HIPPA-HITECH Privacy, Security and Data Breach Notification Glossary

1. **Access** - The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any information system resource.
2. **Access Authorization -** Information-use policies/procedures that establish the rules for granting and/or restricting access to a user, terminal, transaction, program, or process.
3. **Access Control -** A method of restricting access to resources, allowing only privileged entities access. (PGP, Inc.) Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.
4. **Access Level** - A level associated with an individual who may be accessing information (for example, a clearance level) or with the information which may be accessed (for example, a classification level).
5. **Access Modification** - The security policies, and the rules established therein, that determine types of, and reasons for, modification to an entity's established right of access to a terminal, transaction, program, or process.
6. **Accountability -** The property that ensures that the actions of an entity can be traced uniquely to that entity.
7. **Adequate Security** - Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
8. **Administrative Safeguards -** Administrative actions, 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 the covered entity or business associate's workforce in relation to the protection of that information.
9. **Administrative Simplification -** The provisions of HIPAA relating to standards for electronic health care transactions, the privacy and security of health information, and national identifiers.
10. **Advanced Persistent Threat -** An adversary with sophisticated levels of expertise and significant resources, allowing it to use multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of inter action needed to execute its objectives.

11. **Amendment -** The right of an individual to request that a covered entity amend protected health information to correct errors or add omissions.
12. **Analysis Approach** - The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.
13. **ANSI** - The American National Standards Institute, a standard-setting organization
14. **Anti-virus Software** - Software that detects and attempts to prevent installation of malicious software.
15. **Applications and data criticality analysis -** An entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits.
16. **ASC X12 -** The Accredited Standards Committee X12, an organization chartered by the American National Standards Institute (ANSI) to develop uniform standards for inter-industry electronic interchange of business transactions.
17. **ASC X12N Standards:** Standards developed by ASC X12 for the insurance industry. The ASC X12N standards are the official standards for health care institutional, professional and dental transactions.
18. **Assessment** - See Security Control Assessment or Risk Assessment.
19. **Assessment Approach** - The approach used to assess risk and its contributing factors, including quantitatively, qualitatively, or semi-quantitatively.
20. **Assessor** - See Security Control Assessor or Risk Assessor.
21. **Assigned security responsibility -** Practices put in place by management to manage and supervise (1) the execution and use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
22. **Assigned privacy responsibility -** Practices put in place by management to manage and supervise (1) the execution and use of privacy measures to protect data, (2) monitor complaints and (2) the conduct of personnel in relation to the protection of data.
23. **Assurance** - Measure of confidence that the security features, practices, procedures, and architecture of an information [CNSSI 4009] system accurately mediates and enforces the security policy. [NIST SP 800-53] Grounds for confidence that the set of intended security controls in an information system are effective in their application.
24. **Assurance Case** [Software Engineering Institute, Carnegie Mellon University] - A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
25. **Availability** - The property that data or information is accessible and useable upon demand by an authorized person. [44 U.S.C., Sec. 3542] - Ensuring timely and reliable access to and use of information.
26. **Audit controls** - The mechanisms employed to record and examine system activity.
27. **Authentication** - The corroboration that a person or entity is the one claimed. [FIPS 200] - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
28. **Authenticity** - The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
29. **Authorization control -** The mechanism for obtaining consent for the use and disclosure of health information.

30. **Authorization (HIPAA) -** Written permission from an individual allowing the use or disclosure of his or her health information. The written permission must contain certain required elements and statements.
31. **Authorization (Information System)** The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
32. **Authorize** - To grant authority or permission to.
33. **Authorization Boundary** [NIST SP 800-37] - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
34. **Backup** - Creating a retrievable, exact copy of data stored in an information system.
35. **Biometric identification system** - A system in which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.
36. **Breach** - 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.
37. **Breach Exclusions –** Breaches do not include:

    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 the Privacy Rule.
    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 the Privacy Rule.
    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.
38. **Breach Presumption -** Except as provided in the definition of breach exclusions, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule 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

39. **Business associate (BA)** – (1) Except as provided in paragraph (4) of this definition, with respect to a covered entity, a person who:

a. On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, 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, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), 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:

(i) 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.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) 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) of this subchapter apply and are met.

(iii) 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.

40. **Business Associate Agreement** - An agreement between a covered entity and its business associate in which the business associate agrees to restrict its use and disclosure of the covered entity's protected health information.

41. **Business Associate Contract:** The contract between a covered entity and a business associate providing that the business associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity.

42. **Chain of Trust Partner Agreement -** Contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where the data transmitted is agreed to be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originator to the ultimate recipient, for example, a provider may contract with a clearing house to transmit claims to the clearing house; the clearing house, in turn, may contract with another clearing house or with a payer for the further transmittal of those same claims.
43. **Checksum** - A count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received. This number can be regularly verified to ensure that the data has not been improperly altered.
44. **Chief Information Officer** [PL 104-106, Sec. 5125(b)] - Agency official responsible for:
    a. Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;
    b. Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and
    c. Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
45. **Chief Information Security Officer -** See Senior Agency Information Security Officer.
46. **Civil Money Penalty (CMP)** – Monetary penalty imposed by HHS/OCR following findings of violation of the HIPAA-HITECH rules. Prior to the HITECH Act, CMPs were limited to $100 per violation, per day, to a maximum of $25,000 per year. The HITECH Act created four levels of penalty, based on level of culpability, and increased the maximum penalty to $1.5 Million per year, per violation.
47. **Classified National Security Information** [CNSSI 4009] - Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
48. **CMS** - The Centers for Medicare and Medicaid Services, a department within the U.S. Department of Health and Human Services (formerly called the Health Care Financing Administration). Previously charged with overseeing the Security Rule; that oversight was shifted by the HITECH Act to the HHS Office for Civil Rights. *See also: OCR.*
49. **Code of Federal Regulations (CFR)** - The codification of the general and permanent rules and regulations (sometimes called administrative law) published in the *Federal Register* by the executive departments and agencies of the Federal Government of the United States. See also *promulgate.*
50. **Code Set -** The code(s) adopted by rules issued under HIPAA for use in EDI Transactions. (See also *Electronic Data Interchange, Transaction, CDT-4, CPT-4, HCPCS, ICD-9-CM, NDC, HCPCS)*
51. **Combination locks changed** - Documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or a requirement for access to the protected facility/system.

52. **Committee on National Security Systems Instruction No. 4009 (CNSSI 4009)** Information Assurance Glossary - The Committee on National Security Systems (CNSS) Glossary Working Group convened to review and update the National Information Assurance Glossary, CNSSI 4009, dated June 2006. This revision of CNSSI 4009 incorporates many new terms submitted by the CNSS Membership. Most of the terms from the 2006 version of the Glossary remain, but a number of them have updated definitions in order to remove inconsistencies among the communities.
53. **Common Control** [NIST SP 800-37] - A security control that is inherited by one or more organizational information systems. See also *Security Control Inheritance*.
54. **Common Control Provider** [NIST SP 800-37] - An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).
55. **Compensating Security Control [CNSSI 4009]** - A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
56. **Confidentiality** - The property that data or information is not made available or disclosed to unauthorized persons or processes. [44 U.S.C., Sec. 3542] - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
57. **Consent** – Agreement given to a covered entity to use protected health information for treatment, payment, and health care operations. Under the HIPAA final rules on privacy obtaining consent is optional.
58. **Contingency Plan -** A plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. Contingency plans should be updated routinely.
59. **Contrary -** Within the context of HIPAA, when a Covered Entity would find it impossible to comply with both the State and Federal requirements, and/or the provisions of a State law stand as an obstacle to the accomplishment or execution of the full purposes and objectives of HIPAA Administrative Simplification.
60. **Course of Action (Risk Response)** - A time-phased or situation-dependent combination of risk response measures.
61. **Covered entity (CE)** – A health care provider that electronically transmits health information for any of the standardized transactions, a health plan, or a health care clearinghouse.
62. **CPT-4 -** Current Procedural Terminology, Fourth edition; the code-set adopted by HIPAA for physician services, physical and occupational therapy services, radiological procedures, clinical laboratory tests, other medical diagnostic procedures, hearing and vision services, and transportation services.
63. **Cryptographic key** – A variable value that is applied using an algorithm to data to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the data.
64. **Cryptography** - Encrypting ordinary text into undecipherable text (cipher text) then decrypting the text back into ordinary text (clear text).

65. Cyber Attack [CNSSI 4009] - An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
66. Cyber Security [CNSSI 4009] - The ability to protect or defend the use of cyberspace from cyber-attacks.
67. Cyberspace [CNSSI 4009] - A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
68. Data - a sequence of symbols to which meaning may be assigned.
69. Data Aggregation - The combining of such protected health information by a business associate on behalf of more covered entities than one, to permit data analysis relating to the health care operations of the participating covered entities.
70. Data authentication - The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.
71. Data backup – The process of creating a retrievable, exact copy of protected health information.
72. Data backup plan - A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.
73. Data custodian - Refers to those who conduct data processing services for the organization's software applications, data, networks, operating systems, etc. Data custodians perform these services on behalf of data stewards.
74. Data Integrity - The property that data has not been altered or destroyed in an unauthorized manner.
75. Data steward - Refers to individuals with ultimate responsibility for the creation of the data used or stored in organizational information (computer) systems. That is, the System Owners. This individual has overall and final responsibility for the information system.
76. Data Use Agreement - A confidentiality agreement between a covered entity and the recipient of health information in a limited data set.
77. Data user - Any individual who accesses data used or stored in organizational computer systems.
78. Decryption - Refers to the process of converting encrypted data back into its original form, so it can be understood. See also *Encryption*.
79. Defense-in-Breadth [CNSSI 4009] - A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
80. Defense-in-Depth [CNSSI 4009] - Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
81. De-identified Health Information - Health information from which individual identifiers have been removed, so that it cannot be used to identify an individual. De-identified health information is not protected by HIPAA.
82. Department of Health and Human Services (DHHS or sometimes, simply HHS) – A U.S. Federal agency that is responsible for administering programs that deal with health and welfare.

83. Department of Justice (DOJ) - Within the context of HIPAA, the U.S. Federal agency that is responsible for enforcement of criminal violations of HIPAA.
84. Designated Record Set - A health care provider's medical records and billing records about individuals, a health plan's enrollment, payment, claims adjudication, and case or medical management records, and any other records used by a covered entity to make decisions about individuals.
85. Designated Standards Maintenance Organization (DSMO) - An organization designated by DHHS to act as the maintenance organization for standard(s) adopted as part of HIPAA.
86. Digital signature - A cryptographic code that is attached to a piece of data. This code can be regularly verified to ensure that the data has not been improperly altered.
87. Direct Treatment Relationship - The relationship between an individual and a provider who provides health care directly to the individual. Providers who have a direct treatment relationship must furnish their notice of privacy practices to the individual when services are first delivered, and must make a good faith effort obtain a written acknowledgment of receipt of the notice.
88. Disaster - An event that causes harm or damage to information systems. Disasters include but are not limited to: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.
89. Disaster recovery - The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
90. Disaster recovery plan - Part of an overall contingency plan. The plan for a process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
91. Disclosure - The release, transfer, provision of, access to, or divulging in any other manner of protected health information outside the covered entity holding the information.
92. Discovery of a Breach - A breach will be considered to be "discovered" as of the first day on which the breach is known to an entity or should have been known to the entity if the entity had exercised reasonable due diligence. The due diligence requirement means that Covered Entities and Business Associates should have policies and procedures in place to detect and identify breaches, which requires coordination among the individuals and departments that are responsible for the physical, administrative and technical aspects of the entity's compliance with the HIPAA Privacy and Security Rules.
93. Disposal - The final disposition of electronic data, and/or the hardware on which electronic data is stored.
94. Documentation - Written security plans, rules, policies, procedures, and instructions concerning all components of an entity's security.
95. EIN - The employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury.
96. Electronic communications network - any series of nodes (electronic devices on the network) interconnected by communication paths which facilitate the transmission of data (e.g., the Internet). Such networks may interconnect with other networks or contain sub networks.
97. Electronic data interchange (EDI) - Intercompany, computer-to-computer transmission of business information in a standard format. For EDI purists, "computer-to-computer" means direct transmission from the originating application program to the receiving, or processing, application program, and an

EDI transmission consists only of business data, not any accompanying verbiage or free-form messages. Purists might also contend that a standard format is one that is approved by a national or international standards organization, as opposed to formats developed by industry groups or companies.

98. **Electronic media** – 1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or 2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), 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, because the information being exchanged did not exist in electronic form before the transmission.
99. **Electronic protected health information** (ePHI) – Protected Health Information that is transmitted by electronic media or maintained in electronic media. See also *Protected Health Information (PHI).*
100. **Electronic signature** - The attribute that is affixed to an electronic document to bind it to a particular entity. An electronic signature process secures the user authentication (proof of claimed identity, such as by biometrics (fingerprints, retinal scans, hand written signature verification, etc.), tokens or passwords) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven) and supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer. There are several technologies available for user authentication, including passwords, cryptography, and biometrics.
101. **Email** - The common term for "electronic mail", a method for writing, sending and receiving electronic text (and audio and/or video) over a computer network. A variation of email popular with mobile telephone users is the Short Messaging Service (SMS). Email differs to other messaging systems in that it is asynchronous in nature.
102. **Emergency** – A crisis situation.
103. **Employee Welfare Benefit Plan** - A plan, fund or program maintained by an employer or an employee organization that provides medical, surgical or hospital care.
104. **Encryption** - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key. In other words, encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized individuals.
105. **Enterprise [CNSSI 4009]** - An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See Organization.

106. **Enterprise Architecture [CNSSI 4009]** - The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.
107. **Environment of Operation [NIST SP 800-37]** - The physical surroundings in which an information system processes, stores, and transmits information.
108. **Erase tool** - Hardware or software that is capable of completely removing all recorded material from electronic media.
109. **ERISA -** The Employee Retirement Income and Security Act of 1975. Most group health plans covered by ERISA are also health plans under HIPAA.
110. **Executive Agency [41 U.S.C., Sec. 403]** - An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
111. **Facility** - The physical premises and the interior and exterior of a building(s).
112. **Facility security plan** - A plan to safeguard the premises and building(s) (exterior and interior) from unauthorized physical access, and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.
113. **Family member** means, with respect to an individual:
    a. A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
    b. 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).
    (i) First-degree relatives include parents, spouses, siblings, and children.
    (ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
    (iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
    (iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.
114. **Fault Tree Analysis** - A top-down, deductive failure analysis in which an undesired state of a system (top event) is analyzed using Boolean logic to combine a series of lower-level events. An analytical approach whereby an undesired state of a system is specified and the system is then analyzed in the context of its environment of operation to find all realistic ways in which the undesired event (top event) can occur.
115. **Federal Agency** - See Executive Agency.
116. **Federal Information System [40 U.S.C., Sec. 11331]** - An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
117. **FERPA -** The Family Educational Rights and Privacy Act.

118. Fundraising - The use of protected health information by a covered entity (or its related foundation or a business associate) to raise funds for the covered entity.

119. Genetic information:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) 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:

(i) A fetus carried by the individual or family member who is a pregnant woman;

and

(ii) 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.

120. Genetic services - A genetic test; Genetic counseling (including obtaining, interpreting, or assessing genetic information); or Genetic education.

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

122. Group Health Plan - An employee welfare benefit plan (as defined in ERISA) that provides health benefits. A group health plan is a health plan under HIPAA unless it has fewer than 50 participants, and it is administered by the sponsoring employer.

123. Harm Standard - The "harm standard" is a superseded standard that allowed for Covered Entities to determine if a breach of patient information presents a significant risk of harm to the individual(s). See also *Low Probability of Compromise Standard*.

124. Hash (or hash value) - A number generated from a string of text. A sender of data generates a hash of the message, encrypts it, and sends it with the message itself. The recipient of the data then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they are the same, there is a very high probability that the message was transmitted and received intact.

125. Health care – Care, services, or supplies related to the health of a patient. It includes, but is not limited to (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.

126. Health care clearinghouse – A public or private entity that either: (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; 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.

127. **Health Care Component -** A component of a hybrid entity that includes covered functions the entity (and, optionally, related business associate functions), and that the entity designates as a health care component.
128. **Health Care Financing Administration Common Procedure Coding System (HCPCS) -** System. Level I – the CPT-4. Level II – codes for products, supplies, and services not included in CPT-4. Level III – Local codes defined and used by state agencies. (See Code Set.).
129. **Health Care Operations -** Business management and operations, including quality assessment and improvement, peer review, underwriting, medical review an audits, and business planning, management and development.
130. **Health Care Provider -** A person or organization who furnishes, bills, or is paid for health care in the normal course of business.
131. **Health Information -** Any 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 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. *See also: Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI).*
132. **Health Information Technology for Economic and Clinical Health (HITECH) Act** - Enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
133. **Health Insurance Issuer -** A company that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance.
134. **Health Level Seven (HL7) -** An ANSI accredited Standards Developing Organization specializing in the health care arena.
135. **Health Maintenance Organization (HMO)** - A federally qualified HMO, or an organization regulated by State law as a health maintenance organization.
136. **Health Oversight Agency -** A governmental agency 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.
137. **Health Plan -** An organization that provides, or pays the cost of, medical care. Employee health benefit plans are health plans, unless they are self-administered, and have fewer than 50 participants. Government-funded programs whose principal function is providing direct health care services are not health plans.
138. **HFCA -** The Health Care Financing Administration of the Department of Health and Human Services; renamed the Centers for Medicare and Medicaid Services (CMS).
139. **HHS -** The U.S. Department of Health and Human Services.

140. **Hybrid Entity -** A single entity that has both covered (health plan, health care provider or health care clearinghouse) functions, and non-covered functions. A county that provides health services and non-health services is an example.
141. **Hybrid Security Control [NIST SP 800-53]** - A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See Common Control and System-Specific Security Control.
142. **ICD-9 -** (International Classification of Diseases, Ninth Revision): ICD-9 was the official system of assigning codes to diagnoses and a wide variety of signs, symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or disease. It is published by the World Health Organization (WHO) and used worldwide for morbidity and mortality statistics, reimbursement systems, and automated decision support in medicine. The ninth revision was published in 1977.
143. **ICD-9-CM -** (International Classification of Diseases, Ninth Revision, Clinical Modification): is an adaptation of ICD-9 created by the U.S. National Center for Health Statistics (NCHS) and used in assigning diagnostic and procedure codes associated with inpatient, outpatient, and physician office utilization in the United States. The ICD-9-CM is based on the ICD-9 but provides for additional morbidity detail. It is updated annually on October 1. The NCHS and the Centers for Medicare and Medicaid Services (CMS) are the U.S. governmental agencies responsible for overseeing all changes and modifications to the ICD-9-CM.
144. **ICD-10 -** (International Classification of Diseases, Tenth Revision): Work on ICD-10 began in 1983, and the new revision was endorsed by the Forty-third World Health Assembly in May 1990. The latest version came into use in WHO Member States starting in 1994. The ICD-10 classification system allows more than 155,000 different codes and permits tracking of many new diagnoses and procedures, a significant expansion on the 17,000 codes available in ICD-9.
145. **ICD-10-CM -** (International Classification of Diseases, Tenth Revision, Clinical Modification): Adoption of ICD-10 has been slow in the United States. Beginning in 1988, CMS required ICD-9-CM codes for Medicare and Medicaid claims, and most of the rest of the U.S. health care industry followed suit. On 1 January 1999 the ICD-10 (without clinical extensions) was adopted for reporting mortality, but ICD-9-CM was still used for morbidity. Meanwhile, NCHS received permission from the WHO to create a clinical modification of the ICD-10, and has production of all these systems:
    a. ICD-10-CM, for diagnosis codes, and
    b. ICD-10-PCS, for procedure codes.
    Note: On August 21, 2008, HHS proposed new code sets to be used for reporting diagnoses and procedures on health care transactions. Under the proposal, the ICD-9-CM code sets must be replaced with the ICD-10-CM code sets.
146. **Implementation Specification -** In the context of HIPAA privacy and security regulations, these specify how a standard is to be met. For the Security Rule, Implementation Specifications may be classified as "required" meaning a CE *must* implement the specification, or "addressable" meaning a CE *may* implement the specification, or an alternative measure. The CE must document, or document reasoning, for not implementing the addressable specification or an alternative.
147. **Indirect Treatment Relationship -** The relationship between and individual and a provider who typically provides services on the orders of another provider, and reports the results to the requesting provider. A radiologist and a clinical laboratory typically have an indirect treatment relationship. Providers having

an indirect treatment relationship are not required to furnish their notice of privacy practices to individuals routinely, although they must make it available and furnish it on request.

148. Individually Identifiable Health Information - Information that relates to an individual's physical or mental health; the provision of health care to an individual; or the payment for health care provided to an individual, ***and*** that identifies the individual or could be used to identify the individual. See also: *Health Information* and *Protected Health Information*.
149. Industrial Control System - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
150. Information [CNSSI 4009] - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
151. Information Owner [CNSSI 4009] - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See Information Steward.
152. Information Resources [44 U.S.C., Sec. 3502] - Information and related resources, such as personnel, equipment, funds, and information technology.
153. Information Security [44 U.S.C., Sec. 3542] - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
154. Information Security Architecture - A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
155. Information Security Program Plan [NIST SP 800-53] - Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
156. Information Steward [CNSSI 4009] - An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
157. 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. [44 U.S.C., Sec. 3502] - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
158. Information System Boundary - See Authorization Boundary.
159. Information system owner – see Data Steward.
160. Information System Owner (or Program Manager) - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

161. Information System Resilience - The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack.
162. Information System Security Officer - Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
163. Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
164. Information System-Related Security Risks - Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See Risk.
165. Information Technology [40 U.S.C., Sec. 1401] - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:
    a. Requires the use of such equipment; or
    b. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
166. Information Type [FIPS 199] - A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
167. Institutional Review Board (IRB) - A board established by a research institution to review and approve protocols for research on human subjects. Under HIPAA, an IRB may waive the requirement for individual authorization for the use of health information for research.
168. Integrity - The property that data or information have not been altered or destroyed in an unauthorized manner. [44 U.S.C., Sec. 3542] - Guarding against improper information modification or destruction, and includes ensuring information non- repudiation and authenticity.
169. Integrity controls - Security mechanism employed to ensure the validity of the information being electronically transmitted or stored.
170. Inventory - Formal, documented identification of hardware and software assets.
171. Keylogger - A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via email).
172. KPMG – Is one of the largest professional services firms in the world; known as one of the "Big Four" audit firms. In July of 2011, HHS awarded KPMG a $9 million contract to help the Office of Civil Rights create an audit program to verify that healthcare providers, health plans and their business associates

adhere to the HIPAA privacy and security rules and also to visit and audit up to 150 of these covered organizations by the end of 2012 ensure they consistently put their privacy and security policies into practice.

173. Law Enforcement Official - An officer or employee of any governmental agency who is empowered by law to investigate or prosecute violations of law.
174. Limited Data Set - Health information from which specified identifiers have been removed. Information in a limited data set is protected, but may be used for research, health care operations and public health activities without the individual's authorization.
175. Low Probability of Compromise Standard – Standard required by the Omnibus Final Rule to determine breach reporting responsibilities. All breaches are presumed unless the organization can demonstrate that there is low probability of compromise based on completing a risk assessment of the breach event. See also *Breach Presumption*
176. Maintenance of record of access authorizations - Ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information.
177. Maintenance records - Documentation of repairs and modifications to the physical components of a facility, for example, hardware, software, walls, doors, locks. Part of physical access controls (limited access) on the matrix.
178. Malicious code - An executable application (e.g. Java applet or Active X control) designed to damage or disrupt an information system.
179. Malicious software - Software, such as a virus, designed to damage or disrupt an information system.
180. Management Controls [FIPS 200] - The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
181. Marketing - Except as provided in Marketing Exceptions (below) marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. 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.
182. Marketing Exceptions - 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: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; 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.

183. Media controls - Formal, documented policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.
184. Message authentication - Ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent.
185. Message authentication code – A one-way hash of a message that is then appended to the message. Used to verify that the message is not altered between the time the hash is appended and the time it is tested.
186. Minimum Necessary – The minimum amount of protected health information necessary to accomplish a permitted use or disclosure for payment or health care operations.
187. Mission/Business Segment - Elements of organizations describing mission areas, common/shared business services, and organization-wide services. Mission/business segments can be identified with one or more information systems which collectively support a mission/business process.
188. Mobile Device – Class of computing devices that includes smart phones, tablet computers and laptop computers.
189. National Council for Prescription Drug Programs (NCPDP) - An ANSI accredited standards development organization for the pharmacy services sector of the health care industry.
190. National Drug Code (NDC) - A system of universal product identifiers for human drugs. (See Code Set.).
191. National Employer Identifier - A unique identifier assigned to each and every employer. HIPAA has adopted the Internal Revenue Service's Employer Identification Number (EIN).
192. National Institute of Standards and Technology (NIST) - The federal, non-regulatory technology agency that works with industry to develop and apply technology, measurements, and standards. NIST published "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 Revision 1)" in October 2008 to assist covered entities in understanding and properly using the set of federal information security requirements adopted by the Secretary of HHS under HIPAA. See also *Security Rule*.
193. National Provider Identifier (NPI) - A unique (proposed to be 8 alphanumeric characters) identifier assigned by CMS to each and every health care provider.
194. National Security Information - See Classified National Security Information.
195. National Security System [44 U.S.C., Sec. 3542] - Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency

a. The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or

b. Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

196. National Uniform Billing Committee (NUBC) - Formed by the American Hospital Association in 1975 to develop billing forms and data sets.
197. National Uniform Claim Committee (NUCC) - Chaired by the American Medical Association and formed to develop standard data sets for claim and encounter transmittals.
198. Notice of Privacy Practices (NPP) - A notice that a covered entity is required to make available to patients or enrollees describing how the entity uses and disclosures of protected health information, and the individual's rights with respect to protected health information.
199. Notice of Proposed Rule Making (NPRM) - The process by which an agency of the Federal government, e.g. the Department of Health and Human Services, places proposed rules into the public record, e.g. by publishing them in the Federal Register. See also *Promulgate*
200. Office of Civil Rights (OCR) - The federal government agency responsible for enforcement of both the HIPAA Privacy and HIPAA Security rules.
201. Office of the Inspector General (OIG) - An office that is part of many Cabinet departments and independent agencies of the United States federal government as well as some state and local governments. Each office includes an Inspector General and employees charged with identifying, auditing, and investigating fraud, waste, abuse, and mismanagement within the parent agency. The *HHS OIG* is the largest inspector general's office in the Federal Government.
202. Operational Controls [FIPS 200] - The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
203. Organization [FIPS 200, Adapted] - An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). See Enterprise.
204. Organizational Requirements - The contractual relationships necessary to protect shared PHI.
205. Organized Health Care Arrangement (OHCA) - A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; An organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint utilization review, quality assurance or financial risk for health care services.
206. Password - Confidential authentication information composed of a string of characters.
207. Payment - The activities of a health care provider to obtain payment for health care services, or of a health plan to obtain premiums, or to adjudicate and pay claims.
208. Periodic security reminders – A requirement of the Security Rule; includes ongoing training and awareness to workforce members (employees, agents and contractors) on subjects such as malicious logic and password management.
209. Personnel clearance procedure - A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with

the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual.

210. **Personnel security** - The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.
211. **Personally Identifiable Information (PII) -** PII, in general, is any information that by itself or in combination with other information can be used to identify an individual including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PII include, but are not limited to:
    a. Name, such as full name, maiden name, mother's maiden name, or alias
    b. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
    c. Address information, such as street address or email address
    d. Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
    e. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).
212. **Physical safeguards** - Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.
213. **PIN (Personal Identification Number) -** A number or code assigned to an individual and used to provide verification of identity.
214. **Plan Sponsor -** The sponsor of an employee welfare benefit plan (typically an employer or union).
215. **Policies and Procedures and Documentation Requirements -** The creation and maintenance of formal written guidance to meet the requirements of HIPAA.
216. **Policy/guideline on workstation use -** Documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings, of a specific computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site.
217. **Plan of Action and Milestones (POAM) [OMB Memorandum 02-01]** - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
218. **Predisposing Condition** - A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation.
219. **Preemption -** Within the context of HIPAA, when a Federal regulation overrides a State regulation.
220. **Privacy Board –** A board that has members with varying backgrounds and professional qualifications to review the effect of a research protocol on individual health information privacy. Under HIPAA, a privacy

board may waive the requirement for individual authorization for the use of health information for research.

221. **Privacy Official -** The official appointed by a covered entity to be responsible for developing and implementing policies and procedures for complying with the health information privacy requirements of HIPAA.
222. **Privacy Rule** – The federal privacy regulations issued pursuant to HIPAA and codified at 45 C.F.R. parts 160 and 164. First published in December 2000, with periodic updates afterward.
223. **Promulgate** –The official declaration that a law or decree is in effect. The Federal Government promulgates new or revised laws and rules by publishing in the *Federal Register*.
224. **Protected health information (PHI)** – Individually Identifiable Health Information (IIHI) that is:
    a. Transmitted by electronic media;
    b. Maintained in electronic media; or
    c. Transmitted or maintained in any other form or medium
    Exclusion: It does not include certain education records, health information of students, or employment records held by a covered entity in its capacity as an employer. *See also: Health Information, and Individually Identifiable Health Information.*
225. **Provider –** A supplier of medical services as defined in HIPAA.
226. **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 patient's medical record. It excludes 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.
    Note: Psychotherapy notes are maintained separately from other records, and are not shared by the originating provider except in very limited circumstances.
227. **Public Health Activities** - The activities of public health authorities to collect information for the purpose of preventing or controlling disease, illness or injury.
228. **Public Health Authority** - Agencies or authorities of the United States, states, territories, political subdivisions of states or territories, American Indian tribes, or an individual or entity acting under a grant of authority from such agencies and responsible for public health matters as part of an official mandate.
229. **Public Interest Disclosures** - Disclosures for a variety of public interest-related purposes, which HIPAA permits without the individual's authorization.
230. **Qualitative Assessment** - Use of a set of methods, principles, or rules for assessing risk based on nonnumeric categories or levels.
231. **Quantitative Assessment** - Use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
232. **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.

233. Reasonable diligence - The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
234. Removal from access lists - The physical eradication of access privileges.
235. Removal of user account(s) - The termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists.
236. Repeatability - The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments.
237. Reproducibility - The ability of different experts to produce the same results from the same data.
238. Research - a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to general knowledge.
239. Restoration - The retrieval of files previously backed up and returning them to the condition they were at the time of backup.
240. Re-use - The use of electronic media containing EPHI for something other than its original purpose.
241. Risk - The likelihood that a specific threat will exploit a certain vulnerability, as well as the resulting impact of that event. [CNSSI 4009] - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
    a. The adverse impacts that would arise if the circumstance or event occurs; and
    b. The likelihood of occurrence.
    Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
242. Risk Assessment - The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis except when used in the conducting of a *Low Probability of Compromise for Breach Risk Assessment*.
243. Risk Assessment Methodology - A risk assessment process, together with a risk model, assessment approach, and analysis approach.
244. Risk Assessor - The individual, group, or organization responsible for conducting a risk assessment.
245. Risk analysis - A systematic and analytical approach that identifies and assesses risks to the confidentiality, integrity or availability of a covered entity's EPHI. Risk analysis considers all relevant losses that would be expected if specific security measures protecting EPHI are not in place. Relevant losses include losses caused by unauthorized use, disclosure of EPHI and loss of data integrity.
246. Risk Executive (Function) [CNSSI 4009] - An individual or group within an organization that helps to ensure a. That security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with

regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and

b. Managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

247. Risk Factor - A characteristic used in a risk model as an input to determining the level of risk in a risk assessment.
248. Risk management - Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. [CNSSI 4009, adapted] - The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes:
    a. Establishing the context for risk-related activities;
    b. Assessing risk;
    c. Responding to risk once determined; and
    d. Monitoring risk over time.
249. Risk Mitigation [CNSSI 4009] - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
250. Risk Model - A key component of a risk assessment methodology (in addition to assessment approach and analysis approach) that defines key terms and assessable risk factors.
251. Risk Monitoring - Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
252. Risk Response - Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
253. Risk Response Measure - A specific action taken to respond to an identified risk.
254. Role-based access control (RBAC) - An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
255. Root Cause Analysis - A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
256. Sanction policy - A policy that organizations must implement regarding disciplinary actions which are communicated to all employees, agents and contractors, for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment and contract penalties. In addition to enterprise sanctions, employees, agents, and contractors must be advised of civil or criminal penalties for misuse or misappropriation of health information. Employees, agents and contractors, must be made aware that violations may result in notification to law

enforcement officials and regulatory, accreditation and licensure organizations. Sanctions must be consistently applied within the workforce.

257. **Secretary** - The Secretary of Health and Human Services.
258. **Secure work station location** - Physical safeguards to eliminate or minimize the possibility of unauthorized access to information, for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area.
259. **"Secured" PHI** - PHI that is "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 in guidance." Secured PHI is not subject to the breach notification requirements of the HITECH Act.
260. **Security** - Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data.
261. **Security awareness training** - All employees, agents, and contractors must participate in information security awareness training programs. Based on job responsibilities, individuals may be required to attend customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security.
262. **Security Authorization (to Operate)** - See Authorization (to operate).
263. **Security Categorization** - The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
264. **Security configuration management** - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.
265. **Security Controls [FIPS 199, CNSSI 4009]** - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
266. **Security Control Assessment [CNSSI 4009, Adapted]** - The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
267. **Security Control Assessor** - The individual, group, or organization responsible for conducting a security control assessment.
268. **Security Control Baseline [CNSSI 4009]** - The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
269. **Security Control Enhancements** - Statements of security capability to:

a. Build in additional, but related, functionality to a basic control; and/or

b. Increase the strength of a basic control.

270. **Security Control Inheritance [CNSSI 4009]** - A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See also *Common Control*.
271. **Security Impact Analysis [NIST SP 800-37]** - The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
272. **Security incident** - The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
273. **Security incident procedures** - Formal, documented instructions for reporting security incidents.
274. **Security management process** – A process encompassing the creation, administration and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches. It involves risk analysis and risk management, including the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets, both physical and electronic.
275. **Security measures** - Security policies, procedures, standards and controls.
276. **Security Objective [FIPS 199]** - Confidentiality, integrity, or availability.
277. **Security Official** - The Security Rule requirement to designate one individual to be responsible for the development and implementation of policies and procedures that safeguard electronic protected health information.
278. **Security policy** - The framework within which an organization establishes needed levels of information security to achieve the desired information confidentiality, integrity and availability goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. The American Health Information Management Association recommends that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. [NIST SP 800-18] - Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See System Security Plan or Information Security Program Plan.
279. **Security Requirements [FIPS 200]** - Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
280. **Security Rule -** HIPAA required the Secretary to adopt, among other standards, security standards for certain health information. These standards were published on February 20, 2003. In the preamble to the Security Rule, several NIST publications were cited as potentially valuable resources for readers with specific questions and concerns about IT security. See also *NIST*.

281. **Security testing** - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes, but is not limited to, hands-on functional testing, penetration testing, and verification.
282. **Security token system** – A system in which a small hardware device along with a secret code (e.g. password or PIN) is used to authorize access to an information system.
283. **Semi-Quantitative Assessment** - Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts.
284. **Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]** - Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.]
285. **Senior Information Security Officer** - See Senior Agency Information Security Officer.
286. **Small Health Plan** - A health plan with annual receipts of $5 million or less. Small health plans had an extra year to comply with HIPAA.
287. **SPAM** - Unsolicited bulk email, normally sent for a commercial or fraudulent purpose. SPAM is an effective means of advertising as the costs of distribution of SPAM email is very low. With a very low success rate, "Spammers" can afford to send millions of emails to generate a few positive responses.
288. **Spyware -** Term for a class of software that monitors the actions of a computer user. This software falls into a number of categories: Software that may be installed legitimately to provide security or workplace monitoring, software with relatively benign purposes that may be associated with marketing data collection and software that is maliciously installed, either as a general violation of a user's privacy or to collect information to allow further attacks on their computer or online transactions. See also *Keylogger*.
289. **Subcontractor** - 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
290. **Subsystem** - A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
291. **Supplementation (Security Controls)** - The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.
292. **System** - See Information System.
293. **System Security Plan [NIST SP 800-18]** - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
294. **System-Specific Security Control [NIST SP 800-37]** - A security control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.
295. **Tailoring [NIST SP 800-53, CNSSI 4009]** - The process by which a security control baseline is modified based on:

a. The application of scoping guidance;

b. The specification of compensating security controls, if needed; and

c. The specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

296. Tailored Security Control Baseline - A set of security controls resulting from the application of tailoring guidance to the security control baseline. See also *Tailoring*.
297. Technical Controls [FIPS 200] - Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
298. Technical Safeguards - The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
299. Technical security mechanisms - The processes that are put in place to guard against unauthorized access to data that is processed or stored in a computer system or transmitted over a communications network.
300. Termination procedures - Formal, documented instructions, which include appropriate security measures, for removal of access to information systems at the end of an employee's employment, or for an internal/external user's access.
301. Testing and revision – (1) testing and revision of contingency plans refers to the documented process of periodic testing to discover weaknesses in such plans and the subsequent process of revising the documentation if necessary; and, (2) testing and revision of programs should be restricted to formally authorized personnel.
302. Threat – An agent (event or person) that can intentionally or accidentally exploit a vulnerability in an information system. [CNSSI 4009] - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
303. Threat Assessment [CNSSI 4009] - Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
304. Threat Event - An event or situation that has the potential for causing undesirable consequences or impact.
305. Threat Scenario - A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
306. Threat Shifting - Response from adversaries to perceived countermeasures or obstructions, in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome countermeasures or obstacles.
307. Threat Source [CNSSI 4009] - The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.
308. Token - A physical device, which used together with something that a user knows (for example a PIN or password), will enable authorized access to an information system.
309. Trading Partner Agreement - An agreement related to the exchange of information in electronic transactions. Trading partner agreements specify the communications protocols and transaction standards to be used.

310. **Training** - Education concerning the vulnerabilities of the health information in an organization's possession and ways to ensure the protection of that information.
311. **Transaction and Code Sets (TCS)** - The set of EDI transaction set and code sets standardized for use in health care by HIPAA. See also *Electronic Data Interchange, Transaction, and Code Set*.
312. **Transaction** - The transmission of information between two parties to carry out financial or administrative activities related to health care. HIPAA sets standards for the following electronic transactions:
    a. Health care claims or equivalent encounter information.
    b. Health care payment and remittance advice.
    c. Coordination of benefits.
    d. Health care claim status.
    e. Enrollment and disenrollment in a health plan.
    f. Eligibility for a health plan.
    g. Health plan premium payments.
    h. Referral certification and authorization.
313. **Treatment –** The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
314. **Treatment, Payment and Healthcare Operations (TPO):** In the context of HIPAA, TPO refers to activities and disclosures of PHI which may be accomplished without specific authorization or knowledge of the patient, and which do not currently require accounting of disclosures.
315. **Trojan horse** - A program in which malicious or harmful code is contained inside apparently harmless programming or data.
316. **Unique user identification** - The combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity.
317. **"Unsecured" PHI** - 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 in guidance." See also *Secured PHI*.
318. **Use** – The sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains such information.
319. **User authentication** - The provision of assurance of the claimed identity of an entity.
320. **User-based access** - A security mechanism used to grant users of a system access based upon the identity of the user.
321. **Virus** - A piece of code, typically disguised, that causes an unexpected and often undesirable event. Viruses are frequently designed to automatically spread to other computers. They can be transmitted by numerous methods including e-mail attachments, downloads, and on removable media.
322. **Virus checking** - A computer program that identifies and disables viruses.
323. **Vulnerability** - A flaw or weakness in system security procedures, design, implementation, or internal controls that can be exploited by a threat and result in misuse or abuse of EPHI.
324. **Vulnerability [CNSSI 4009]** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

325. Vulnerability Assessment [CNSSI 4009] - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
326. Willful neglect – The conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provisions.
327. Workforce member - Employees, volunteers, medical staff, faculty and other persons whose conduct, in the performance of work for the covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part-time employees, affiliates, associates, volunteers and students who have access to PHI in order to satisfy a clinical experience requirement for a program of study.
328. Workforce – A company's employees, volunteers, trainees, and other persons under the direct control of the company.
329. Workstation - An electronic computing device, for example, a laptop or desktop computer, or any other device (e.g. Smart phone or PDA) that performs similar functions, and electronic media stored in its immediate environment.
330. Worm - A piece of code, usually disguised, that spreads itself by attacking and copying itself to other machines. Some worms carry destructive payloads that delete files or distribute files; others alter Web pages or launch denial of service attacks.