;

   f. Establishing and maintaining administrative, physical and technical security safeguards to prevent, detect, contain and correct security violations involving PHI in electronic form; and

   g. Receiving, investigating, recommending resolution and responding to alleged breaches of the Security Rule.

2. The Security Official may assign other persons (including but not limited to the HIPAA Liaisons) to assist with any of the above responsibilities.

B. Security Risk Management.

1. A Risk Management process will be used to prioritize, educate and implement appropriate risk-reducing security controls recommended from the Risk Assessment process to ensure the Confidentiality, Integrity and Availability of ePHI.

2. Each HCC will implement a Risk Management program sufficient to reduce information system risks and Vulnerabilities to a reasonable and appropriate level. The Risk Management Program will ensure the Confidentiality, Integrity, and Availability of its ePHI; protect against reasonably anticipated Threats or hazards; and prevent any reasonably expected prohibited disclosures of information.

3. All Workforce members must fully cooperate with all persons executing Risk Management responsibilities.

4. Each HCC accessing or storing ePHI will conduct an annual security Risk Assessment of the potential risks and Vulnerabilities that may compromise the Confidentiality, Integrity, and Availability of that data. The Risk Assessment will:

    a. Include an inventory of all systems and determine which systems are used to collect, store, process, or transmit ePHI.

    b. Address the open items and mitigation efforts noted in previous assessments or audits.

    c. Identify events that can potentially impact system security or operations.

    d. Identify system Vulnerabilities and Threats to physical and technical safeguards.

    e. Identify systems where additional data Integrity solutions are required.

    f. Assess the impact a security compromise or prolonged disruption in service will cause.

    g. Be reported annually to the Security Official.

5. In addition to an annual assessment, each HCC will conduct thorough, timely Risk Assessments related to any material changes to the environment, any newly discovered potential Vulnerabilities, and any Threats to the Confidentiality, Integrity and Availability of its ePHI, and develop strategies to efficiently and effectively reduce risks identified in the assessment process.

C. Access Control

1. The HCC must ensure that unique user identification and authentication is required for all Workforce members, and is established as noted below:

    a. Each Workforce member must be provided with a unique user identification to utilize when accessing workstations, servers, portable computing devices (including laptops, tablets, and smartphones), and UI information assets. A centrally administered UI identity management system should be used to manage this identity information wherever possible.

    b. Workforce members are prohibited from sharing usernames and passwords, and usernames and passwords should not be written down or recorded in unencrypted electronic files or documents.

    c. Each Workforce member's user identification must have a strong password.

    d. Unless an exception is approved by the Security Official, Workforce members will use multi-factor authentication to access or modify ePHI or for privileged access to any system hosting ePHI.

2. The HCC must develop and document procedures to determine the access needs of all Workforce members in their unit. The HCCs must maintain an inventory of all applications, systems, and data repositories housing ePHI to determine who requires access and whether any ePHI is available to unauthorized individuals.

3. A Workforce member's access to ePHI requires the following controls:

    a. All access determinations and privilege assignments, and any changes to access and privilege assignments (e.g., additions or deletions) must be approved by the individual's supervisor or other appropriate HCC official authorized to make such determinations.

    b. HCCs must create and implement procedures to ensure that access to ePHI is limited only to authorized Users.

    c. HCCs must create and implement procedures to ensure that access to ePHI is the minimum access necessary for authorized users to perform duties.

    d. When access to ePHI is granted, the HCC that grants the access must retain documentation for six years supporting the approval and granting of user access to the ePHI.

    e. Unless an exception is approved by the Security Official, the HCC must perform an annual review of the roles and individuals who have been granted access to ePHI, including any time a person's role changes, and update access privileges as necessary.

    f. Access privileges must be updated immediately when any of the following occur:

        (1) An individual's job duties change such that his/her current access privileges are no longer appropriate;

        (2) When the individual is no longer under the administrative control of the HCC granting the access privileges; or,

        (3) When the individual is no longer employed by UI.

    g. Each HCC must develop and implement a procedure for terminating access to ePHI, including but not limited to:

        (1) Deactivation of computer access accounts;

        (2) Recovery of UI computers, devices, and data; and,

        (3) Recovery of access control articles such as identification badges, keys, access cards, etc.

4. Each HCC must develop and document procedures to obtain access to necessary ePHI during an emergency situation.

D. Security Auditing

1. HCC's have the responsibility for auditing information system access and activity for

those systems that store ePHI.

2. The HCC will implement system-level logging mechanisms for all systems that contain ePHI. The recorded log events must be stored on a separate event or log management system.

3. Where the system has the capability, for each user obtaining access to ePHI, each system's audit log will include at least the user ID, user IP address, login date and time, and logout date and time.

4. The HCC will retain log records until it is determined they are no longer needed, in accordance with this Directive and/or Illinois record retention requirements.

5. On a continual basis, the HCC will review and analyze log records for indications of inappropriate and anomalous activity and report findings of concern to the Security Official.

6. Audit logging infrastructure will be monitored and appropriate staff will be alerted in the event of an audit infrastructure failure.

7. IT systems and log monitoring management platforms will protect audit information from unauthorized access, modification, and deletion.

E. Data Security

1. Safeguarding PHI Available Electronically (Data in Transit):

a. All transmissions of ePHI over Non-Secure Networks or any other non-secure communications channel, must be secured in a fashion that protects the Integrity and Confidentiality of the data. Specifically:

(1) The identities of the sender and the recipient must be authenticated. If the transmission is uni-directional from the sender to the recipient, then the identity of the recipient must be authenticated.

(2) The recipient must agree to participate in the data transmission.

(3) The data transmission must be encrypted. Either the data transmission channel must be encrypted, or the data must be encrypted prior to transmission according to the requirements set forth by the Security Official.

(4) The sender and receiver must be aware of the risks involved respectively in sending and receiving ePHI.

b. All ePHI transmissions over Non-Secure Networks must be digitally signed to ensure that modification without detection does not occur.

c. Data encryption transmission security settings must meet or exceed the minimum standard as specified by the Security Official.

d. Assuming all Privacy and Security prerequisites in this section (II.E.1) for transmitting ePHI by email are met and the HCC otherwise allows transmission of ePHI by email, then any HCC Workforce member sending email containing

ePHI must include a standard ePHI warning banner approved by the Privacy and Security Official in the email.

e. Questions regarding encryption or transmission of ePHI over non-secure networks should be directed to the Security Official.

2. Data at Rest

a. Each HCC must encrypt all HCC laptops and any HCC portable data storage devices used to access, process or store ePHI or has the potential to access, process or store ePHI, including but not limited to, flash drives, handheld devices, removable media, and backup media. Data encryption storage specifications must meet or exceed the minimum standard specified by the Security Official.

b. In any instance under which encryption of a device is not possible, with the approval of the Security Official, a procedure must be implemented to track the individual storage devices and/or media containing the ePHI, their location, and the parties in physical possession of and responsible for the devices and/or media.

c. Encryption of ePHI on non-portable devices as an access control mechanism is not required unless the custodian of the ePHI has, by means of the physical security and Risk Assessment, deemed it a necessary control.

d. Each HCC must document and implement procedures for the secure removal of ePHI from storage media before making the storage media available for reuse within the HCC or relinquishing control or possession of the storage media to a person or entity outside the HCC.

(1) If all ePHI on the storage media cannot be rendered unrecoverable, the storage media must be destroyed.

(2) The HCC must follow UI or campus guidelines, as appropriate, on the sale, donation, or transfer of computer hard drives and other magnetic media. All data destruction must be in accordance with Illinois law and UI data retention policies.

(3) For storage devices not specifically identified in the Data Security on State Computers Act or in UI policy, ePHI must be rendered unrecoverable before disposal.

(4) If a process to remove ePHI cannot be implemented, then the Security Official should be consulted for instructions.

e. Transmission of ePHI to External Entities. The transmission of ePHI from an HCC or Workforce member to an External Entity via a messaging or data transfer system is permitted if the sender has ensured that ePHI transmission security conditions are met.

(1) Workforce members must use a UI-administered secure data transfer system to transmit ePHI to External Entities; however, if the External Entity requires use of its own data transfer system, the Workforce member must be able to verify the system meets or exceeds the minimum standard specified by the Security Official prior to using the External Entity's system.

(2) All contracts and data sharing agreements required by law and this Directive

have been executed in accordance with UI policy.

F. System Security

1. To protect the Confidentiality, Integrity and Access to data, all systems must have appropriate security software installed and enabled that protects the computer from malicious software.

2. To prevent unauthorized access, all computers accessing ePHI must be configured to automatically lock the device or disconnect the user session after a period of inactivity as specified by the Security Official.

3. Access controls should be implemented for workstation or server network services:

   a. All unnecessary network services should be disabled.

   b. Access control lists should be configured and implemented for each active network service, defining the allowed or denied protocol, port and network connections as narrowly as possible.

   c. For systems containing ePHI, the method with which any access control list is implemented should be documented. Examples include a host operating system packet filtering firewall (e.g. Microsoft Windows operating systems firewalls, or Linux iptables). When implemented, the current access control list must also be documented.

4. HCCs must implement intrusion detection capabilities in any information system it administers to facilitate regular appraisal of the effectiveness of network perimeter and host network access controls and the forensic investigation of potential or actual intrusion activity.

   a. Intrusion detection must be implemented for all workstations and servers containing ePHI.

   b. Detected intrusion activity must be logged, and intrusion logs must be reviewed regularly.

5. All systems allowing remote login (or remote desktop) access must be configured to meet standards established by the Security Official. Remote login/desktop access to workstations should be disabled unless there is a business need.

6. All devices used to access, process or store ePHI must be configured to standards established by the Security Official.

7. Each HCC must develop an audit control and review plan to record and examine activity in the information systems it administers, which then allows assessment of how well the HCC is complying with this Directive on a per-system basis. The audit control and review plan must include:

   a. A list of the systems and applications to be logged;

   b. The information to be logged for each system or application;

c. The specifications for log reports for each system or application; and

d. The procedures to review all audit logs and activity reports.

8. Workforce members shall not use their personal computers or any other devices not administered and secured by HCC staff to manipulate or store ePHI.

G. Physical Safeguards:

1. HCCs must:

a. Classify each workstations, server, portable computing device (including laptops, tablets, and smartphones), and UI information asset into types based on the location, mobility, capabilities, connections, and allowable activities for each.

b. Develop Unit level policies and/or procedures for the allowed usage of each type of workstation, server, portable computing device (including laptops, tablets, and smartphones), and UI information asset, identifying and accommodating their unique issues while securing them and permitting their correct utilization.

2. HCCs will at least annually analyze and rank the existing physical security Vulnerabilities of any location where their devices containing ePHI are located and will develop a Facility Security Plan to protect such equipment from unauthorized physical access that could lead to theft, tampering, or unauthorized viewing, altering or erasing of data.

a. As part of the Facility Security Plan, HCCs will analyze the physical surroundings of each device identified in the inventory of ePHI systems to:

(1) Determine which types of Facility locations require physical access controls to safeguard data.

(2) Determine whether changes in physical access controls or equipment location are required in order to reduce risk associated with the physical location to a level acceptable by the HCC.

(a) The HCC will document repairs and modifications to the physical components of a Facility that are related to physical security and maintain records for no less than six years.

(b) Based upon the outcomes of this assessment, the HCC may implement procedures to control and validate an individual's access to Facilities based on his/her role or function, including visitor control procedures.

3. HCCs shall have appropriate controls in place to prevent unauthorized access to facilities and equipment that contain ePHI. Possible measures include, but are not limited to, locked doors, alarms, signs warning of restricted areas, surveillance cameras, identification badges, visitor badges and escorts.

4. A Facility with servers containing ePHI must have appropriate automated logging mechanisms for physical access to the Facility.

5. All HCCs that handle ePHI must:

    a. Create and maintain a list of software programs used by the HCC to access or manipulate ePHI or, in the case of HCC's performing BA functions, software installed by the HCC-BA at the request of an outside Covered Entity.

    b. Create and implement procedures to control access to these software programs for their use, testing, and revision.

H. Network Security

1. An HCC's network includes any network administered by the HCC, as well as any network to which the HCC's workstations, data storage devices, or servers have direct access to or the capability to directly access.

2. Access points to other networks from that HCC network define the perimeter of the HCC network.

    a. Units will, in accordance with their Risk Management Plan, implement network perimeter security and corresponding network access controls, such as the use of network firewalls, routers, or Virtual Local Area Networks (VLANs).

    b. The configuration of the firewalls, routers, VLANs, or other network access controls used to protect the HCC network environment must be documented and available to the HCC and the Security Official.

I. Contingency Operations/Disaster Planning

1. Each HCC will establish and implement a data backup plan that will detail all backups to be performed, media used for the backups, security considerations, location used to store the backups, and procedure for recovery of the backup data.

2. The data backup plan will be documented and available to the Security Official.

3. All individuals with specific responsibilities in the data backup plan must be trained in those responsibilities.

4. Data backup plans must detail plans to create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

5. The HCC will maintain a Disaster Recovery Plan (DRP) with procedures to recover the systems and data.

6. The HCC will periodically assess if the DRP meets its business continuity plan requirements.

7. Where the HCC will use the services of a third party Business Associate to manage information technology or data for the HCC or the HCC's primary technology support unit, the HCC will be responsible for ensuring the Business Associate can meet or exceed its required DRP components.

8. The HCC will document procedures necessary to comply with its BAAs. An HCC-BA must also comply with the terms of the BAA, which may affect backup and recovery requirements.

9. The current DRP will be accessible off-site by key HCC Workforce members in the event of a disaster.

10. All individuals with specific responsibilities in the DRP must be trained in those responsibilities.

11. HCCs that handle ePHI must coordinate with the Security Official, Public Safety, Facilities & Services and other appropriate campus units to develop procedures to allow Facility access in support of the restoration of lost data in the event of a disaster or an emergency. Contingency operations for access to data will depend on the type of emergency and the ability to re-enter the Facility.

12. Each HCC will establish a process to test its data backup plan, DRP, and as appropriate, emergency mode operations plan. HCC Workforce members must be trained in their specific roles and responsibilities prior to testing.

13. Each plan will be tested periodically and results/findings will be documented and shared with the Security Official.

14. Each HCC will assess the relative criticality of its specific applications and data in support of other contingency plan components. This list must be used when creating the HCC's DRP, data backup plan and emergency mode operations plan to ensure that the most critical applications are backed up and restored in the appropriate order.

15. HCCs that handle ePHI that is critical to patient care must:

    a. Establish procedures (the "Emergency Mode Operations Plan" or "EMO") to enable the continuation of UI business processes and protect the security of ePHI while operating in emergency mode.

    b. Train all individuals with specific responsibilities in the EMO Plan.

    c. Document the EMO Plan and make it available to key HCC Workforce members.

J. Incident Response

1. Where Workforce members have a reasonable belief that an activity may present a Threat to, or has affected the, Confidentiality, Integrity, or Availability of ePHI, they must immediately report the situation to the HIPAA Security Official.

III. BREACH NOTIFICATION

A. Purpose: This Directive relating to Breaches of Unsecured PHI is intended to establish a process for responding to such Breaches in accordance with the requirements of the HIPAA Breach Notification Rule.

B. Presumed Breach: An acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA is presumed to be a Breach unless the acquisition, access, use, or disclosure is specifically excluded from the definition of a Breach, or a Risk Assessment determines that there is a low probability that the PHI has been compromised. The Risk Assessment must include, at a minimum, an assessment of the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or used; and,
4. The extent to which the risk to the PHI has been mitigated.

C. Response

1. Notification of Potential Breaches. Upon discovering a potential Breach, an HCC Workforce member shall immediately report the potential Breach to the HCC, which shall immediately notify the Privacy Official.
    a. If the HCC Workforce member has concerns about reporting the potential Breach to the HCC, the Workforce member may report the potential Breach directly to the Privacy Official.
    b. The HCC Workforce member may also report the potential Breach to the Ethics Line at 866-758-2146 or ethicsofficer@uillinois.edu.
2. The HCC shall also take immediate action to terminate the potential Breach if it is still ongoing.
3. The Privacy Official shall apprise appropriate UI officials of the potential Breach and keep them informed regarding any significant developments or issues encountered.
4. Where an HCC is performing Business Associate services for an outside Covered Entity, the Privacy Official and HCC shall comply with the terms of the BAA with respect to the required Breach response.
5. Where an external Business Associate of an HCC has reported a potential Breach to the Privacy Official, the Privacy Official shall be responsible for enforcing the terms of UI's BAA as to the Business Associate as well as carrying out the procedures in this Directive.
6. Analysis of Potential Breaches. Upon receiving a report of a potential Breach, the Privacy Official will gather additional information as necessary. All Workforce members and external Business Associates shall cooperate with the Privacy Official in collecting and assessing relevant information. The Privacy Official will evaluate the information in accordance with this Directive and determine whether a Breach occurred and whether the PHI involved was Unsecured PHI.

7. If the Privacy Official determines that a Breach of Unsecured PHI occurred, Individuals, the media and HHS will be notified as required by the Breach Notification Rule. The Privacy Official also must consider the notification requirements of other pertinent security breach laws and make sure that notifications meet the required elements and standards. The Privacy Official also will forward the written investigative report to the UA or campus official exercising disciplinary authority over the Workforce member(s) responsible for the Breach.

   a. Notification to Individuals

      (1) The Privacy Official must notify each Individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used or disclosed as a result of the Breach. Notification must be made without unreasonable delay and in no case more than 60 calendar days after discovery of a Breach unless required earlier by a BAA. A Breach is considered to have been discovered as of the first day on which the Breach was known to an HCC Workforce member or agent (other than the person who committed the Breach) or, by exercising reasonable diligence, would have been known by the HCC.

         (a) Preparation of the Breach notice. The Privacy Official will work with the HCC Workforce members and others who have knowledge of the circumstances of the Breach to prepare a Breach notice. If a Business Associate of the HCC is responsible for a Breach and the Privacy Official determines that Individuals need to be notified, the Privacy Official will work with the applicable Business Associate to prepare a Breach notice. The Breach notice must be written in plain, easy to understand, language.

         (b) Contents of Notice: In either case, the Breach notice will include the following information:

            i. A brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;

            ii. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

            iii. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

            iv. A brief description of what the HCC is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and

            v. Contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone number, e-mail address, website, or postal address.

         (c) Method of Notification. When Individuals are required to be notified pursuant to this Directive, notifications will be made as follows:

i. Written notice by first-class mail will be provided to the Individual at his/her last known address or, if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

ii. If the HCC knows that an Individual is deceased and has the address of the next of kin or Personal Representative of the Individual, written notification by first-class mail will be provided to either the next of kin or Personal Representative.

iii. If contact information for an Individual is insufficient or out-of-date such that written notification as described above is not possible, the Privacy Official will provide notice using a substitute form reasonably calculated to reach the Individual, as indicated below. No substitute notice is necessary when there is insufficient or out-of-date contact information for next of kin or a Personal Representative.

iv. If there is insufficient or out-of-date contact information for fewer than 10 Individuals, substitute notice will be provided in an alternate form of written notice, telephone, or other means.

v. If there is insufficient or outdated contact information for 10 or more Individuals, substitute notice will be provided in the form of either a conspicuous posting for a period of 90 days on the home page of the HCC website or conspicuous notice in major print or broadcast media in the geographic areas where the Individuals affected by the Breach likely reside. The notice will include a toll-free number that will remain active for at least 90 days where an Individual can learn whether the Individual's Unsecured PHI may be included in the Breach.

vi. (F) In situations deemed by the Privacy Official to require urgency due to the possible imminent misuse of Unsecured PHI, the Privacy Official may provide information to Individuals by telephone or other means, as appropriate, in addition to the methods described above.

b. Notification to Media. If the Breach involves more than 500 residents of a state or jurisdiction, the Privacy Official must notify prominent media outlets serving the state or jurisdiction no later than 60 calendar days after discovery of the Breach, except in the case of permitted law enforcement delay.

c. Notification to HHS.

(1) If a Breach of Unsecured PHI involves 500 or more Individuals, the Privacy Official must notify the Secretary of HHS at the same time as affected Individuals are notified, in the manner specified on the HHS website at http://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf. If the Breach involves fewer than 500 Individuals, the Privacy Official will maintain a log or other documentation of such Breaches and, no later than 60 days after the end of each calendar year, provide notification in the manner specified on the HHS website.

d. The HCC will mitigate, to the extent practicable, any harmful effect known to be the result of the use or disclosure of PHI in violation of HIPAA.

e. Subject to UI policies, practices and procedures, the HCC responsible for the Breach event is also responsible for the costs required to investigate and respond to the event.

f. Delay Required by Law Enforcement. The Privacy Official will delay making the required notifications if a law enforcement official states that such notification would impede a criminal investigation or cause damage to national security. The Privacy Official will delay the notification as specified in a written statement from law enforcement or, if no written statement is provided, for not more than 30 days from the date that the Privacy Official received oral notification from law enforcement (which the Privacy Official must document in writing).

g. Memoranda of Understanding (MOU). The Privacy Official may enter into MOUs with HCCs to address any or all of the requirements in this section.

h. Inquiries Regarding Breach Directive. Any questions or concerns regarding this Directive relating to HIPAA Breach response and notification should be directed to the Privacy Official.

IV. TRAINING

A. Scope and Responsibility. All HCC Workforce members shall be trained to understand and implement this Directive and related procedures prior to their having access to PHI. Each HCC is responsible for ensuring its Workforce is trained.

B. Security Reminders. The Security Official shall provide Workforce members with periodic security reminders to keep them aware of current Threats and best practices.

C. Timing of Training. Training shall be provided as follows:

1. Before a Workforce member is granted access to PHI and within 30 days of being identified as a member of an HCC's Workforce;
2. Within a reasonable time after material changes to this Directive or any related procedures; and,
3. Annually and whenever, in the determination of the Privacy Official, additional training is necessary to maintain compliance with the HIPAA Privacy, Security and Breach Notification rules.

D. Documentation. The Privacy Official will maintain records of who has been trained, what training occurred, and the date of training for six years following the date of the training.

V. SANCTIONS FOR BREACH

A. Initial Actions

1. HCCs shall report all privacy and security incidents to the Privacy Official. The Privacy Official shall document all reported privacy and security incidents in a log and ensure an appropriate investigation is conducted as required by Section III.C.

2. In coordination with the relevant HCC and Human Resources office, the Privacy Official or Security Official may suspend access to systems or arrange for other interim measures to protect PHI from loss or disclosure pending completion of the investigation and implementation of any final corrective action.

3. When the Privacy Official determines, following investigation, that a Breach of Unsecured PHI has occurred, the log entry for the incident shall reflect that the incident was substantiated. If the Privacy Official determines that a case is not a Breach, then the log entry for the incident shall reflect that there was no Breach.

4. The Privacy Official will keep all pertinent documentation on file for no less than six years.

B. Initiation of Disciplinary Action

1. If the Privacy Official determines, following investigation, that a Breach of Unsecured PHI has occurred, a written investigative report will be forwarded to the UA or campus official exercising disciplinary authority over the Workforce member. For faculty, the investigation report and recommendations will be forwarded to the campus Provost.

   a. The Privacy Official shall include with the investigation report his/her recommendations for appropriate sanctions for the individuals responsible for the Breach.

      (1) Recommended sanctions must be commensurate with the severity, frequency, and intent of violations.

      (2) Progressive sanctions, ranging from verbal and written warnings up to termination, should be considered, as appropriate.

   b. The Privacy Official may consult with the Office of University Counsel, Human Resources, campus student disciplinary authorities, or other UI officials, as appropriate, in formulating his/her recommendations.

2. After receiving the written investigation report and Privacy Official recommendations, the UA or campus official exercising disciplinary authority over the Workforce member shall initiate disciplinary proceedings against the Workforce member following established employee or student disciplinary procedures, as appropriate.

3. Subject to applicable privacy laws and regulations, the UA or campus official exercising disciplinary authority over the Workforce member will notify the Privacy Official of the results of the disciplinary proceedings, which shall be placed in the employee or student's official records as required by the applicable disciplinary process. If the disciplinary proceedings are not completed within 30 days of the date the investigation report was received, the UA or campus official shall provide the Privacy Official with monthly status updates until the matter is resolved.

4. The Privacy Official shall maintain a confidential file documenting the investigation, his/her recommendations, all supporting documentation, and the result of the disciplinary proceedings subject to applicable privacy laws and regulations. The file will be maintained for no less than six years and as otherwise required by records retention requirements. This requirement is in addition to any record retention requirement of the applicable disciplinary process.

C. No Retaliation

1. Workforce members shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any person who:

    a. Exercises his or her rights or participates in the HIPAA complaint process;

    b. Files a complaint with the Secretary of Health and Human Services;

    c. Testifies, assists, or participates in an investigation, compliance review, proceeding or hearing; or

    d. Opposes any act or practice unlawful under HIPAA.

2. Any person may allege retaliation using any UA, campus or external agency complaint resolution/disciplinary process.

Appendix A - Glossary

Administrative Safeguards	The administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the Health Care Component's Workforce members in relation to the protection of that information. 45 CFR §164.304
Availability	Data or information is accessible and usable upon demand by an authorized person. 45 CFR § 164.304
Breach	The unauthorized acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the Protected Health Information. A Breach may occur with respect to Protected Health Information in any form, and not only in electronic form. "Breach" does not include: (a) Any unintentional acquisition, access, or use of Protected Health Information by a member of the Health Care Component Workforce or by a person acting under authority of the Health Care Component or the Health Care Component's Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule. (b) Any inadvertent disclosure by a person who is authorized to access Protected Health Information at the Health Care Component or Health Care Component's Business Associate to another person authorized to access Protected Health Information at the Health Care Component or the Health Care Component's Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule. (c) A disclosure of Protected Health Information where the Health Care Component or the Health Care Component's Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
Business Associate	A person not a member of any Health Care Component's Workforce or entity that (i) on behalf of a Health Care Component, creates, receives, maintains or transmits Protected Health Information for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management, and repricing; or (ii) provides, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial

	services to or for a Health Care Component where the provision of the service involves the disclosure of Protected Health Information from such Health Care Component, or from another Business Associate of such Health Care Component to the person. 45 CFR §160.103
Business Associate Agreement	A contract between a Covered Entity (or Hybrid Entity) and its Business Associate governing the uses and disclosures of PHI. In most cases, the Covered Entity and Business Associate will enter into a companion services contract describing the covered functions or activities being performed by the Business Associate, the compensation and other terms of the transaction.
Clergy	Ordained or equivalent religious representatives of the community's faith groups who are not members of an HCC Workforce.
Confidentiality	The property that data or information is not made available or disclosed to unauthorized persons or processes. 45 CFR §164.304
Covered Entity	A Health Plan, Health Care Clearinghouse or Health Care Provider that transmits any Health Information in electronic form in connection with a transaction covered by HIPAA. 45 CFR § 160.103
Covered Functions	Those functions of a Covered Entity the performance of which makes the entity a Health Plan, Health Care Provider, or Health Care Clearinghouse. 45 CFR § 164.103
De-identified Information	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. The HIPAA Privacy Rule provides two methods for de-identifying PHI, the most common of which is removal of 18 enumerated direct and indirect identifiers. 45 CFR § 164.514(b)(2)(i).
Designated Record Set	A Health Care Provider's medical and billing Records; a Health Plan's enrollment, payment, claims adjudication and case or medical management Records systems; and any information used, in whole or in part, by or for the covered entity to make decisions about Individuals.
Disaster Recovery Plan	A plan to protect the people, information, technology, and facilities used to deliver health care. Action plans should be based on risks identified in a risk analysis and typically include administrative, physical, and technical safeguards; policies and procedures; and organizational standards,
Disclosure	The release, transfer, provision of access to, or divulging in any manner of Protected Health Information by an individual within the Health Care Component to a person or entity outside the Health Care Component.
Electronic Media	(1) Electronic storage media on which data are or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be

	transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission. 45 CFR § 160.103
Electronic Protected Health Information (ePHI)	The subset of Protected Health Information that is (i) transmitted by Electronic Media; or (ii) maintained in any medium constituting Electronic Media. 45 CFR § 160.103
Emergency Mode Operations Plan	Procedures established to enable the continuation of UI business processes and to ensure protection of the security of ePHI while operating in emergency mode.
External Entity	Any entity or unit outside the Hybrid Entity.
Facility	Physical premises and the interior and exterior of a building(s). 45 CFR § 164.304
Facility Directory	A publication (in any medium) that contains elements of an Individual's Protected Health Information, such as name, location in the Facility, the Individual's general condition, and religion.
Facility Security Plan	A plan that manages physical security for IT resources.
Health Care Clearinghouse	A public or private entity that a) processes or facilitates the processing of Health Information received from another entity in a non-standard format or containing non-standard data content into standard data elements or a standard transaction; or b) receives a standard transaction from another entity and processes or facilitates the processing of Health Information into non-standard format or non-standard data content for the receiving entity. 45 CFR § 160.103
Health Care Component	A component or combination of components of a Hybrid Entity designated by the Hybrid Entity as component(s) that meet the definition of Covered Entity or Business Associate if such component(s) were separate legal entities. 45 CFR § 164.103; 45 CFR § 164.105(a)(2)(iii)(D)
Health Care Operations	Business and administrative functions including conducting quality assessment and improvement activities; reviewing the competence or qualifications of health care professionals; conducting training programs; accreditation; credentialing; conducing or arranging for medical review, legal services, and auditing functions; business planning and development; and business management and general administrative activities. 45 CFR § 164.501. Health Care Operations do not include research and many marketing and fundraising activities.
Health Care Provider	A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. 45 CFR § 160.103
Health Information	Any information, including genetic 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. 45 CFR § 160.103
Health Plan	An individual or group plan that provides, or pays the cost of, medical care. 45 CFR § 160.103

HIPAA Liaison	An individual appointed by the head of the Health Care Component who serves in that role for a Health Care Component, with the following responsibilities with respect to that Health Care Component: Work with the Health Care Component head, as defined for the Health Care Component, to identify members of the Health Care Component's Workforce who engage in activities that involve use of Protected Health Information and assure they are trained; cooperate with the Privacy and Security Official(s) in the development of policies and procedures and other compliance activities; and serve as point of contact for questions, audits and problem resolution regarding the Health Care Component's compliance with HIPAA.
Hybrid Entity	A single legal entity: (1) that is a Covered Entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates its Health Care Components. 45 CFR § 164.103
Individual	The person who is the subject of Protected Health Information.
Individually Identifiable Health Information	Information that is a subset of Health Information, including demographic information collected from an Individual, and that 1. is created or received by a Health Care Provider, Health Plan, employer, 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; and 3. a. identifies the Individual, or b. with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. 45 CFR § 160.103
Integrity	The property that data or information has not been altered or destroyed in an unauthorized manner. 45 CFR § 164.304
Limited Data Set	Protected Health Information that excludes the 16 direct identifiers set forth at 45 CFR § 164.514(e)(2).
Marketing	Making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Marketing does not include a communication made: (b) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for a patient, only if any financial remuneration received by the Health Care Component in exchange for making the communication is reasonably related to the Health Care Component's cost of making the communication; or, (c) For the following Treatment and Health Care Operations purposes where the HCC does not receive any financial remuneration (including direct or indirect payment) in exchange for making the communication: i. For Treatment of a patient by the Health Care Component-Provider, including case management or care coordination for

	the patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the patient; ii. To describe a health-related product or service (or payment for such product or service) that is provided by the Health Care Component, including communications about the entities participating in a Health Care Provider network or Health Plan network, replacement of, or enhancements to, a Health Plan, and health-related products or services available only to a Health Plan enrollee that add value to, but are not part of, a plan of benefits; or iii. For case management or care coordination, contacting of patients with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of Treatment.
Non-Secure Network	Networks other than a UI campus network.
Payment	The activities undertaken by: a. A Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan; and b. A Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of health care. Such activities include, but are not limited to: a. Determinations of eligibility or coverage and the adjudication or subrogation of health benefit claims; b. Risk adjusting amounts due based on enrollee health status and demographic characteristics; c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing; d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and, f. Disclosure to consumer reporting agencies certain information relating to collection of premiums or reimbursement. 45 CFR § 164.501
Personal Representative	A person with authority to act on behalf of another individual, including a deceased individual, in making decisions related to health care and/or health care information. 45 CFR § 164.502(g)

Physical Safeguards	Physical measures, policies and procedures (e.g., locks and identification cards) to protect the Health Care Component's electronic information systems and related buildings and equipment, from natural and environmental hazards and from unauthorized intrusion. 45 CFR §164.304
Privacy Official	A person designated by the president of the University who is responsible for the development and implementation of the Hybrid Entity's HIPAA privacy policies and procedures. The Privacy Official may delegate responsibility for privacy functions unless otherwise indicated. The Privacy Official may also serve as the Security Official if so designated. 45 CFR § 164.530(a)(1)(i)
Protected Health Information (PHI)	A subset of Individually Identifiable Health Information that is (a) transmitted by Electronic Media; (b) maintained in any medium constituting Electronic Media; or (c) transmitted or maintained in any other form or medium. 45 CFR §160.103 (Note: Information pertaining to a patient who has been deceased for more than 50 years is no longer Protected Health Information.) Protected Health Information does not include Individually Identifiable Health Information in education records under FERPA or employment records held by a Covered Entity as an employer.
Public Health Activities	The activities of public health authorities that are legally authorized to receive Protected Health Information for the purpose of preventing or controlling disease, injury or disability. 45 CFR § 164.512(b)
Record	Any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for the Covered Entity.
Research	A systematic investigation including research development, testing and education, designed to develop or contribute to generalizable knowledge. 45 CFR § 164.501
Risk Assessment	The process that identifies the security risks to information system security and determines the probability of occurrence and the resulting impact for each Threat/Vulnerability identified given the security controls in place; prioritizes risks; and results in recommended possible actions/controls that could reduce or offset the determined risk.
Risk Management	A process that prioritizes, evaluates and implements security controls that will reduce or offset the risks determined in the Risk Assessment process to satisfactory levels, given the organization's mission and available resources.
Secure Network	UI campus network infrastructure.
Security Audits	Internal process of reviewing information system access and activity, done on a periodic basis, as a result of a potential breach, in response to a complaint or on suspicion of employee wrongdoing.
Security Incidents	The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. 45 CFR § 164.304
Security Official	The person designated by the president of the University who is responsible for the development and implementation of the Hybrid Entity's HIPAA security policies and procedures. The Security Official may delegate responsibility for security functions unless otherwise

	indicated. The Security Official may also serve as the Privacy Official if so designated. 45 CFR § 164.308(a)(2)
Subcontractor	A person or organization to whom a Health Care Component-Business Associate delegates a Business Associate function, activity, or service, other than in the capacity of a member of the Workforce of the Health Care Component. 45 CFR § 160.103
Technical Safeguards	The technology, policy, and procedures for the use of Electronic Protected Health Information that protect and control access to it. 45 CFR § 160.103
Threat	The potential for a particular threat source to cause loss or to successfully exploit a particular Vulnerability.
Treatment	The provision, coordination, or management of health care and related services by one or more Health Care Providers, including the coordination or management of health care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or the referral of a patient for health care from one Health Care Provider to another. 45 CFR § 164.501
Unit	A University of Illinois school, college, division, department or other unit.
Unsecured Protected Health Information	Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services. Protected Health Information is deemed "secured" only if it is encrypted or destroyed in accordance with the guidance referenced by Health and Human Services and published by the National Institute of Standards and Testing.
Use	The employment, application, examination or analysis of Individually Identifiable Health Information by an individual within the Health Care Component or the sharing of Protected Health Information with an individual within the Health Care Component.
Vulnerability	A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and leads to a compromise in the integrity of that system.
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an HCC is under the direct control of the HCC.

Appendix B - Acronyms

BAA	Business Associate Agreement
DRP	Disaster Recovery Plan
ePHI	Electronic Protected Health Information
HCC	Health Care Component
HCC-BA	Health Care Component – Business Associate
HCC-PL	Health Care Component – Health Care Plan
HCC-PR	Health Care Component – Health Care Provider
HIPAA	Health Insurance Portability & Accountability Act of 1996
IP	Internet Protocol
IRB	Institutional Review Board
IT	Information Technology
OCR	Office for Civil Rights in the U.S. Department of Health and Human Services
PHI	Protected Health Information
URL	Universal Resource Locator
VLAN	Virtual Local Area Network