This Glossary is not meant to be an exhaustive list of all terms used in the Privacy Policies and Procedures, but is only intended to place pertinent definitions within easy reach of readers. If the definitions of other terms are needed, please see the relevant source documents, such as the Federal Register, State statutes, University Regulations, etc.

Access: The ability or right to approach, enter, exit, communicate with, or make use of.

**HIPAA Privacy: Right of Access** – An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set.

**HIPAA Security:** The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any information system resource.

Active Records: Records, in any format, that are currently being used for ongoing patient care, student education, employment, payment, litigation, research, or other activities for which the record was created.

Acknowledgement of Receipt (HIPAA): A statement mandated by federal law and preferably signed by the patient, indicating that the patient received the Notice of Privacy Practices.

Addendum: Entries added to a health record to provide additional information in conjunction with a previous entry. The addendum should be timely, bear the current date, time, and reason for the additional information being added to the health record.

Administrative Safeguards: Administrative actions and policies and procedures within an organization, to manage the selection, development, implementation, and maintenance of security measures to protect electronic personal, financial, and health information and to manage the conduct of the covered entity’s or business associate’s workforce in relation to the protection of that information.

Administrative Simplification Provisions: means any requirement or prohibition established by:

b. Section 264 of Pub. L. 104–191;
c. Sections 13400–13424 of Public Law 111–5; or
d. 45 CFR Parts 160 - 164.

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

Amendment: The formal and deliberate alteration of a health record, after the original documentation has been completed and signed by the provider, to make the original documentation more accurate. No individual entries may be altered, obliterated, removed or destroyed.

Archiving / Storage: The act of physically or electronically moving inactive records to a storage location until the retention requirements for those records are met.

Audio-conference: Real-time verbal communications over distances, using electronic transmission systems, between two or more persons.

Authentication: The corroboration that a person is the one claimed; most often refers to an ability to prove authorship, by written signature, initials or computer password.
Authorization: A document or the action or fact of giving consent or permission or conferring authority on another person or entity.

Authorized Access: Rights granted to an individual to allow access to information.

Authorized Disclosure: The permissible release, transfer, provision of, access to, or, divulging in any other manner of information by any means of communication outside the entity holding the information.

Availability: The property that data or information is accessible and usable upon demand by an authorized person.

Back-up: Copy of files and applications made to avoid loss of data and facilitate recovery of data and information.

Breach (HIPAA): the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the protected health information.

1. Breach excludes:
   a. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a 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 under subpart E of this part.
   b. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
   c. A disclosure of protected health information where a covered entity or 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.

2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under [HIPAA] subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
   a. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
   b. The unauthorized person who used the protected health information or to whom the disclosure was made;
   c. Whether the protected health information was actually acquired or viewed; and
   d. The extent to which the risk to the protected health information has been mitigated.

Business Associate (HIPAA):

1. Except as provided in paragraph (4) of this definition, with respect to a covered entity or of an organized health care arrangement, in which the covered entity participates, a person, not a member of the workforce, who:
   a. On behalf of a covered entity or of an organized health care arrangement, 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 CFR 3.20, billing, benefit management, practice management, and repricing; or
b. Provides legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

2. A covered entity may be a business associate of another covered entity.

3. Business associate includes:
   a. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
   b. A person that offers a personal health record to one or more individuals on behalf of a covered entity.
   c. A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

4. Business associate does not include:
   a. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
   b. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of §164.504(f) apply and are met.
   c. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
   d. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(a) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(b) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Certification of Review (HIPAA): Approval from the IRB for a researcher to access protected health information either in preparation for conducting research, or for conducting research using decedent information.

Civil money penalty or penalty: the amount determined under § 160.404 of this part and includes the plural of these terms.

Code Set (HIPAA): Any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

Common Control (HIPAA) exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common Ownership (HIPAA) exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Compromise: In regard to electronic data, access in excess of that intended to be available.

Confidentiality: The practice of controlling data or information such that it is not made available or disclosed to unauthorized persons or processes.
Contrary (HIPAA): When used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this federal regulation, means:
1. A covered entity or business associate would find it impossible to comply with both the State and federal requirements; or
2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of the regulations.

Correction: The formal and deliberate alteration or other modification of documentation to make it more accurate. In electronic records, corrections must be made as addendums; they may also involve removing information from one record and posting it to another within the electronic document management system.

Correctional Institution: any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

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

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

Data Aggregation (HIPAA): The combining by a business associate of protected health information from more than one covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Data Set (HIPAA): A semantically meaningful unit of information exchanged between two parties to a transaction.

Data Use Agreement (HIPAA): 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.
Database: A collection of information, usually recorded in alpha or numeric terms, and organized for rapid search and retrieval, as by a computer.

De-Identification: Manipulating protected health information to meet the following criteria:

1. Generally accepted statistical and scientific principles and methods for rendering information not individually identifiable are applied by a person with appropriate knowledge of, and experience with, such principles and methods:
   a. Determining that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
   b. Documenting the methods and results of the analysis that justify such determination; or
2. The following identifiers of the individual and relatives, employers, or household members of the individual are removed:
   a. Names;
   b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
      1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
      2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
   c. 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;
   d. Telephone numbers;
   e. Fax numbers;
   f. Electronic mail addresses;
   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 by paragraph (c) of this section; and
3. The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
Deletion: The action of permanently eliminating information that is not viewable in a paper record or tracked in a previous version of an electronic record. UF does not allow permanent deletions of clinical information from any health records.

Designated Record Set (HIPAA):

1. A group of records maintained by or for a covered entity that is:
   a. The medical records and billing records about individuals maintained by or for a covered health care provider;
   b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
   c. Used, in whole or in part, by or for the covered entity to make decisions about patients.

2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Destruction of Records: The systematic permanent disposal of records that have been maintained for the prescribed retention period.

Direct Treatment Relationship (HIPAA): A treatment relationship between an individual and a health care provider in which the provider makes decisions about the health care management of the patient.

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

Disposal of Records: The day-to-day discarding of duplicate or extra reports which are not required to be maintained, and are not pertinent to the purpose for which the records were created.

Documentation: Evidence, proof, or substantiation that certain actions were completed, information was collected, used or disclosed, or requirements were met. The act of making a record or setting down facts in permanent form.

Electronic Data Interchange (HIPAA): Electronic transfer of information, such as electronic media health claims, in a standard format between trading partners.

Electronic Media:

1. Electronic storage material on which data is or may be recorded electronically, including devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

2. Transmission media used to exchange information already in electronic storage media.
   a. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dialup lines, private networks, and the physical movement of removable/transportable electronic storage media.
   b. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
Electronic Protected Health Information (HIPAA): information transmitted by or maintained in electronic media that comes within the definition of protected health information.

E-mail (Electronic Mail): A means or system for transmitting written messages electronically (as between terminals linked by telephone lines, cable networks, or microwave relays).

Employer (HIPAA): is defined as it is in 26 U.S.C. 3401(d).

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.

Expiration Date (Authorizations): The date through which an authorization may be used to disclose information created prior to the date the authorization was signed.

Facility: The physical premises and the interior and exterior of a building(s).

Family member: with respect to an individual:
1. A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
2. Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
   a. First-degree relatives include parents, spouses, siblings, and children.
   b. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
   c. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
   d. Fourth-degree relatives include great-great-grandparents, great-great-grandchildren, and children of first cousins.

Fax: A means or system for transmitting copies of documents electronically, usually between terminals linked by telecommunications networks.

Fundraising: The organized activity of soliciting and acquiring monetary or other resources for an institution or organization.

Genetic Information (HIPAA):
1. Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
   a. The individual’s genetic tests;
   b. The genetic tests of family members of the individual;
   c. The manifestation of a disease or disorder in family members of such individual; or
   d. 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.
2. Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:
   a. A fetus carried by the individual or family member who is a pregnant woman; and
   b. Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.
3. Genetic information excludes information about the sex or age of any individual.
Genetic Services (HIPAA):
1. A genetic test;
2. Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

Genetic Test (HIPAA): 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.

Group Health Plan (HIPAA): (also see definition of Health Plan) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
1. Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
2. Is administered by an entity other than the employer that established and maintains the plan.

Health and Human Services: (HHS) stands for the Department of Health and Human Services.

Health Care (HIPAA): Care, services, or supplies related to the health of a patient. Health care includes, but is not limited to, the following:
1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a patient or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse (HIPAA): A public or private entity, including a billing service, repricing 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.

Health Care Component (HIPAA): A component or combination of components of a hybrid entity designated as meeting the definition of a covered entity if the component were a separate legal entity. Designations must include any component that would meet the definition of a covered entity if it were a separate legal entity. May also include a component only to the extent that it performs: (1) Covered functions; or (2) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

Health Care Operations (HIPAA): Any of the following activities of the covered entity to the extent that the activities are related to covered functions:
1. Conducting Quality Assessment and Improvement activities, including:
   a. Outcomes evaluation and development of clinical guidelines (that cannot be classified as research);
   b. Patient safety activities (as defined in 42 CFR 3.20);
   c. Population-based activities relating to improving health or reducing health care costs;
   d. Protocol development, case management and care coordination;
e. Contacting of health care providers and patients with information about treatment alternatives; and
f. Related functions that do not include treatment;

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

3. Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

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, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

6. Business management and general administrative activities, including, but not limited to:
   a. Management activities relating to implementation of and compliance with the requirements of the privacy regulations;
   b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
   c. Resolution of internal grievances;
   d. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
   e. Creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.

**Health Care Provider (HIPAA):** A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnish(s), bills, or is paid for health care in the normal course of business.

**Health Information (HIPAA):** 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 a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient.

**Health Oversight Agency (HIPAA):** An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
Health Plan (HIPAA): A patient or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). (See the federal register text for detailed inclusions and exclusions.)

Hybrid Entity (HIPAA): 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 health care components in accordance with paragraph § 164.105(a)(2)(iii)(C) of the regulations.

Inactive Records: Records of individuals who have not received services, made payments for services, or been involved in litigation or research for a designated period of time, but which must still be retained for a period of time prescribed by law.

Incident: An event, whether electronic, physical or social that adversely impacts the confidentiality, integrity or availability of University of Florida data or information systems; or a real or suspected action, inconsistent with University of Florida Privacy or Acceptable Use policies. (See also Privacy Incident and Security Incident.)

Indirect Treatment Relationship (HIPAA): A relationship between an individual and a health care provider in which:
1. The health care provider delivers health care to the individual based on the orders of another health care provider; and
2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual: The person who is the subject of protected health information or personal identification information.

Individually Identifiable Health Information (HIPAA): Information that is a subset of health information, including demographic information collected from a patient, 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.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Institutional Review Board: A committee established by the University of Florida to protect the rights and welfare of human subjects recruited to participate in research activities conducted under the auspices of the University.
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 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 means a subpoena issued by or under the jurisdiction of a Florida or federal court. Subpoenas issued by other state courts will not be honored.

Legal Health Record: A formally defined legal business record, made by a healthcare organization, in the routine course of business at or near the time that events occurred. Documentation is comprised of individually identifiable data, recorded in any medium, collected from multiple healthcare disciplines, and used by healthcare professionals while providing patient care or services, reviewing patient data, or documenting observations, actions, or instructions.
1. The legal health record is a subset of the entire patient database, and serves to identify what information constitutes the official business record of an organization for evidentiary purposes.
2. Documentation that makes up the legal health record may physically exist in separate and multiple paper-based files or electronic/computer-based databases. These components would be compiled and released upon receipt of a legally authorized request.
3. Documentation may include personal identification information, diagnoses, treatments and services provided, and payment for services. Documentation may also include copies of records, created elsewhere, that are considered relevant to decisions made about care or services provided at UF.

Limited Data Set (HIPAA): A limited data set is health information that excludes all direct identifiers, as defined by the HIPAA Privacy Rule, except for dates and postal address information other than town or city, State, and zip code related to the patient or to relatives, employers, or household members of the patient. (That is, whole dates (day/month/year), town/city, State, and zip codes may be included in a Limited Data Set.)

Malicious Software means electronic instructions, named by function (virus, worm, “Trojan horse”, etc.) designed to damage or disrupt a computer system, usually inserted surreptitiously into the system.

Manifestation or manifested: with respect to a disease, disorder, or pathological condition, the fact that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Marketing:
1. Except as provided in paragraph (2) of this definition, to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
2. Marketing does not include a communication made:
   a. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.
b. For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication

1) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

2) 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:
   a) The entities participating in a health care provider network or health plan network;
   b) Replacement of, or enhancements to, a health plan;
   c) 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

3) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

3. Financial remuneration means 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.

**Mitigation:** To make less severe, to partially remove, or to correct, so that harmful effects of a privacy violation are reduced or eliminated.

**Modify or modification** refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

**More Stringent (HIPAA):** When comparing a provision of State law and a federal requirement, a State law that meets one or more of the following criteria:

1. The law prohibits or restricts a use or disclosure which would otherwise be permitted under the federal privacy regulation, except if the disclosure is:
   a. Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with the privacy regulations; or
   b. To the individual who is the subject of the individually identifiable health information.

2. The law permits greater rights to the individual who is the subject of the individually identifiable health information, regarding access to or amendment of the information.

3. The law provides that a greater amount of information be provided to the individual about a use, a disclosure, rights, and remedies.

4. With respect to the form, substance, or the need for express legal permission from the individual for use or disclosure of individually identifiable health information, the law provides requirements that narrow the scope or duration, increase the privacy protections afforded, or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

5. With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

6. The law provides greater privacy protection for the individual who is the subject of the individually identifiable health information in any other matter.

**National Provider Identifier - NPI (HIPAA):** The standard unique health identifier for health care providers; a 10-position numeric identifier, with a check digit in the 10th position, and no intelligence about the health care provider in the number.
**Need-to-Know:** Approved access to, or knowledge or possession of specific information required to carry out official duties by officers and employees of the enterprise that maintains the data. (See also Professional Need to Know.)

**Notice of Privacy Practices (HIPAA):** A statement mandated by federal and state laws that outlines how the University of Florida and its affiliates will use and disclose patients’ protected health information and how patients may gain access to that information.

**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.

**Organized Health Care Arrangement (HIPAA):**
1. A clinically integrated care setting in which patients typically receive health care from more than one health care provider;
2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
   a. Hold themselves out to the public as participating in a joint arrangement; and
   b. Participate in joint activities that include at least one of the following:
      1) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
      2) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
      3) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

**Password:** Confidential authentication information composed of a string of characters, used to gain access to all or part of a computer system or program.

**Patient Records:** Recorded information about individually identifiable patients, including healthcare, financial, and research records, maintained in any format.

**Payment (HIPAA):**
1. The activities undertaken by:
   a. Except as prohibited under §164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
   b. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
2. The above activities relate to the patient to whom health care is provided and include, but are not limited to:
   a. Determinations of eligibility or coverage (including coordination of benefits or determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
   b. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
   c. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
   d. Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
   e. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
      1) Name and address;
      2) Date of birth;
      3) Social security number;
      4) Payment history;
      5) Account number; and
      6) Name and address of the health care provider and/or health plan.

**Person** means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

**Personal Health Record** (PHR): As defined in section 13407(f)(2) of ARRA/HITECH, the term “personal health record” means an electronic record of identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

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

1. [Names and Numbers:]
   a. Name,
   b. Postal or electronic mail address,
   c. Telephone number,
   d. Social security number,
   e. Date of birth,
   f. Mother’s maiden name,
   g. Official state-issued or US-issued driver's license or identification number,
   h. Alien registration number,
   i. Government passport number,
   j. Employer or taxpayer identification number,
   k. Medicaid or food stamp account number,
   l. Bank account number,
   m. Credit or debit card number, or
   n. 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, voiceprint, retina or iris image, or other unique physical representation;

3. Unique electronic identification number, address, or routing code; or

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.

Personal Information: As defined by Florida Statute 817.5681(5) and for which notification is required, if breached: “An individual’s first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:
   1. Social security number.
   2. Driver’s license number or Florida Identification Card number.
   3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account. (more)
   “For purposes of this section, the term “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.”

Personal Portable Data Device: Any easily mobile, usually hand-held, device that provides manipulation, storage and/or retrieval capabilities for information, sound, or images for personal or business purposes, used by University of Florida faculty, staff, students or volunteers.

Personal Representative: A person acting on behalf of the patient who must be treated as the patient for the purposes of the privacy regulations.

Physical Safeguards: Tangible measures, with corresponding policies and procedures, to protect a covered entity’s or business associate’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and from unauthorized intrusion.

Primary Record: Original documentation created and maintained in any format as a result of a patient or client encounter in any of UF’s healthcare facilities, including faculty practice clinics and student health clinics.
   1. Documentation may include elements of personal identification, diagnoses, treatment, services provided, and payment for services, which are created and collected by the health professionals contributing to that patient’s care.
   2. Documentation may also include copies of records created elsewhere that are considered relevant to the patient’s care provided by UF.
   3. Primary paper records are usually maintained in and/or by the entity where the care was given and are considered the legal documents for clinical and financial purposes.

Privacy: Freedom of an individual from intrusion or observation; the right to maintain sole control over personal information; and the expectation that others will respect the individual’s privacy rights.

Privacy Complaint: 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.

Privacy Incident: A known or suspected action, inconsistent with the organization’s policies and procedures, or an adverse event, related to protected health information or other restricted information.

Privacy Officer (HIPAA): A member of the University of Florida’s staff, appointed to serve as the privacy official for the University, as mandated by the federal privacy regulations.

Private Data: Any and all personal identification information, financial information, protected health information, and other information protected by law (i.e., student records and reports; or, human resource data, including...
disciplinary actions). (See also Restricted Information and Sensitive Information. More details available on the UF IT Security website.)

Professional Need to Know: Specific and limited information necessary to complete assigned work.

Protected Health Information (PHI) (HIPAA):
1. Individually identifiable health information that is:
   a. Transmitted by electronic media;
   b. Maintained in electronic media; or
   c. Transmitted or maintained in any other form or medium.

2. PHI excludes individually identifiable health information:
   b. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
   c. In employment records held by a covered entity in its role as employer; and
   d. Regarding a person who has been deceased for more than 50 years.

Psychotherapy Notes (HIPAA): 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 patient’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.

Public Health Authority (HIPAA): An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Public Official: a person elected or appointed to carry out some portion of a government’s sovereign powers.

Qualified Protective Order (HIPAA): An order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
1. Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
2. Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

Reasonable Cause: an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

Reasonable Diligence: the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Reasonable Person Standard: A hypothetical person who exercises qualities of attention, knowledge, intelligence and judgment that society requires of its members for the protection of their own interest and the interests of others. (i.e. A test for negligence is based on either a failure to do something that a reasonable person, guided
by considerations that ordinarily regulate conduct, would do, or on the doing of something that a reasonable person would not do.

Record Schedule: A list of definitions for record types, uses, and retention requirements, prescribed by State of Florida statutes and regulations. (More information is available on the UF Records Management website.)

Required by law (HIPAA) means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to:
1. Court orders and court-ordered warrants;
2. Subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information;
3. A civil or an authorized investigative demand;
4. Medicare conditions of participation with respect to health care providers participating in the program; and
5. Statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Respondent: A covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

Restricted Information: Any and all personal identification information, protected health information, financial information, and other information protected by law or contract, applicable to the University of Florida or its affiliated entities, as the case may be, or their respective personnel in their official capacities, in any format (paper, electronic, or other). Examples include: medical records and medical record numbers; student UFID numbers, grades, schedules, records, and reports; selected human resource data; social security numbers; and any individual consumer financial account information, including credit and debit card numbers.

Safeguards: Rules and specific methods established to protect health and identification information from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure to unintended recipients.

Satisfactory Assurance (HIPAA): A written statement and accompanying documentation demonstrating that the patient is aware of judicial proceedings for disclosure of protected health information and any objections have been satisfactorily resolved.
Scheduling Records: Procedure of identifying types of records and then determining how long the type of record must be retained, according to the UF General Records Schedule.

Security or Security Measures encompass all of the administrative, physical, and technical safeguards used to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration or destruction, and to maintain the integrity of the information.

Security Incident (HIPAA): The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

“Shadowing” or Observing (HIPAA): The extra-curricular observation of patient care or procedures that is outside the scope of a student’s required course work, or of a health care professional’s job duties; or viewing of patient care areas and/or health-related procedures by visitors (see definition).

Shadow Record: Primary record materials that are temporarily kept apart from the primary record, usually for the convenience of health care providers or their staff.

1. Shadow records may contain original documents that will eventually be included in the primary record, as well as materials that health care personnel desire to save temporarily, but that are not required in the primary record (material to be purged).
2. Shadow records may include billing information, extra copies of outside records, correspondence, raw test data, telephone notes, etc.

NOTE: Records that are created and maintained in UF clinics are not shadow records, even though they may share documents with other parts of UF, UFP and Shands HealthCare.

Standard means a rule, condition, or requirement:
1. Describing the following information for products, systems, services, or practices:
   a. Classification of components.
   b. Specification of materials, performance, or operations; or
   c. Delineation of procedures; or
2. With respect to the privacy of protected health information.

Standard Transaction (HIPAA): A transaction that complies with the applicable standard adopted under this part.

Standard transactions include:
1. Health care claims or equivalent encounter information
2. Payment and remittance advice
3. Claim status inquiry and response
4. Eligibility inquiry and response
5. Referral certification and authorization inquiry and response
6. Enrollment and disenrollment in a health plan
7. Health plan premium payments
8. Coordination of benefits

State refers to one of the following:
1. For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.
2. For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.
Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Super-Confidential Health Information: Information pertaining to Substance Abuse, Mental Health Conditions, HIV Testing, HIV/AIDS, Sexually Transmitted Diseases, and Genetic Information, as defined and protected by specific federal and state laws and regulations.

Technical Safeguards: The technology and the policy and procedures for its use that protect electronic information and control access to it.

Trading partner agreement (HIPAA): An agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement.

Transaction (HIPAA): The transmission of information between two parties to carry out financial or administrative activities related to health care, including:
1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
10. Health claims attachments.
11. Other transactions that the Secretary may prescribe by regulation.

Treatment (HIPAA): 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 Protected Health Information: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary [of Health and Human Services]; specifically, encryption for electronic PHI, and destruction for all other PHI.

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

User: A person or entity with authorized access to an information system.

Valid Business Purpose: Assigned job activities that provide a requirement to use your authorized access to view, read, modify, possess, or communicate data or information.

Verbal Communications: Includes all types of oral and assisted communications where the intent is to carry on a dialogue between one or more persons.
Verification of Identity: The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information.

Videoconference: A meeting among persons where both telephony (speech and sound transmission) and closed circuit television technologies are utilized simultaneously. Video teleconference communication is multi-way and synchronous, as it would be if all parties were in the same room. Also know as teleconferencing, tele-health and tele-medicine.

Violation or violate (HIPAA): as the context may require, failure to comply with an administrative simplification provision.

Violation (UF): Infraction of a law; going against established rules.

Visitors (HIPAA): Any person who is not formally associated with the University of Florida's health care components including, but not limited to:
1. Trade representatives,
2. Maintenance technicians,
3. Visiting health care professionals,
4. Visiting students (including non-HSC UF students),
5. Visiting family members of UF employees,
6. Applicants for University of Florida positions,
7. Any other similar persons or groups.
   The term “visitor” does not include UF students who are enrolled in a Health Science Center College or Program, volunteers, patients, or family members or friends visiting or accompanying patients.

Volunteering: providing, of an individual’s own free will, limited services that are within the scope of the individual’s expertise, with no monetary or material compensation for the services performed. Volunteers are not authorized to provide any direct patient care.

Waiver of Authorization (HIPAA): 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.

Willful neglect: conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

Workforce (HIPAA): employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

Workforce (UF): University of Florida (UF) faculty, staff, students, volunteers, trainees, and any other person, including, but not limited to, visiting and associate clinicians, visiting faculty, Business Associates, and other persons performing services for health care components of UF, whether temporary or permanent, whose conduct, in the performance of work with or for UF, is under the University’s direct control, regardless of whether the person is paid for their services or not.

Workstation: An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.
Electronic Data Classifications
http://www.it.ufl.edu/policies/security/uf-it-sec-data.html

Unrestricted Data
Data, which, if available to the public, will not harm an individual, group, or institution. Data in this classification must:

1. Be labeled appropriately.
2. Reside on an appropriately secured host.
3. Have appropriate integrity protection.
4. Have redundant systems to maintain availability as appropriate.
5. Be retained according to public record requirements.
6. Have an appropriate recovery plan.

Examples: UF home page, UF course catalog, seminar schedules, press releases, job announcements, advertisements

Sensitive Data
Data, which if available to unauthorized users, may harm an individual, a group or the institution, but is not Restricted Data as defined below. Data in this classification must meet all the requirements for Unrestricted Data and must:

1. Have a clearly defined purpose.
2. Be easily identified.
3. Have appropriate classification documentation.
4. Have individuals assigned for Data Principal and Data Custodian roles.
5. Have a clearly defined and documented user access list.
6. Have appropriate documentation available to users that explains their obligations to protect the data.
7. Be available only to those who are authorized.
8. Be stored and transmitted securely to prevent unauthorized access.
9. Be rendered unreadable prior to disposal.
10. Have other protection as required by law or UF policy, standards, and procedures.

Examples: Staff salaries, infrastructure diagrams such as building and network, strategy documents, financial information, purchasing information, policies, standards, and procedures, business recovery plans, system configurations, emergency response plans, emergency equipment inventories

Critical Data
Data with the highest level of protection includes, but is not limited to, data restricted by law, data restricted by legal contracts, security-related data such as passwords and risk assessments, and intellectual property. Data in this classification must meet all the requirements of Sensitive Data and must require authorization and authentication to view, change or delete.

Examples: Student grades, social security numbers, passwords, credit card numbers, bank account numbers, security plans and assessments