CHMSP

Additional Terms & Definitions You Need for the Mock and Certification Exams

The Certified HIPAA Managed Service Provider (CHMSP) exam is open note, open book. It is recommended to have this list below handy while taking the Mock and Certification Exams. Retake the Mock Exam over and over to help prepare for your certification exam. The certification exam is 100 questions, proctored and must be completed within 3 hours. Passing grade is 80%, so keep retaking the mock exam until you increase speed and consistently score well above 80% each time!

Access - The ability or the means necessary to read, write, modify or communicate data / information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.)

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

Adverse Event - Any event that has a negative consequence. For example: a system crashes, a network is under attack by high traffic hackers, a user acquires privileged access on the network they are not authorized to use, unauthorized access is made to sensitive data, data is corrupted or destroyed.

Amend/Amendment – When used in reference to EHR systems, an amendment to ePHI should always be in the form of information added to the existing ePHI. This additional information may contain items that substantially change the initial PHI, make parts of the initial ePHI more precise, or show some of the original ePHI to be incorrect. However, the original ePHI is never altered. Changes are indicated by the addition of the amended information.

Authentication - To corroborate or confirm that a person is the one they are claimed

Authorization - A person served statement of agreement to the use or disclosure of Protected Health Information to a third party.

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

BAs – Business Associates (BA) – The businesses that provide services to CEs that need them to have some level of access to ePHI (create, receive, maintain or transmit). They may have access because they do the insurance billing or because they do the shredding of paper reports with ePHI. There are many companies that offer these kinds of services such as transcription, claim processing, statement printing, shredding, legal, accounting and more. **HITECH revised liability for BAs who are now separately and equally liable for compliance with the Security Rule and portions of the Privacy Rule.**

BAA – Business Associate Agreement – The legal contract required under the Privacy Rule between all CEs and BAs as well as between two BAs if a BA uses a subcontractor. The HITECH Final Rule defines BAs as BAs based on the work they do, not on actually having an agreement in place. An agreement *must* be in place but the *lack* of one does not remove compliance requirements.

Breach – Generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. If PHI is seen, used or accessed in a manner outside the Privacy guidelines it is considered a Breach.

Breach Exclusions - when performing an analysis of an incident to determine if a breach has occurred the following exclusion.

- 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.
- 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.
- 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.

Breach Notification Rule – Defines specific action that must be taken by CEs in the event of a breach. Notification must be made to the patients and HHS and, in cases involving over 500 patients, to the media. Notification information and timelines are specifically defined in the rule. Beginning with the Final Rule, all breaches are assumed to require notification to the patient unless an assessment is completed and documents there has been no specific harm to the patient due to the breach.

Breach Risk Assessment - Covered entities and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors:

- The **nature and extent of the protected health information involved,** including the types of identifiers and the likelihood of re-identification;
- The **unauthorized person** who used the protected health information or to whom the disclosure was made;

- Whether the protected health information was **actually acquired or viewed**; and
- The **extent** to which the risk to the protected health information has been **mitigated**.

Breaches treated as discovered by BA. A breach shall be treated as discovered by a BA as of the first day on which such breach is known to the BA or, by exercising reasonable diligence, would have been known to the BA. A BA shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate.

Breaches treated as discovered by CE. A breach shall be treated as discovered by a CE as of the first day on which such breach is known to the CE, or, by exercising reasonable diligence would have been known to the CE. A CE shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

Burden of proof. In the event of a use or disclosure, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by law or that the use or disclosure did not constitute a breach.

Business Associate (BA) - A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Manage Service Providers are business associates when the client is a HIPAA covered entity or CE.

Business Associate Agreement (BAA) – A written contract also known as "Business Associate Contracts" between a Covered Entity (CE) and Business Associate (BA). The written contract must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements

applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

Business Associate Notification - In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires business associates to notify the covered entity of the breach. It is important to determine if the BA is functioning as an agent or independently.

NOTE: The notification timeline begins immediately for the CE if an agent relationship exists. It starts when the notification by the BA occurs otherwise. the Organization's Business Associate Agreements (BAA) require notification in [notification days in BAA]. However, all BAAs are not the same. Refer to the specific agreement with a business associate to determine their required timelines.

Business Continuity Plan - A plan that will allow continuity of service or care in support of restoration of lost data in the emergency mode of operations of your business or practice.

Business Culture - Business Culture includes the values, visions, beliefs and habits an organization share as a whole. The business culture is rooted by the organization's goals and strategies and often is implied, not expressly defined. The business culture can shift over time as the organization's beliefs, visions and values change.

Civil Penalties – Non-compliance fines also referred to as Civil Monetary Penalties or CMPs under HIPAA were limited to $25,000 per year per violation. HITECH fines are now limited to $1.5 Million per calendar year per violation with minimum required fines as much as $50,000 per violation. The Federal Civil Penalties Inflation Adjustment Act of 1990 (the Inflation Adjustment Act) will adjust the fines.

CMS – Centers for Medicare and Medicaid Services is a division of HHS that manages all Medicare and Medicaid activities plus the Children's Health Insurance Program.

Communication System - Electronic mechanisms or devices used to disseminate verbal or written information. Examples of communication systems include, but are not limited to, FAX, Email, Text Messages, Messaging Apps, etc.

Compliance-based privacy and security program - This type of program approach focuses on meeting the minimum necessary requirements for regulations, sometimes seen as a checklist approach to meeting compliance obligations. A compliance-based program just worries about protecting PHI, not all risks to the organization.

Note: If your organization's primary concern is meeting HIPAA compliance obligations, then it would lean more towards a compliance-based approach.

Compliance Team - A group of individuals to ensure that an organization adheres to external rules and internal controls. It is recommended that this team is made up of individuals from different departments. For example, Human Resources, Finance, Management, IT, Privacy and Security Officers, etc.

Computer Security Incident - A violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices. For example:

- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user posts sensitive information on a social networking site.
- Your computers are infected with a malware that utilizes your network to attack other external networks with high volumes of connection requests originating from a botnet on your network.

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

Confidentiality, Integrity and Availability (CIA) - Protecting the CIA of ePHI is the core objective of the HIPAA Security Rule for all covered entities and business associates.

Confidential Information - Any information that shouldn't be released to the general public, such as protected health information, company sensitive information, personal information, etc.

Consent - A document signed and dated by the individual that a covered entity obtains prior to using or disclosing protected health information to carry out treatment, payment or healthcare operations. Consent is not required under the privacy rule.

Corrective Action Plan (CAP) - One of the consequences, and part of an aggressive enforcement action imposed by OCR, in response to a HIPAA-covered entity or business associate that has egregiously violated HIPAA laws.

Court Order - An order issued by a competent court that requires a party to do or abstain from doing a specific act.

Covered Entity (CE) - A health plan, a healthcare clearinghouse, or a healthcare provider that is covered by the Privacy and Security Rules.

Create, Receive, Maintain, Transmit (CReMaT) - These are functions that a business associate (BA) might perform on behalf of a covered entity or another business associate (BA) regarding protected health information (PHI). If a person or entity, other than a member of a covered entity's workforce, creates, receives, maintains, or transmits protected health information on behalf of a covered entity (CE), then the person or entity is considered a business associate (BA)

Criminal Penalties – Since June 2005, CEs as well as BAs and their directors, employees or officers may also be criminally liable. Criminal cases are prosecuted by the *U.S. Department of Justice*. A federal criminal case can be brought if it is determined that PHI is obtained or disclosed, even if you simply just know it happened. One year imprisonment and fines up to $50,000 can be levied in simple cases. If it is done under false pretenses penalties rise to $100,000 and 5 years. The penalties are $250,000 and up to 10 years in cases involving *intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm*.

Cybersecurity Committee (CSC) - A management structure to direct the continuous cycle of development, management, and implementation of client's cybersecurity management.

Cybersecurity Framework (CSF) - The Cybersecurity Framework provides a voluntary, risk-based approach based on existing standards, guidelines, and practices to help organizations to understand, communicate and manage cybersecurity risks.

Data Aggregation - Protected health information (PHI) created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Data Governance - Defines who can take what action, upon what data, in what situations, using what methods. The rules for data.

Data Security - Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Data Transmissions - Refers to electronic point-to-point transmission of data initiated from the Organization's network to a destination outside the Organization network. Types of data transmissions include File Transfer Protocol (FTP), Network Data Mover (NDM), etc. Email or Fax transmissions or non-electronic transmissions of data are not included.

Defense-in-Breadth - 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).

Defense-in-Depth - Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

De-Identification - The process of converting individually identifiable information into information that no longer reveals the identity of the person served.

De-identified Health Information - Health information that does not identify an individual and does not contain information that can identify or link the information to the individual to whom the information belongs.

Designated Record Set - A group of records maintained by or for the Organization that is:

- The medical records and billing records about individuals maintained by or for the Organization; or,
- Used, in whole or in part, by or for the Organization to make decisions about individuals.

For purposes of this definition, the term "record" means any item, collection or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for the Organization.

Disaster Recovery Plan (DRP) - A Plan that will be used in the event of a disaster to restore any loss of data.

Disclosure - The release, transfer, provision of access to, or divulging in any other manner of information outside the Organization. The two types of disclosure are:

- **Routine Disclosure** - Customary disclosures of PHI that the Organization discloses on a regular basis.
- **Non-Routine Disclosure** - Disclosures of PHI that are not usually disclosed by the Organization.

Dual Factor Authentication - See Two Factor Authentication.

EHR – Electronic Health Records – Patient medical charts in electronic formats. The clinical information your healthcare providers keep on file originally on paper is now done with computer systems called EHRs.

Electronic Media - Electronic storage media including memory devices in computers such as hard drives and any removable and/or transportable digital memory medium, such as magnetic tape, magnetic disk, optical disk, or digital memory cards.

Emergency Access - Emergency access is access to the Organization's *information assets* on a temporary basis; that circumvents the standard access request processes due to the urgency of the access need.

Encryption - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Encryption is a means of securing electronic transmissions, including email, data files and electronic commerce transactions by transforming confidential plain text into cipher text. Encryption combines data with values called keys or ciphers to "lock" the message to limit unauthorized viewing when traveling through the Internet or other *open networks*.*

Encryption at rest - Refers to data that is encrypted when it is stored in a persistent state, such as on a disk, tape, or other storage media.

Encryption in transit - Refers to data that is encrypted as it is transmitted between one place to another, such as over the internet or within a private network.

Enforcement Rule – The original HIPAA rules had very little enforcement included. HITECH added a whole new Enforcement Rule with serious civil and criminal penalties for non-compliance. It also requires OCR to do random audits of CEs and BAs. The audit program was tested in 2012 and resumed in 2016.

ePHI or Electronic Protected Health Information - Any protected health information that is produced, saved, transferred, or received in an electronic form.

Event - Any observable occurrence in a system or network. For example: a user logged on to a system, a server processed a request for a web page, a user sending an email, etc.

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

FERPA - The Family Educational Rights and Privacy Act (FERPA) is a federal privacy law that gives parents certain protections regarding their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules. As a parent, you have the right to review your child's education records and to request changes under limited circumstances. To protect your child's privacy, the law generally requires schools to ask for written consent before disclosing your child's personally identifiable information to individuals other than you. School nurse and infirmary records are included under FERPA and not HIPAA.

Final Rule – Final guidance and interpretations of the legal requirements of the HITECH Act that are required to be enacted. Released January 25, 2013. Effective March 26, 2013, with a grace period that ends September 23, 2013.

Financial Records - Admission, billing, and other financial information about a person served included as part of the designated record set.

FIPS 140-2 - The Federal Information Processing Standard (FIPS) Publication 140-2 is a United States government computer security standard for encryption models issued by NIST.

FISMA - The Federal Information Security Modernization Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. FISMA was signed into law as part of the Electronic Government Act of 2002.

Frameworks - Blueprints used to guide the development of a privacy and security program.

Fundraising - An organized campaign by a private, nonprofit, or charitable organization designed to reach out to certain segments of the population or certain identified populations in an effort to raise money for their organization or for a specific project or purpose supported by their organization.

Governance - The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements. It also includes that management is informed of their cybersecurity risk.

Healthcare - Includes, but is not limited to, the following:

- Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body; and,
- Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse - **HHS Description General Provisions: Definitions - Health Care Clearinghouse as a** public or private entity, including billing services, repricing companies, community health management information systems or community health information systems, and "value-added" networks and switches, that does either of the following functions:(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Healthcare Operations - Any of the following activities of the Organization to the extent that the activities are related to covered functions:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities;
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and,
- Business management and general administrative activities of the Organization, including, but not limited to:
    - Management activities relating to implementation of and compliance with the requirements of these policies and the HIPAA Regulation;
    - Person served service;
    - Resolution of internal grievances;
    - The sale, transfer, merger, or consolidation of or part of the Organization with another covered entity, or an entity that following such activity should become a covered entity and due diligence related to such activity; and,
    - Consistent with the applicable requirements of PRV-059 De-identified Data and Data Use Agreements and creating de-identified health information or a limited data set, and fundraising for the benefit of the Organization, and marketing for which an individual authorization is not required.

Health Plan - § 160.103. **Health plan** means an individual or group **plan** that provides, or pays the cost of, **medical care** (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

Healthcare Provider - An entity that provides healthcare, service or supplies related to the health of an individual,

e.g., medical, dental, physical therapy, occupational therapy, speech therapy, behavioral health services or chiropractic clinics or hospitals.

Health Oversight Agency - An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory or an Indian tribe that is authorized by law to oversee the healthcare 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.

HHS – U.S. Department of Health & Human Services is the principal agency for protecting the health of Americans and providing essential human services to our citizens. There are many divisions and offices within HHS including Centers for Disease Control and Prevention, National Institutes of Health and the Food and Drug Administration.

HHS 405(d) - A program created under the Cybersecurity Act of 2015 and managed by the Department of Health and Human Services. The charter of the 405(d) Task Group is to enhance cybersecurity and align industry approaches by developing a common set of voluntary, consensus-based, and industry-led guidelines, practices, methodologies, procedures, and processes that healthcare organizations can use to enhance cybersecurity. The Task Group includes experts from many areas of both public and private organizations.

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) - Healthcare specific guidance that uses the NIST CSF as its foundation. It is customized specifically for implementation by what healthcare organizations need for cybersecurity. It is customized specifically for implementation in healthcare organizations and provides specific guidance for implementing cybersecurity protections for small, medium, and large organizations.

HIPAA – *Health Insurance Portability and Accountability Act of 1996*, Public Law 104-191 which included several sections. HIPAA law requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy and security of protected health information. The primary discussions on Small Provider HIPAA relate to the Privacy Rule and the Security Rule.

HIPAA Violation Civil Money Penalties - Penalties for violations of HIPAA are determined by the Health and Human Services Office for Civil Rights (HHS OCR). Penalties will be based on the organization's culpability for the HIPAA violation. According to the HITECH Act of 2009, the maximum penalty per violation is $50,000 with a cap of $1,500,000 for all violations of an identical requirement or prohibition during a calendar year. However, the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (the 2015 Act) adjusted all federal civil money penalties for inflation including those in the HITECH Act. Minimum penalties are tiered based on the determined organizational culpability as adjusted by the 2015 Act:

Organization Culpability Tier	Minimum Penalty Per Violation	Maximum Penalty Per Violation	Annual Maximum for Identical Violations
Did not know the act was a HIPAA violation and would not have known by exercising reasonable diligence	$110	$55,010	$1,650,300
The HIPAA violation had a reasonable cause and was not due to willful neglect	$1,100	$55,010	$1,650,300
The HIPAA violation was due to willful neglect but was corrected within 30 days	$11,002	$55,010	$1,650,300
The HIPAA violation was due to willful neglect but was not corrected	$55,010	$1,650,300	$1,650,300

HIPAA Violation Criminal Penalties - Potential jail sentences can be applied if an investigation by the Department of Justice determines the violation meets the criminal liability elements of the statutes. Knowingly obtaining and disclosing PHI can be considered criminal.

Criminal penalties are also applied based on tiers of culpability and intent.

Culpability and/or intent	Potential Jail Sentence	Criminal Fines
Knowingly obtained or disclosed PHI in violation of HIPAA	Up to 1 year	$50,000
Under false pretenses	Up to 5 years	$100,000
With the intent to sell, transfer, or use PHI for personal gain or malicious reasons	Up to 10 years	$250,000

HITECH – *Health Information Technology for Economic and Clinical Health* enacted as part of the *American Recovery and Reinvestment Act of 2009*. This act made changes to the original HIPAA provisions in the Privacy Rule plus added Enforcement requirements and a Breach Notification Rule that were never in place before 2009. The act includes many more provisions, but our discussions here address only these areas.

HITRUST - Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and

assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience. The HITRUST framework is also called CSF. Any reference to this CSF will specifically note that it is the HITRUST CSF.

Hybrid Covered Entity - An entity that is is a single legal entity that performs both covered and non-covered functions.

Incident Response Plan - A formal written plan for detecting, responding to and limiting the effects of a security incident. An organized and well-planned reaction to an incident can mean the difference between complete recovery and total disaster.

Incident Reporting - Implementing mechanisms that will perform audits and reporting in order to address security incidents, suspicious network activity, and security device failures at the Organization.

Individually Identifiable Health Information (IIHI) - Any information, including demographic information, collected from an individual that:

- Is created or received by a healthcare provider, health plan, business associate, employer or healthcare clearinghouse; and
- Relates to the past, present or future physical or mental health or condition of an individual, and
    - Identifies the individual or
    - With respect to which there is reasonable basis to believe that the information can be used to identify the individual.

Information Access - Access to *information assets* with the ability to use, view, modify, replace, create or delete without direct supervision, regardless of medium. Persons with access to data and systems must have a business need for access and must be authorized according to formally documented procedures.

Information Asset - All company data storage devices (i.e., *media**), systems (i.e., personal computers and laptops), equipment (i.e., fax machines, printers and copy machines), and all information that is created, stored, or transferred within the company's facilities and/or systems.

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

Integrity - The property that data or information has not been altered or destroyed in an unauthorized manner.

Interim Rule – Guidelines and interpretations of the legal requirements of the HITECH Act effective November 30, 2009. CEs and BAs were to use these guidelines while the specifics were finalized.

Integrity Controls - Security mechanisms and methods that are employed at the Organization to ensure the validity of information that is electronically transmitted or stored, such as the use of checksums or encryption of files either at rest or in transit.

IoT - Refers to "the internet of things" or the connection of physical devices that are embedded with electronics, software, sensors, etc. that enable objects to collect and exchange data.

Likelihood of Occurrence - A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Limited Data Set (LDS) - A data set that includes elements such as dates of application, termination, birth, and death as well as geographic information such as the five-digit zip code and the individual's state, county, city, or precinct but still excludes the other 16 elements that "de-identify" information. In addition, this limited data set can only be used if a covered entity enters into a "data use agreement" with the data recipient similar to the agreements entered into between covered entities and their business associates.

Low Probability of Compromise (LoProCo) - an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability of compromise of the protected health information. Through completing a breach risk assessment and documenting all the details, LoProCo can be determined, and notifications are not required.

Malicious software (Malware) - Software that is intended to damage or disable computers and computer systems.

Marketing - To make a communication about a product or service, the purpose of which is to encourage recipients of the communication to purchase or use the product or service. Face-to-face communications or those where only a gift of nominal value is provided are not considered marketing under the Privacy Rule. Marketing does not include the following:

- Communications by a covered entity for the purpose of describing the entities participating in a healthcare provider network or healthcare plan network or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits.
- Communications tailored to the circumstances of a particular individual if the communications are made by a healthcare provider to an individual as part of the treatment of the individual and for the purpose of furthering the treatment of that individual.
- Communications by a healthcare provider or healthcare plan to an individual in the course of managing the treatment of that individual or for the purpose of directing or recommending to that individual alternative treatments, therapies, healthcare providers or settings of care.

Media - Any physical medium or device capable of storing the Organization information assets*. Examples of types of media include but are not limited to CD-ROM, tapes, hard drives, diskettes, microfiche, microfilm, and paper documents.

Meetings by design - Meetings should include topics that could create privacy or security concerns in advance. Any policies, projects, next steps, etc. from meetings should consider privacy and security.

Minimum Necessary - Refers to the rule that states when someone working on behalf of a covered entity (CE) or business associate (BA) is using or disclosing protected health information (PHI), they much make reasonable efforts to limit the PHI to the minimum amount necessary to accomplish the task.

Mobile Devices - Transportable workstation devices include but are not limited to laptops, palm pilots, text pagers, notebooks, and wireless communications systems. Compliance to the Mobile Device Privacy and Security and description of "mobile device" is explained by ONC for health care professionals on their website healthIT.gov

Need to Know - Limiting use, disclosure of, or requests for, the Organization information assets, such as corporate information assets, to the minimum amount of information that is necessary to accomplish the purpose of the use, disclosure or request based on the principle of least privilege.

NIST - National Institute of Standards and Technology is a measurement standards laboratory and agency within the United States Department of Commerce whose mission is to promote innovation and industrial competitiveness. NIST provides a framework for improving cybersecurity among the sixteen defined critical infrastructure sectors under Homeland Security, of which Healthcare is one.

NIST Cybersecurity Framework (CSF) - The Cybersecurity Framework provides a voluntary, risk-based approach based on existing standards, guidelines and best practices to help organizations understand, communicate and manage cybersecurity risks.

Notice of Privacy Practices (NPP) – Also known as a "NOPP" which is a document required by health plans and health care providers under HIPAA that provides the person served with information about their rights under the Privacy Rule and how the Organization generally uses their Protected Health Information. OCR provides a "model" or sample NPP and options for meeting the requirement to create notices of privacy practices on their website "Model Notice of Privacy Practices".

Notifications and Timelines - In breach cases that require notification, there are specific time frames that must be met by law. The applicable time frames and notifications required are determined by the number of patients involved.

Patients Involved	Patient Notifications	HHS Notifications	Media Notifications
Fewer than 500	Within 60 days of discovery of breach	Annually but no later than Feb 29 or March 1 of each calendar year for the previous calendar year incidents	Not required
500 or more	Within 60 days of discovery of breach	Within 60 days of discovery of breach	Within 60 days of discovery of breach

OCR – Office for Civil Rights is the entity within HHS that is responsible for enforcing HIPAA among other activities including offering guidance on the rules and performing audits and investigations.

Office of Inspector General (OIG) – Government's fraud and abuse enforcement agency.

Omnibus Final Rule or Omnibus HIPAA Rulemaking - The U.S. Department of Health and Human Services (HHS) Office for Civil Rights finalized the HIPAA Omnibus Rule in January 25, 2013 and went into effect on March 26, 2013 with a compliance date for CEs and BAs of September 23, 2013. This final rule implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ONC – Office of the National Coordinator for Health Information Technology is the principal federal entity charged with coordination of nationwide efforts to implement and use health information technology and the electronic exchange of health information.

Open network - A network that is exposed to various external networks during the course of carrying out daily business operations. Examples of external networks would be the Internet, and vendor connectivity and email systems.

Opt Out - To make a choice to be excluded from services, procedures or practices. Person served rights under HIPAA include many situations where the person served may request to be excluded from a service, procedure or practice. In most cases, the Organization should comply or attempt to comply with the request to be excluded.

Order - A mandate, precept; a command or direction authoritatively given; a rule or regulation. When using this term with a health care provider, the word "order" also refers to a written or verbal order for patient treatment, so clarify use of this word when working with providers.

Password - A group of characters used to authenticate a *user** to a system, application or network. Passwords are used to control access to *information assets** to authorized individuals. Password uses include but are not limited to user-level accounts, system-level accounts, web accounts, email accounts, screensaver protection, voicemail accounts and local router logins.

Payment - The activities undertaken by a healthcare provider or payer to obtain reimbursement for the provision of care and services. "Payment" is better known as "Reimbursement" when distribution of funds is made to pay a health care claim to a health care provider.

Person Served - Refers to persons applying, waiting for or receiving services from the Organization.

Personal Representative - The term used in the Privacy Rule to indicate the person who has authority under law to act on behalf of a person served. For purposes of the Privacy Rule, the Organization should treat a personal representative as having the same rights as the person served unless there is a reasonable belief that the personal representative has subjected the person served to abuse or neglect or treating the person as the personal representative could endanger the person served.

PCI - The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

PHI – Protected Health Information under HIPAA law. PHI relates to patient information protected under the Privacy and Security rules.

Phishing - A malicious attempt, typically via email, to trick someone into revealing sensitive information such as usernames, passwords, and credit card information to a hacker or other cybercriminal.

Physical safeguards - The physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Policy - The documentation of the organization that outlines how you will handle operational requirements.

Policy by design - Any policy being created, updated, or reviewed includes an evaluation of privacy and security needs the policy must address. The policy documents any assumptions made in that evaluation.

Privacy and Security by Design – Privacy and Security by Design is meant to reflect a holistic approach at an organization level. When privacy and security concerns are built into every process, system, discussion, etc. as a matter of habit, not an added burden.

Privacy Breach - A violation of one's responsibility to follow privacy policy and procedure that results in the PHI of a person served being accessed by unauthorized persons.

Privacy Officer - the Organization workforce member who has been designated, pursuant to the Privacy Rule, with responsibility for ensuring the Organization's compliance with the Privacy Rule.

Privacy Rule – The portion of HIPAA that defines the "who, what, where and when" of using or accessing PHI that is collected and maintained by healthcare organizations. This section includes the required HIPAA form most people recognize from signing when they visit their healthcare providers. Effective since April 14, 2003.

Private Network - A network established and operated by an organization or corporation for users within that organization or corporation.

Procedure - A process or series of steps to be followed as a consistent and repetitive approach to accomplishing an end result. Procedures often support a related policy.

Production Data - Any data that is a record of business activity or otherwise directly affects business decisions.

Proper Disposal - The HIPAA Privacy Rule requires that covered entities and business associates apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI). This includes the destruction or disposal of PHI. A covered entity or business associate must implement policies and procedures to address the final disposition of electronic PHI and hard copy forms of PHI in accordance with the HIPAA Security Rule.

Protected Health Information (PHI) - all the medical records, insurance records and billing records relating to a patient's care. Also referred to as **ePHI** when speaking specifically about the electronic versions of this information. This is the information that all these rules are attempting to make sure only those necessary are allowed to access it.

Psychotherapy Notes - Notes that are recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. Psychotherapy notes should be kept separate from the rest of the master record of the person served.

Public Law 104-191 – is the Health Insurance Portability & Accountability Act approved August 21, 1996. This is an act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Public Network - A network established and operated by a telecommunications administration or by a Recognized Private Operating Agency (RPOA) for the specific purpose of providing circuit-switched, packet-switched, and leased-circuit services to the public.

Qualified Protective Order - A legal command intended to protect a person or thing from an unfair or unjust action.

Re-Identification - The process of converting de-identified health information back to individually identifiable health information. Re-identified health information does reveal the identity of the person served and should be treated as PHI under the Privacy Rule.

Remote Access - Refers to a connection to a local system from a remote location. For example, users might connect to the office network from a location outside the office, such as their home. Usually this is accomplished using a VPN connection or other hardware and software configurations.

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

Residual Risk - Portion of risk remaining after security measures have been applied.

Revoke - To cancel or withdraw an authorization to release medical information.

Risk Analysis Related Terms:

- **Threats** – Define circumstances or events with the potential to cause problems for your business. Include human, natural and environmental threats. Think of everything from power failures and floods or fire to burglary or employee sabotage or accidents to hard drive failures on your computers. What if the country is attacked again or terrorists (foreign or domestic) attack your area; that is a potential threat in the world today. What if you come into work and your server is off and won't turn on or start up at all?
- **Vulnerability** – Define the weaknesses in your facilities, policies or information systems that could be exploited if a threat actually occurs. Group them into technical and non-technical categories. Non-technical could be things like ineffective or non-existent policies, procedures or guidelines. Technical might include holes in the information systems security or improperly implemented systems.
- **Impact** – Define how bad it would be if those things (mentioned above) did happen. Would it be a pain but just a bump in the road, or would it be devastating harm to your business. Would it damage your reputation or your equipment or your ability to treat patients?
- **Likelihood** – Now you define how likely this is to occur and cause the impact or harm you have assessed previously.
- **Risk** – The combination of information determined above. A very high-risk item (vulnerability) would be one that is almost certain to occur (likelihood) and cause serious harm (impact) to your business. You can assign numeric values (or ranges) to define risk ratings or letter ratings or simply very low to very high ratings.
- **Controls** – Safeguards that could be administrative, physical or technical that are put in place to control risk.

Risk Assessment - The process of understanding the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals.

Risk based privacy and security program - This type of program will consider the privacy and security risks the organization faces as a whole and how they should be addressed. A risk-based program worries about managing all risks to the organization, not just legal requirements, and PHI.

- Note: If your organization's primary concern is protecting the privacy and security of your patient information which includes HIPAA compliance obligations, then it would be a risk-based approach.

Risk Management - The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions. The plan of action identified after a Risk Analysis or Assessment and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Sanctions - A range of penalties for your workforce that fail to comply with your Security and Privacy Policies and Procedures. The type of sanctions could be a meeting, documentation in an employee chart, additional training, time off without pay or termination.

Safeguards - A measure taken to protect someone or something or prevent something undesirable, or the implementation of these measures. The HIPAA privacy rule requires covered entities and business associates to implement appropriate administrative, physical and technical safeguards in order to protect the privacy of PHI. The HIPAA Security Rule establishes a minimum requirement for each class of safeguard.

Screen Saver - Any software program designed to, after a certain period of inactivity, display on a workstation monitor a random display of patterns, images, or to simply make the monitor blank so as to prevent an image from being burnt into the monitor.

Secured Areas - Any the Organization facility areas that require physical access authorization beyond the authorization needed to gain access to the physical perimeter, due to increased sensitivity of *information assets** stored within the facility area. Examples of secured areas are server rooms and data centers.

Security or Security measures - Measures to encompass all of the administrative, physical, and technical safeguards in an information system.

Security Impact Analysis - 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.

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

Security Objective – Achieving confidentiality, integrity and availability of patient data.

Security Officer - Under HIPAA, this is a person who is responsible for the ongoing management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all protected health information systems.

Security Rule – The portion of HIPAA that defines the safeguards that should be in place to provide protection of PHI. The rules cover the physical buildings and offices, the networks and computer systems plus the training and rules for workforce members. Effective since April 20, 2005.

Software Patch - A program designed to upgrade or update a software program or application to fix vulnerabilities or improve its usability or performance. See also Windows Update

Spam - Unsolicited, usually commercial, or objectionable form of communication (e.g., using email, instant messaging etc.) sent to a large number of recipients.

Spyware - Spyware is a generic name for unsolicited software installed without notice -- either by other programs' set up routines or by hostile Websites that exploit flaws in Microsoft's Internet Explorer browser.

Subcontractor - A person or entity who acts on behalf of the Organization.

Subpoena - A process to cause a witness to appear and give testimony, commanding him/her to lay aside pretenses and excuses and appear before a court or magistrate therein named at a time therein mentioned to testify for the party named under a penalty thereof. There are two (2) kinds of subpoenas:

- **Duces tecum** - A request for witnesses to appear and bring specified documents and other tangible items. The subpoena duces tecum requires the individual to appear in court with the requested documents, or simply turn over those documents to the court or to counsel requesting the documents.
- **General subpoena (a.k.a. ad testificandum)** - A command to appear in court at a certain time and place to give testimony regarding a certain matter, for example, to testify that the record was kept in the normal course of business.

System User ID - Any user identification not associated with a person or group of persons that is utilized to control access to electronic data. System user IDs include but are not limited to production batch, disaster recovery, system backup, system or application software and other similar IDs.

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

Termination - Termination of employment or of a contract to perform services for the Organization. Termination requires discontinuation of all contracts, obligations, and access to the Organization's *information assets** by the separated member of the Organization's *workforce** or outside contractor.

Test Data - Any subset of actual or made-up data used for testing systems or applications modifications.

Threat - 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.

Threat Assessment - Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Token - A physical item that contains the identity of the holder or "something you have." Examples of tokens include ID badges and smart cards.

Training - An organized activity aimed at communicating information and/or instructions to others in an effort to educate, teach a new skill, or improve performance.

Treatment - The provision, coordination or management of healthcare and related services by the Organization, including the coordination or management of services by the Organization with a third party; consultation with other providers relating to a person served; or the referral of a person served for services between the Organization and another authorized care provider.

Treatment, Payment and Operations (TPO) - The Privacy Rule allows sharing of information for purposes of treatment, payment and healthcare operations. Treatment includes the use of person served information for providing continuing services. Payment includes sharing of information in order to bill for provision of services to the person served. Healthcare operations are certain administrative, financial, legal, and quality improvement activities that are necessary for the Organization to run its business and to support the core functions of treatment and payment.

Two Factor Authentication (2FA) - An authentication method requiring a person to enter two of the three distinct verification factors: a knowledge factor ("something you know"), possession factor ("something you have"), and inherence factor ("something you are"). For example, a person might be asked to enter a password ("something you know") and depress their thumb on a fingerprint scanner ("something you are").

Two Step Verification (2SV) - An authentication method where one enters a username and password for an account and is then sent a one-time code via a phone call, email, text message (SMS), or pre-verified device. The person must enter the code within a specified amount of time in order to gain access to the account.

Unauthorized Disclosure - A disclosure or sharing of information to an individual who is not authorized to receive it.

Unsecured protected health information - Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

Use - With respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of that information within the Organization. (See also **Disclosure**)

User - An individual or entity with authorized access.

User ID (User Identity or UID) - A group of characters that are used to identify a person or other entity when accessing networks, systems or applications. User ID's accompanied by a password, known only to the individual associated with the ID, are used to gain access to a system or application.

Visitor - A visitor is any person who is not a member of the Organization's workforce, and who physically accesses any the Organization facilities.

Virtual Private Network (VPN) - A method used to connect one system or network to another over the internet through a secure tunnel. VPNs add security and privacy to a private or public network.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability Assessment - 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.

Whistleblower - A person, usually a workforce member, who reveals wrongdoing within an organization to public agencies, government agencies or to those in positions of authority.

WiFi or Wireless Networking - A networking technology that uses radio waves vs. physical wired connections to provide wireless high-speed Internet and network connections.

Willful Neglect – A category assigned when there are compliance problems identified within an organization by HHS/OCR. Willful Neglect means a company clearly ignores their obligation to comply with HIPAA. There are two levels considered in the designation. One is that problems are corrected in a reasonable amount of time when mistakes are discovered and the other is when no changes are made. Neither designation is desirable since they define the ***minimum fines required by law per violation*** are $10,000 and $50,000, respectively.

Windows Update - Refer to software patches or updates to a Windows operating system to fix vulnerabilities or add functionality. Windows Update is a Microsoft service that provides updates or patches to not only Windows operating systems but also other Microsoft products.

Workforce - Includes all employees, temporary employees, volunteers, trainees, and interns both part-time and full-time, who perform services for a practice or organization.

Workstation - An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.