FLORIDA ATLANTIC UNIVERSITY

DIVISION OF RESEARCH

SUBJECT: Disclosure and Use of Protected Health Information (PHI) in Research	**Policy Number:** 10.3.7	**Effective Date:** March 28, 2022
	Supersedes: October 31, 2018	**Pages:** 14
	Responsible Authorities: Vice President for Research Assistant Vice President, Research Integrity Institutional Review Board	

I. Background

The Health Insurance Portability and Accountability Act of 1996 (also known as HIPAA) went into effect in 2003. HIPAA is a federal law that establishes national standards for protecting the privacy and security of **protected health information (PHI)** and defines specific rights for individuals with respect to their PHI.

Updates to HIPAA, known as the Health Information Technology for Economic and Clinical Health Act (HITECH), went into effect in March 2013. The HITECH Act includes several measures designed to broaden the scope and increase the rigor of HIPAA compliance and strengthens the privacy and security protection of individual health information. HITECH specifically requires that patients be notified in the event of a breach of privacy or security and establishes penalties for non- compliance with HIPAA.

II. Purpose

The purpose of this policy is to outline the conditions under which FAU faculty, staff, students, residents, and post-doctoral fellows (collectively "FAU faculty, staff and students) as well as non-employees may obtain, create, use or disclose **PHI** for research purposes. PHI refers to individually identifiable health information (oral, written, or electronic) that is created or received by a "covered component" and that relates to an individual's physical or mental health, or the provision of health care to an individual or payment for their health care.

III. General Statement

Florida Atlantic University (FAU) is committed to protecting the privacy and security of PHI, while at the same time ensuring that researchers continue to have access to the medical information necessary to conduct research. Accordingly, research must be conducted in compliance with all applicable laws, regulations, and University policies.

As noted above, HIPAA applies specifically to certain "covered components" (as defined in appendix A). FAU is a "hybrid" covered entity which means only certain components of the university (Student Health Services, Charles E. Schmidt College of Medicine, Christine E. Lynn College of Nursing, and the College of Education Communication Disorders Clinic) meet the federal definition of a covered entity. It is the expectation that all FAU

faculty, staff and students have an awareness of HIPAA and how it may affect them as they work with PHI for research purposes.

IV. Definitions (See Appendix A)

Refer to FAU HIPAA glossary and terms at http://www.fau.edu/hipaa/

V. Policy

At FAU all research that is conducted using PHI from patients of a covered component must be conducted in accordance with HIPAA privacy and security regulations as well as relevant state laws and regulations, and FAU regulations, policies and procedures. If State of Florida laws provide greater privacy protections or rights with respect to a patient's PHI, then state laws supersede HIPAA.

As a general policy, faculty, staff and students of an FAU covered component must obtain authorization from all participants in a research study prior to the internal use or external disclosure of PHI unless he/she obtains a waiver of authorization. However, a member of a covered component at FAU is authorized to use or disclose, for research purposes, health information which has been appropriately de- identified as outlined in 45 CFR 164.502(d) and 164.514(a)-(c) of the HIPAA Privacy Rule.

Regarding PHI, FAU faculty, staff and students conducting research should strive to use the "minimum necessary" information whenever possible. For example, researchers should not request an Individual's entire medical record unless the entire medical record is justified as reasonably necessary to accomplish the research objectives.

All faculty, staff, or students who use PHI for research purposes must complete appropriate HIPAA training via the Collaborative Inter-Institutional Training Initiative (CITI) site. CITI's Information Privacy and Security (IPS) materials cover the principles of data protection, focusing on the healthcare-related privacy and information security requirements of the Health Insurance Portability and Accountability Act (HIPAA). Additional training related to Covered Component requirements may also be required by the institution and must be followed as applicable.

VI. Accountability

The Principal Investigator (PI) will be responsible for:

- Assessing when PHI is involved in his/her research study.
- Completing, and ensuring all study team members have completed, appropriate HIPAA training prior to working with PHI.
- Determining the minimum necessary PHI required for the research.
- In consultation with FAU's Office of Information Technology (OIT) and the relevant College information technology representative, evaluating data security provisions for safeguarding PHI as described in the IRB protocol to ensure security provisions are sufficient to protect the privacy and confidentiality of human subjects.
- Submitting to the IRB/Privacy Board the appropriate HIPAA permission forms as appropriate for the type of activity that will be performed.
- Obtaining IRB/Privacy Board approval prior to obtaining and using PHI for research purposes.
- Securing a data use agreement, as necessary.
- Correcting improper procedures, including failure to obtain authorization, by

either obtaining authorization from subjects or destroying the data/specimens already collected.

- Promptly reporting to the IRB/Privacy Board all data security breaches or any related unanticipated problem involving risks to study participants or others.
- Promptly ceasing PHI data transfers to a recipient if it is determined that the terms of a Data Use Agreement have been violated.

The IRB will be responsible for:

- Evaluating all research proposals involving the use or disclosure of PHI obtained from a Covered Component in accordance with applicable standards of the HIPAA Privacy Rule **including:**
  a) Requests to use PHI for identification of prospective research participants, evaluation of clinical trial sites, and protocol development;
  b) Requests to use PHI for the purpose of contacting prospective research participants;
  c) Research protocols for which participant authorization is sought to use, maintain or disclose their PHI;
  d) Requests to obtain limited data sets and the accompanying data use agreements required for this purpose;
  e) Requests to obtain a waiver of authorization, in whole or in part, including provisions necessary to provide an accounting of disclosures (e.g., retrospective chart reviews);
  f) Requests to access decedent PHI along with accompanying representations regarding the vital status of the individuals;
  Where an investigator elects not to use a data use agreement, authorization, or waiver of authorization, the IRB will review the investigator's proposed written representation to ensure that it is appropriate or justified.
  g) Requests to use biological materials or tissues accompanied by protected health information and created about or received from patients of a Covered Component, or maintained by or on behalf of Covered Component;
  h) Requests to create and populate research databases and repositories of protected health information at a Covered Component, and the subsequent use of the information in such databases and repositories.
- Conducting annual, or more frequent reviews if warranted, of the projects under its purview and obtaining updated privacy and security information for applicable studies.
- Evaluating and responding to situations when PHI has been obtained without proper authorization or applicable exemption and specifying corrective action, which could include requiring immediate destruction of the data or obtaining authorization forms from subjects.
- In consultation with FAU's Office of Information Technology (OIT) and the relevant College information technology representative, evaluating data security provisions for safeguarding PHI as described in the IRB protocol

to ensure security provisions are sufficient to protect the privacy and confidentiality of human subjects.
- Evaluating and responding to data security and privacy breaches as appropriate to protect human subjects involved in FAU research protocols.

The Research Integrity office will be responsible for:
- Advising researchers on HIPAA compliance, in consultation with FAU's Chief Privacy Officer and General Counsel's office, as appropriate.
- Ensuring HIPAA forms and documented approval letters contain the appropriate content and review criteria as outlined in federal regulations.
- Pre-reviewing IRB submissions to determine when HIPAA forms should be included for IRB/Privacy Board review.
- Coordinating with OIT and other IT professionals, as warranted, to ensure appropriate expertise is available to review data security plans for PHI used in research.
- Verification that researchers have completed appropriate training prior to working with PHI for research purposes.

Division of Research Offices (Sponsored Programs, Legal, etc.) will be responsible for:
- Coordinating review and signature of relevant contractual agreements with appropriate reviewing and signature authorities.
- Requesting and obtaining from the PI relevant documentation as outlined by the applicable agreement before final approval and signature is secured.

VII. Procedures

For persons who are FAU faculty, staff or students of a Covered Component and persons that are not members of a Covered Component but who wish to obtain PHI for research purposes[1], the following procedures apply:

Research Using De-Identified Health Information:

To use or disclose "de-identified" data for research purposes, the following is required:

- The patient data must be de-identified using one of the following methods:
  a. ***The Safe Harbor Method:*** Remove the 18 key identifiers from the PHI dataset. This can be done by the workforce members of the Covered Component (e.g., clinic, hospital, etc.) and documented via the Assessment Tool 2: Am I Using PHI (De-Identification Certification Form), or through the services of an Honest Broker (see definition in Appendix A below). If the Covered Component wishes to use the services of the Honest Broker, they must enter into a Business Associate Agreement with that person/entity prior to this service. **OR**
  b. ***Expert Determination:*** Obtain documentation that a statistician (or other person with appropriate knowledge and experience with generally accepted statistical and scientific principles for rendering information not individually identifiable) has determined that the risk is minimal that the

information could be used, alone or in combination with other available information, to identify the person whose information is being used.

- The Covered Component providing the data is permitted to assign and retain a code to allow the re-identification of PHI. However, the code cannot be derived from or related to the information about the subject. (e.g., the subject's initials and last 4 digits of their social security number cannot be used). Also, the Covered Component cannot disclose the re-identification code or the method of re-identifying the PHI to the researchers or to anyone else.

Research Use/Disclosure with Individual Authorization:

To use or disclose PHI with authorization by the research participant, the following is required:

- Prepare and submit, as part of the IRB submission package, either the standalone HIPAA Authorization Form or the combined Consent Form/Authorization (see templates in IRBNet).
- Obtain an additional, separate authorization if the research involves the use or disclosure of psychotherapy notes.
- Maintain an accounting of PHI disclosed for research purposes so that an individual who requests this data can see to whom and how often their PHI has been disclosed.

This accounting must include disclosures of PHI that occurred during the six years prior to an individual's request for an accounting in general. (See 45 CFR 164.528) As part of the study, if you collect PHI from more than fifty subjects, you may use a simpler *Modified Accounting System* as referenced in Definitions below. (45 CFR 164.528)

Research Use/Disclosure without Authorization: (For example, to conduct medical records research, a waiver may be appropriate when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants' authorization were required.) 45 CFR 164.512(i)(1)(i)

To use or disclose PHI *without* authorization by the research participant, the following is required:

- Submit a request to the IRB/Privacy Board for waiver or alteration of the authorization requirement using Form 7, Request for Waiver of HIPAA Authorization Requirement as part of the IRB submission package. The responses on the form should contain thoughtful and substantive responses to the criteria for a waiver or alteration of authorization as outlined on the form and in the federal regulations.
- Obtain documentation from the IRB/Privacy Board that an alteration, or waiver of authorization, for use or disclosure of a research participant's PHI has been approved.
- **Note:** If a Covered Component uses or discloses PHI based on an IRB approved waiver or alteration of the authorization requirement, the covered entity must retain the IRB's documentation on which it relied for at least 6

years from the date the waiver or alteration was obtained, or the date when it was last in effect, whichever is later. (§ 164.316(b)(2)(i)).

Review of PHI as Preparation for Research:

To obtain PHI solely as *preparation for research* (e.g., to design a research study, assess the feasibility of conducting a study, or to prepare a grant application), the following is required:

- Submit the Request to use PHI Preparatory to Research to the primary privacy contact of the Covered Component. Ensure the request addresses the required elements outlined in 45 CFR 164.512(i)(1)(ii) including a) that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research, b) that the researcher will not remove any PHI from the covered entity, and c) that the PHI for which access is sought is necessary for the research purposes.
- Obtain documented approval prior to conducting these activities and submit a copy along with your IRB submission. Also, submit as appropriate to the Privacy Officer and/or person responsible for release of medical information in the unit.

Review of PHI to Recruit Research Participants:

To obtain PHI to contact potential research participants, the following is required:

- <u>If you are the treating health care provider/staff,</u> you may review patient records to identify prospective research participants and contact them to discuss the research opportunity.

  Submit the Request to use PHI Preparatory to Research to the primary privacy contact of the Covered Component.

- <u>If you are NOT the treating health care provider/staff,</u> you may review patient records to identify prospective research participants using the review of PHI preparatory to research mechanism (which requires certain representations and approvals as described herein). However, it is preferred that the treating health care provider contact them to discuss the research opportunity.

- In some cases, and with justification, the IRB may approve a method where contact is made jointly by the researcher and treating provider, or by the primary health care provider referring the patient to the researcher, if eligible for participation. The goal is to ensure recruitment is done in a manner that is the least intrusive to an individual's privacy.

  In these cases, the researcher must either obtain a signed Authorization form, or request and obtain a Partial Waiver of Authorization to use PHI to contact a covered component's patients as part of the overall IRB application. The request should be accompanied by a letter of cooperation indicating that the treating health provider has agreed to this method.

  If the researcher also needs to screen potential research participants for eligibility after contacting them, and that involves soliciting health information to

ensure they meet inclusion criteria, this should be included in the authorization or waiver of authorization request submitted to the IRB.

Research on the Protected Health Information of Decedents

To conduct research on the Protected Health Information of decedents (deceased persons):

- Submit a request to use PHI of decedents to the primary privacy contact of the Covered Component.
- Ensure the request addresses the required elements outlined in 45 CFR 164.512(i)(1)(iii), including that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research and, at the request of the Covered Component, documentation of the death of the individuals about whom information is being sought.
- Obtain documented approval from the primary privacy contact of the Covered Component stating that the request has been approved and meets the requirements of the federal regulations (45 CF 164.512(i)(1)(iii)). Submit as appropriate to the Privacy Officer and/or person responsible for release of medical information in the unit.
- As set forth under the privacy rule, individually identifiable health information of a person who has been deceased for more than 50 years is not PHI.

Research with a Limited Data Set

A limited data set excludes all direct identifiers of the individual or his/her relatives, employers, or household members, EXCEPT dates directly related to an individual and town, city, state, zip code. (See Assessment Tool 2 as a resource)

To disclose or obtain this type of data set, the following is required:

- A data use agreement or "DUA" (see FAU template found in IRBNet) must be entered into by both the Covered Component and the researcher, so that the Covered Component may disclose a limited data set to the researcher for research, public health, or health care operations.
- The DUA must be accompanied by a list of requested data elements and be reviewed by Counsel and signed by the Director of Sponsored Programs or his/her designee
- Those disclosing the data must ensure the data is stripped of all identifiers except dates directly related to an individual and town, city, state, zip code.
- The DUA accompanied by the list of requested data from the medical record must be submitted to the IRB as part of the related research protocol review and approval.

Research Use/Disclosure involving Business Associates

- FAU uses the services of a variety of businesses or independent contractors to carry out some of its activities, services and functions. HIPAA allows a Covered Component to disclose PHI to these external parties if they enter into a Business Associate Agreement (BAA) with FAU that obligates the business associate to take

appropriate steps to safeguard the information consistent with the HIPAA guidelines.

- Under HITECH, Business Associates of a Covered Entity are directly liable for compliance with certain HIPAA privacy and security rules and requirements.
- A BAA is not needed to share PHI with a Business Associate for **treatment, payment, or health care operations** (which includes training and other activities related to running or improving a health care site).
- In research, one of the most common scenarios where Covered Components involve Business Associates is for recruitment or protocol development. A business associate may need to access PHI to assist them with identifying or contacting study participants, or to help design a research protocol. Contact Research Integrity or General Counsel for guidance.

In situations where FAU personnel obtain PHI from Covered Components outside of the university (hospitals, nursing homes, mental health facilities, doctors' offices, etc.) the same general procedures apply but researchers may be required to follow the institution-specific procedures of that Covered Component. If that Covered Component does not have an IRB, Privacy Board, or Privacy Office/official that conducts such reviews, the PI should consult with the FAU IRB.

VIII. Policy Renewal: As needed

IX. References

45 CFR 160 and 164

POLICY APPROVAL

Initiating Authority

Daniel C. Flynn, Ph.D. Date: 2022.03.29 14:43:45 -04'00'

Signature: Date: 3/29/22

Name: Daniel C. Flynn, Ph.D., Vice President for Research

Executed signature pages are available in the Initiating Authority Office(s)

Appendix A: Definitions

Authorization: Written permission given by the individual, or his/ her Legally Authorized Representative, to allow a Covered Entity to use or disclose protected health information about the individual. The requirements of a valid authorization are defined by the HIPAA regulations.

Accounting for Disclosures of PHI: The provision of a list of disclosures made by a Covered Component of FAU. Accountings include information that describes a covered entity's disclosure of PHI that has taken place within six (6) years of the date of the request. Accounting of disclosures is not required in the following situations:

- Disclosures for treatment, payment, and health care operations ("TPO")
- Disclosures to the individual
- Disclosures made pursuant to valid authorizations
- Disclosures for national security or intelligence purposes
- Disclosures to correctional institutions or law enforcement officials
- Disclosure of Limited Data Sets
- Disclosure of de-identified data
- Disclosures of PHI prior to April 14, 2003

Breach: The unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property.

Business Associate: Generally an entity or person who performs a function involving the use or disclosure of Protected Health Information (PHI) on behalf of a covered entity (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation). For example, an individual or company hired by an investigator (who is part of a covered entity) to review PHI to identify and recruit potential research subjects would be a "business associate."

Clearinghouse: Health care clearinghouse means a public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Covered Component: Components of a covered entity that engage in 'covered functions' and, any component that engages in activities that would make it a 'business associate' of a component that performs covered functions if the two components were separate legal entities.

Covered Entity: A health plan, a health care provider, or a health care clearinghouse who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.

There are three Covered Entities at FAU: 1) the College of Medicine; 2) the College of Nursing (including the Community Health Center (CHC) and Louis and Anne Green Memory and Wellness Center (MWC)); and 3) Student Health Services and Pharmacy.

Covered Functions: Activities of a covered entity, the performance of which makes the entity a health plan, a health care provider, or a health care clearinghouse.

Data Use Agreement: An agreement or contract, which serves as satisfactory assurance that the recipient of a limited data set will only use or disclose the protected health information for limited purposes. A data use agreement between the covered entity and the limited data set recipient must:

1) Establish the permitted uses and disclosures by the recipient of information in the limited data set. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of the privacy rules;
2) Establish who is permitted to use or receive the limited data set; and
3) Provide that the limited data set recipient will:
   a. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
   b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
   c. Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

De-Identified Data: Data (containing health information) that does not identify an individual and with respect to which there is no reasonable basis to believe that information within the data can be used to identify an individual. Consistent with the Privacy Rule, health information is considered de-identified: 1) upon the removal of a list of eighteen (18) direct identifiers defined under HIPAA that could be used to identify an individual; 2) if an expert, who can determine and document, using generally accepted statistical and scientific principles and methods, that there is a very small risk that the information used alone or in combination with other reasonably available information could be used to identify the subject of the information. The 18 identifiers are as follows:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Census Bureau: (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;

10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted by item #3.

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

Electronic Protected Health Information (ePHI) – PHI in electronic form.

EMR: Electronic Medical Record

Health Care Operations: Any of the following activities of a covered entity that relate to its covered functions:

1. Conducting Quality Assessment and Improvement activities, including the following: outcomes evaluation and development of clinical guidelines; patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; and contacting health care providers and patients with information about treatment alternatives;
2. Reviewing the competence or qualifications of health care professionals including the following: evaluating practitioner and provider performance; conducting training programs; accreditation; certification; licensing; or credentialing activities;
3. Underwriting (except as prohibited under 45 CFR §164.502 (a)(5)(i)(e.g., involving genetic information)), enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance of health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care;

4. Conducting or arranging for medical review, legal services and auditing functions including fraud and abuse detection and compliance programs;
5. Business planning and development such as conducting cost-management and planning-related analyses related to managing and operating the entity; and
6. Business management and general administrative activities including the following: management activities relating to implementation of and compliance with the requirements of the privacy regulations; customer service; resolution of internal grievances; the sale, transfer, merger, or consolidation of all or part of the covered entity; and creating de-identified health information or a limited data set; and fundraising for the benefit of the covered entity.

HIPAA – Health Insurance Portability and Accountability Act of 1996.

Honest Broker: An entity which keeps sets of private information but distributes parts of those sets to other entities who should not have access to the entire set.

For example, in research involving biological specimens donated for research, the honest broker would keep both the specimen and associated protected health information, but only allow researchers to have access to the specimen without the protected health information.

Individually Identifiable Health Information: Information that includes demographic information collected from an individual, and

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 (a) that 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.

Hybrid Entity: A single legal entity that is a covered entity, whose business activities include both medical services (also known as "Covered Components") and non-medical activities (also known as "Non-Covered Components"), and that designates health care components in accordance with the Privacy Rule.

Legally Authorized Representative: A person authorized either by state law or by court appointment to make decisions, including decisions related to health care, on behalf of another person, including someone who is authorized under applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure involved in the research.

Limited Data Set: Protected health information that excludes 16 HIPAA categories of direct identifiers of the individual or of relatives, employers, or household members of the individual, but may retain city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. A limited data set is described as health information that excludes certain listed direct identifiers: 1) Names. 2) Postal address information, other than town or city, state and ZIP Code. 3) Telephone numbers. 4) Facsimile numbers. 5) Electronic mail addresses. 6) Social security numbers. 7) Medical record numbers. 8) Health plan beneficiary numbers. 9) Account numbers. 10) Certificate/license numbers. 11)

Vehicle identifiers and serial numbers, including license plate numbers. 12) Device identifiers and serial numbers. 13) Web universal resource locators (URLs). 14) Internet protocol (IP) address numbers. 15) Biometric identifiers, including fingerprints and voiceprints. 16) Full- face photographic images and any comparable images.

Limited data sets may only be used for research, public health or for health care operations; and only with a data use agreement that limits the use of the data by the recipient.

Minimum Necessary: Reasonable efforts made to limit the use, disclosure, or request for PHI to the minimum necessary to accomplish the intended purpose.

Modified Accounting System: A system of accounting that can be utilized only in research studies that involve more than fifty records, where the covered entity must provide the individuals with just the following information:

- The name of the protocol or other research activity;
- Plain language description of the research protocol or activity including the purpose of the research, and criteria for selecting particular records;
- A brief description of the type of protected health information that was disclosed;
- The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

- A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

Personal Identification Information (PII) – As defined by Florida Statute 817.568(1)(f), under which fraudulent use is prohibited, PII means "any name or number that may be used, alone or in conjunction with other information, to identify a specific individual, including any:

1. Name, postal or electronic mail address, telephone number, Social Security number, date of birth, mother's maiden name, official state-issued or US-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code;
4. Medical records;
5. Telecommunication identifying information or access device; or
6. Other number or information that can be used to access a person's financial resources."

Privacy Rule – The regulations at 45 CFR §§ 160 and 164 that detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.

Protected Health Information (PHI): Individually identifiable health information collected from an individual that is: 1) transmitted by electronic media; 2) maintained in electronic media; or 3) transmitted or maintained in any other form or medium by a Covered Component.

PHI encompasses information that identifies an individual or might reasonably be used to identify an individual and relates to: the individual's past, present or future physical or mental health or condition of an individual; the provision of health care to the individual; or the past, present or future payment of heath care to an individual.

PHI excludes individually identifiable health information in: a) education records covered by the Family Educational Rights and Privacy Act (FERPA); b) records described at 20 U.S.C.

§1232g(a)(4)(B)(iv); c) employment records held by a covered entity in its role as employer; and d) regards to a person who has been deceased for more than 50 years.

Research: A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research.

Reviews Preparatory to Research: Using or reviewing PHI for the purposes of developing a research protocol or formulating a research hypothesis.

Sensitive Information – Information that is protected against unwarranted disclosure. Access to sensitive information should be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations. Sensitive information also includes any information that is protected by FAU policy from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, some types of research data (such as research data that is

personally identifiable or proprietary), public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

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 provider to another.

Waiver of Authorization: Approval by the IRB for a researcher to use and disclose protected health information for a research activity, including but not limited to, identifying, recruiting, and/or enrolling subjects without the patient's permission.

Waiver, Partial Waiver or Alteration of Authorization: The document that the covered entity or covered component obtains from the IRB or Privacy Board which states that the Board has waived or altered the requirements of the HIPAA Privacy Rule, that an individual must authorize the use or disclosure of an individual's PHI for research purposes.

Workforce Members: Employees, volunteers, trainees, and other persons whose conduct in the performance of work for a covered entity is under the direct control of such entity, whether or not they are paid by that entity.