Glossary and Terms

Affiliated Covered Entity: Legally separate covered entities that are associated in business.

Asset – Any tangible or intangible thing or characteristic that has value to an organization. There are many types of assets. Some of these include obvious items such as machines, facilities, patents, and software. But the term can also include less obvious items such as services, information, people, characteristics such as reputation and image or skill and knowledge.

Authorization – Permission given by the individual to use and/or disclose protected health information about the individual. The requirements of a valid authorization are defined by the HIPAA regulations.
Suggestion: 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.

Availability – Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users.

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).

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.

Common Control – If an entity has the power, either directly or indirectly, to significantly influence or direct the actions or policies of another entity.

Complaint (Privacy) – An allegation by an individual that an organization is not complying with the requirements of federal and/or state privacy regulations or the organization's own policies and procedures related to the privacy of personal information.

Confidential Communications – Refers to the ability of an individual to request that his/her health information be protected through the use of an alias or by using a different mailing address.

Confidentiality – The practice of controlling data or information such that it is not made available or disclosed to unauthorized persons or processes.

Controls – Any administrative, management, technical, or legal method that it used to manage risk. Controls are safeguards or countermeasure. Controls include things like practices, policies, programs, techniques, guidelines, and organizational structures. [not sure whether we want to modify; taken verbatim from Information and Data Security Policies COM]

Covered Component - Health care components of a Hybrid Entity, named and designated by the Hybrid Entity, that engage in Covered Functions, and any component that engages in activities that would make it a Business Associate of a Covered Component if the two components were separate legal entities.

.

Covered Entity – A health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule; the Covered Entity refers to the health care components of FAU that engage in Covered Functions.

Covered Functions - Activities of a Covered Entity, the performance of which makes the entity a health plan, a health care clearinghouse, or a health care provider subject to the Privacy Rule.

Data Set – A semantically meaningful unit of information exchanged between two parties to a transaction.

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;
    d. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
    e. Not re-identify the information or contact the individuals.

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.

Designated Record Set – 1) The medical records and billing records about individuals maintained by or for a covered health care provider; 2) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; 3) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

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

Encryption – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Financial Remuneration – Direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Fundraising - A communication to an individual that is made by a covered entity, an institutionally related foundation, or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity.

Genetic Information – Information about: 1) the individual's genetic tests; 2) the genetic tests of family members of the individual; 3) the manifestation of a disease or disorder in family members of the individual; 4) any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. Genetic information includes the genetic information of a pregnant woman's fetus or that of a family member or of any embryo legally held by the individual or family member using

an assisted reproductive technology. Genetic information does not include the sex or age of an individual.

Genetic Services – Genetic test, genetic counseling (including obtaining, interpreting or assessing genetic information), or genetic education.

Genetic Test – An analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder or pathological condition.

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.

Hybrid Entity – A single legal entity that is a Covered Entity, performs business activities that include both Covered and non-Covered Functions, and that designates its health care components in accordance with the Privacy Rule.

Incident – An event, whether electronic, physical or social that adversely impacts the confidentiality, integrity, or availability of FAU data or information systems; or a real or suspected action, inconsistent with FAU's privacy or acceptable use policies. [We may want to add in greater specificity such as "Privacy, Confidentiality, and Information Security Agreement" and "Acceptable Use" policies - - are these in draft or final form?]. These include but are not limited to:

1. Attempts (either failed or successful) to gain unauthorized access to a system or its data;
2. Theft or loss of an information system asset or property;
3. Unwanted disruption or denial of service;
4. The unauthorized use of a system for the processing or storage of data; or
5. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.

Individually Identifiable Health Information – A subset of "heath information," including 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
3. Identifies the individual, or might reasonably be used to identify the individual.

Information Privacy – The privacy of personal information, usually relating to personal data stored on computer systems. The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business relations information or website data. Information privacy is also known as data privacy.

Institutional Review Board (IRB) – The IRB is an administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated.

Integrity – The condition that data or information have not been altered or destroyed in an unauthorized manner.

Law Enforcement Official – An officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or a territory, or an Indian tribe, who is empowered by law to: 1) investigate or conduct an official inquiry into a potential violation of

law; or 2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Lawfully Issued Subpoena – generally means a subpoena issued by or under the jurisdiction of a Florida or federal court.

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.

Marketing: To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, except the following:
Marketing does not include a communication made:

1. To provide refill reminders or other communications about a drug or biologic that is currently being prescribed for the individual, or if the financial remuneration received by the covered entity in exchange for making the communication is reasonable in relation to the covered entity's costs of making the communication; or
2. For the following purposes except where the covered entity receives financial remuneration in exchange for the communication:
    a. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication including communications about:
        i. The entities participating in a health care provider network or health plan network;
        ii. Replacement of, or enhancements to, a health plan; or
        iii. 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

b. For treatment of the individual, including case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; or
c. For case management or care coordination, contacting of individuals with information about treatment alternatives and related functions to the extent that these activities do not fall within the definition of treatment.

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.

Notification – The act of informing persons affected by a breach of private information that their information was included and steps they can take to protect themselves and their privacy.

Payment – The activities undertaken by a:
1) Health plan, except as prohibited under 45 CFR §164.502 (a)(5)(i)(e.g., use and disclosure of genetic information for underwriting purposes), to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan (as further described in §164.501) ; or
2) A health care provider or health plan to obtain or provide reimbursement for the provision of health care.

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.

Psychotherapy Notes – Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

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.

Risk – The likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; hence, it is vulnerable to a threat, such as a thunderstorm, which creates a risk. [not sure whether we want to modify; taken verbatim from Information and Data Security Policies COM]

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.

Threats – The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

TPO – Treatment, payment and health care operations. The HIPAA Privacy Rule permits disclosure of PHI only for TPO or when a regulatory exception applies (e.g., public health reporting).

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.

Unsecured Protection Health Information – Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of Health and Human Services in guidance related to Health Information Privacy. This guidance specifies that only encryption and destruction, consistent with the National Institute of Standards and Technology (NIST) guidelines, renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that notification is not required in the event of a breach of such information.

Use – The sharing, employment, application, utilization, examination, or analysis of individually identifiable information within an entity that maintains or holds such information.

Vulnerabilities – Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.

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.