Glossary of HIPAA Terms

Administrative Safeguards – Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of a covered entity's or business associate's workforce in relation to the protection of that information.

Authentication – Verification that a person is the one claimed.

Availability – Data or information is accessible and useable upon demand by an authorized person.

Breach- The acquisition, use, or disclosure of protected health information in a manner not permitted under the HIPAA privacy rules which compromises the security or privacy of the protected health information. Breach excludes:

- Any unintentional acquisition, access or use of protected health information by a workforce member or person acting under authority of a covered entity or a business associate, if such acquisition, access, use 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 the HIPAA privacy rules.
- 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 by the HIPAA privacy rules.
- 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 the information.

Business Associate – Generally, an entity or person who performs a function involving the use or disclosure of protected health information 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 protected health information (such as legal, actuarial, accounting, accreditation).

Confidentiality – Data or information is not made available or disclosed to unauthorized persons or processes.

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 HIPAA.

Data Integrity – Data or information have not been altered or destroyed in an unauthorized manner.

Data Use Agreement – An agreement between a covered entity (the holder of the protected health information) and the recipient of the protected health information (such as a research

investigator) in which the recipient agrees to only use or disclose the protected health information provided by the covered entity for limited purposes.

De–identified data – Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Health information is considered de–identified (1) if stripped of all of the 18 direct identifiers defined under HIPAA, or (2) if an expert in statistical and scientific method determines that there is a very small risk that the information could be used alone or in combination with other information to identify an individual.

Designated Record Set – Medical, clinical research and billing records about an individual maintained by or for a covered entity or used to make decisions about the individual and the individual's treatment. Information contained in a designated record set is subject to an individual's right to request access and amendment.

Disclosure – The release, transfer, provision of access to, or divulging in any manner of protected health information outside of the entity holding the information.

Electronic Media – Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; transmission media used to exchange information already in electronic storage media. Examples of transmission media include the Internet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic Protected Heath Information (ePHI) is protected health information in electronic form.

Encryption - 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.

Genetic Information – Information about (1) an 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, or (4) any request for or receipt of genetic services including participation in clinical research which includes genetic services by the individual or their family member. Genetic information includes the genetic information of a pregnant women'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.

Group Health Plan – An employee welfare benefit plan (as defined in the Employee Retirement Income and Security Act of 1974 (ERISA)), including insured and self–insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that has 50 or more participants; or is administered by an entity other than the employer that established and maintains the plan.

Health Care – Care, services, or supplies related to the health of an individual, including (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 an individual 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 – Entity that performs either of the following functions (1) processes or facilitates 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; or (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 Operations – Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities include: (1) Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; (2) reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) underwriting and other activities relating 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 health care claims; conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; (4) business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and (5) business management and general administrative activities.

Health Care Provider – A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Plan – An individual or group plan as defined in HIPAA that provides, or pays the cost of, medical care.

HIPAA – Health Insurance Portability and Accountability Act of 1996.

Individual – The person who is the subject of protected health information.

Individually Identifiable Health Information – Subset of health information, including demographic information collected from an individual, (1) that is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) that 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 payment for the provision of health care to an individual; and (3) that identifies the individual, or might reasonably be used to identify the individual.

Institutional Review Board (IRB) – A committee whose primary responsibility is to protect the rights and welfare of human research subjects. An IRB reviews research proposals to ensure risks have been minimized and the potential for benefit has been maximized before human subjects participate in the research.

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.

Limited Data Set – Protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) names; (2) postal address information, other than town or city, state, and zip code; (3) telephone numbers; (4) fax numbers; (5) email addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license numbers; (11) vehicle identifiers and serial numbers, including license plate numbers; (12) device identifiers and serial numbers; (13) web Universal Resource Locators (URLs); (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

Malicious Software – Software, such as a virus, designed to damage or disrupt a system.

Marketing – To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

Minimum Necessary –Limiting the use, disclosure, or requests for protected health information to the minimum necessary to accomplish the intended purpose.

OCR – Office of Civil Rights, the branch of the Department of Health and Human Services that is responsible for federal oversight of the privacy regulations.

Password – Confidential authentication information composed of a string of characters.

Payment – Activities undertaken by (1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan, except as prohibited when involving the use and disclosure of genetic information for underwriting purposes; or (2) a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Personal Representative – Someone with the legal authority to act on behalf of an incompetent adult patient, a minor patient or a deceased patient or the patient's estate in making health care decisions or in exercising the patient's rights related to the individual's protected health information.

Physical safeguards - Physical measures, 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 unauthorized intrusion.

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

Protected Heath Information (PHI) – Any individually identifiable health information (1) transmitted by electronic media; (2) maintained in electronic media; or (3) transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information in education records covered by the Family Educational Right and

Privacy Act (FERPA) and employment records held by a covered entity in its role as employer. Protected health information also excludes information related to individuals who have 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 – Any systematic investigation (including research development, testing, and evaluation) that is designed to contribute to generalizable knowledge.

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

Technical safeguards - The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Treatment – Provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Unsecured Protected Health Information – Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services.

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

Workforce – 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 the covered entity.

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.