DEFINITIONS

The following are terms commonly used within the Federal HIPAA Privacy and Security rules.

Familiarity with these terms will assist in your overall understanding of the Privacy rule and Business Associate requirements.

Access - means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative Safeguards - this term is used to define the administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect information.

American Recovery & Reinvestment Act of 2009 - ARRA, commonly referred to as the Stimulus or The Recovery Act is an economic stimulus package enacted by the 111th U S Congress in February 2009. The act included specific healthcare incentives.

Authentication - process used to verify the identity of a person whose protected health information is being requested, and the authority of the requester to access that person's protected health information.

Authorization - document that gives Covered Entities the permission to use or disclose Protected Health Information for specific purposes, typically for reasons other than treatment, payment or health care operations.

Breach - the unintentional or unauthorized release of Protected Health Information.

Business Associate - a person or organization that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of a Covered Entity.

Business Associate Agreement - an agreement mandated by the Privacy rule between a Covered Entity and a business associate providing services involving Protected Health Information.

Complaint - any concern or expression of dissatisfaction regarding privacy issues of protected information.

Confidentiality - means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Confidentiality Agreement (Non-disclosure Agreement) - executed contract which requires a third party to safeguard protected health information.

Covered Entity - as defined by federal Privacy regulation:

. Health Care clearing houses – public or private organizations that process or facilitate the processing of data elements of health information received from other covered entities, including billing services.

. Health Plans – individual or group plans that provide, or pay the cost of, medical care,including group health plans, HMOs, etc.

. Health Care Providers – physicians or other health care providers, licensed, accredited, or certified to perform specific health care services.

De-identification - is the process of removing key identifiers from an individual's protected health information so that the remaining information no longer identifies the individual, and the information cannot be re-identified to the individual.

Disclosure - is the act of releasing, transferring, divulging, or providing access to protected health information to an organization other than the Covered Entity maintaining the information.

Electronic Health Record - EHR is the systematic collection of electronic health information about individual patients.

Encryption - means 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 Information - as defined in Gramm-Leach-Bliley regulations, term pertains to elements such as bank account numbers, routing numbers and loan numbers.

Gramm-Leach-Bliley Act (GLBA) - federal law passed in 1999 that includes provisions to protect consumer's personal financial information and governs the collection and disclosure of their financial information.

Health Insurance Portability and Accountability Act (HIPAA) Title II - Administrative Simplification – federal law containing administrative provisions for health plans, providers, and health care clearinghouses. The privacy portion of

the law, designed to ensure the privacy of protected health information became effective April 14, 2003.
HITECH Act - part of ARRA. ARRA contains specific healthcare incentives including information on enforcement of privacy and security, breach notification requirements, electronic health record access and additional impacts to Business Associate agreements.
Incidental Disclosure - secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use and disclosure.
Individual - Individual means the person who is the subject of Protected Health Information.
Individually-Identifiable Health Information - any information that may identify an individual and relates to the past, present, or future mental or physical condition of the individual. For example, a name, address, telephone number, birth date, or Social Security number in combination with a diagnosis or other health-related information.
Individual Privacy Rights - according to HIPAA Title II regulations, individuals are entitled to individual privacy rights that include the following items:
. Right to Notice of Privacy Practices
. Right to Restrictions on Use and Disclosure of Protected Health Information
. Right to Alternate Communications
. Right of Access to Protected Health Information
. Right to Amend Protected Health Information
. Right to an Accounting of Disclosures of Protected Health Information
. Right to file a privacy complaint
Information system - means 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.
Integrity - means the property that data or information have not been altered or destroyed in an unauthorized manner.
Malicious software - means software, for example, a virus, designed to damage or disrupts a system.
Minimum Necessary Standard - is the practice of limiting the amount of information to the minimum amount of Protected Health Information necessary to accomplish the intended purpose of the Use or Disclosure.
Nonpublic Personal Information - “personally identifiable information” is information about a consumer which is provided by the individual in order to obtain a product or service.
Non-Routine Disclosure - disclosure of protected health information is a disclosure that does not ordinarily happen in routine operations or on a recurring basis.
Notice of Privacy Practices - a document required by the HIPAA Privacy rule that health care providers and health plan operations must provide individuals to inform the individual of their privacy rights and explains how their organization uses & discloses their Protected Health
Information. Password - means confidential authentication information composed of a string of characters.
Privacy Officer- the person designated to develop, implement, and oversee the entity’s compliance with the HIPAA Privacy Rule.
Physical safeguards - are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
Protected Health Information (PHI) - as defined by federal privacy regulation is information that:
. Contains data elements or combinations of data elements that could identify a person, or provides a reasonable basis to believe someone could be identified;
. Contains health-related information about that person; and
. Is maintained or transmitted in any form (electronic, written, or oral).
Routine Disclosures - is a disclosure of protected health information that

ordinarily happens in payment and health plan operations, or on a recurring basis.
Safeguards - processes and procedures to provide protection of PHI using administrative, physical and technical methods.
Sanction - penalty for non-compliance.
Security or Security measures - encompass all of the administrative, physical, and technical safeguards in an information system.
Security Incident - means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Technical Safeguards - security controls, safeguards and counter measures applied to an information system.
TPO - term that stands for treatment, payment and health care/plan operations.
Transaction - means the transmission of information between two parties to carry out financial or administrative activities related to health care.
Treatment - means the provision, coordination, or management of health care or health care related services by one or more health care providers.
US Department of Health and Human Services - The Department of HHS responsible for the enforcement and administration of the HIPAA law.
Use - is the sharing, Use, examining, or analysis of Protected Health Information within a Covered Entity that maintains that information.
User - means a person or entity with authorized access.
Workforce - term for employees, volunteers, trainees, and other persons who perform work for a Covered Entity.
Workstation - means an electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.