GLOSSARY OF TERMS

HIPAA - *Health Insurance Portability and Accountability Act. A set of rules to be followed by doctors, hospitals and other health care providers that help to ensure all medical records, medical billing, and patient accounts meet certain consistent standards with regard to documentation, handling and privacy.*

Protected Health Information (PHI*) – data that allows the identification of a patient and therefore must be treated as confidential*

Least Privilege Principle – *The principle of allowing an entity the least amount of entitlements necessary to perform its intended function.*

Need to Know Principle – *The information access control principle where users' access is limited to what is necessary to accomplish their jobs*

PHI is any **health information** that is **individually identifiable.** ***Health information:*** *includes any information about an individual's physical or mental health (including just the fact that an individual is a patient or receiving medical care).* ***Individually Identifiable****: Under HIPAA, the inclusion of any of the following elements would make health information identifiable: (1) name; (2) all geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, (3) all dates related to the individual, including birth date, admission date, discharge date, death date, and all ages over 89; (4) telephone number; (5) email address; (6) Mayo Clinic number or any other account number or unique identification number; (7) Social Security Number.*

Computer System Security – *the protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure; NOTE: Security also pertains to personnel, data, communication, and the physical protection of computer installations (IEEE 610.12-1990).*

Authorization: *Approval, permission, or empowerment for someone or something to perform a task.*

Authentication: *The process of proving a person or entity is, in fact, who or what it is claimed to be.*

Access: *The ability and opportunity to gain knowledge of information*

Authentication factors: *Elements employed to verify identity. These include one or more of the following:*

- *Something you know – a password, passphrase, personal identification number (PIN) or secret answer to a question*
- *Something you have – a token, smart card or personal device*
- *Something you are – biometric traits such as fingerprints, palm prints, retina patterns or iris patterns*

Identity: *The set of characteristics recognized as belonging uniquely to an entity.*

Password: *A string of characters used to authenticate an identity.*

Identification: *The process of presenting individual credentials, usually a unique alphanumeric string.*

Soft token: *A computer application that resides on a portable electronic device that periodically generates a one-time authentication code.*

System: *Generally describes an information system but can also represent any hardware, software or data store on which access controls are enabled.*

Identity and Access Management: *The security discipline that enable the right individuals to access the right resources at the right times for the right reasons.*

User/Account Provisioning: *creates, modifies, disables and/or deletes user accounts across IT infrastructure and applications.* [Gartner®]