# GLOSSARY OF HIPAA RELATED TERMS

| Term | Definition |
|---|---|
| ***Access:*** | The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource. |
| ***Accounting for Disclosures*** | Information that describes a covered entity's disclosures of PHI other than for treatment, payment and health care operations; disclosures made with authorization; and certain other limited disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the 6 years (or a shorter time period at the request of the individual) prior to the date of the request for an accounting. |
| ***Administrative Safeguard*** | 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. |
| ***Amendment and Correction*** | An amendment to a record would indicate that the data is in dispute while retaining the original information. A correction to a record alters or replaces the original record. |
| ***Authorization:*** | Written permission by the patient or the patient's personal representative to use and/or disclose protected health information about the individual. The requirements of a valid authorization are defined in the HIPAA regulations. |
| ***Blog*** | A contraction of the term weblog. A website, usually maintained by an individual or a group of individuals with regular entries of commentary, description of events, or other material including graphics or video. |
| ***Breach:*** | The unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed, would not reasonably have been able to retain such information.<br>*An impermissible use or disclosure 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.* |
| ***Business Associate:*** | An individual or entity who performs certain functions or activities on behalf of IU that involve the use or disclosure of PHI. Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. A covered entity may be a business associate of another covered entity. |
| ***Business Associate Agreement:*** | A written contract between a covered entity and a business associate (BA) that establishes the permitted and required uses and disclosures of protected health information by the BA; requires the BA to implement appropriate safeguards to prevent unauthorized use or disclosure; requires BA to report to covered entity |

| Term | Definition |
|---|---|
| | any uses and disclosures not provided for in the contract; to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, requires the business associate to comply with the requirements applicable to the obligation; requires BA to ensure any subcontractors agree to the same restrictions. |
| ***Complaint:*** | A statement that a situation is unsatisfactory or unacceptable; An allegation of wrongdoing against an individual or organization. |
| ***Covered Entity:*** | A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with transactions covered by the HIPAA Privacy Rule. |
| ***Critical Data*** | Data if inappropriately handled may result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, or unauthorized access by an individual or many individuals (e.g., student loan information, social security number, driver's license number, passport or Visa number, state ID card number and protected health information). |
| ***Data Use Agreement:*** | An agreement required by the Privacy Rule between a covered entity (the holder of the PHI) and a person or entity that receives the limited data set (e.g. a research investigator) when the data are in the form of a limited data set. A Data use agreement establishes the ways in which the information in the limited data set may be used and how it will be protected. |
| ***De-Identified Health Information:*** | Health information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. |
| ***Designated Record Set:*** | A group of records maintained by or for a covered entity that is: the medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or used, in whole or in part, by or for the covered entity to make decisions about individuals.<br><br>Any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. |
| ***Disclosure:*** | Release, transfer, provisions of, access to, or divulgence in any manner of information outside the entity holding the information. |
| ***Electronic Protected Health Information:*** | Protected health information (PHI) created, maintained or transmitted in electronic form (**ePHI).** |
| ***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. |
| ***Fundraising:*** | Appeals for money, sponsorship of events, etc. for the benefit of a covered entity. HIPAA allows the disclosure of protected health information for this purpose |

| Term | Definition |
|---|---|
| | without an individual's authorization. |
| ***Health Information Exchange (HIE)*** | The process of reliable and interoperable electronic health-related information sharing conducted in a manner that protects the confidentiality privacy and security of the information. The electronic movement of health-related information among organizations according to nationally recognized standards. |
| ***Health Information Exchanges (HIE)*** | An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards. |
| ***Health Information Technology for Economic and Clinical Health Act (HITECH Act):*** | Federal law enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009. The HITECH Act promotes adoption and meaningful use of health information technology; widens the scope of privacy and security protections available under HIPAA; increases the potential legal liability for non-compliance; and provides for more enforcement. |
| ***Health Insurance Portability and Accountability Act (HIPAA):*** | A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Also gives Health and Human Services (HHS) the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. |
| ***Healthcare Operations:*** | Certain activities of the covered entity that are related to covered functions. These activities include, but are not limited to: administrative, financial, legal, underwriting and quality improvement activities that are necessary for a covered entity to run its business. |
| ***Incidental Use and Disclosure:*** | Secondary use[s] and disclosure[s] of protected health information (PHI) that cannot reasonably be prevented, limited in nature and that occur as a byproduct of an otherwise permitted use or disclosure. |
| ***Individual:*** | The person who is the subject of protected health information. |
| ***Individually Identifiable Health Information (IIHI):*** | A subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, 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; and identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. |

## GLOSSARY OF HIPAA RELATED TERMS

| Term | Definition |
|---|---|
| ***IU Fundraising Personnel:*** | Includes any IU employees or other IU personnel, including but not limited to the IU Office of Gift Development, who perform any fundraising activities on behalf of, or in affiliation, with another covered entity, such as the IU Health Physicians, the IU School of Medicine Clinical Departments or other HIPAA Covered Entity, and may have access to or use Protected Health Information for fundraising purposes. |
| ***IU HIPAA Affected Areas (IU HAAs):*** | Any school, department, division, or unit that may be a health care component; perform business associate services to another covered entity or a health care component; or have access to protected health information for education and/or research purposes. |
| ***Limited Data Set:*** | A data set of protected health information that excludes specified direct identifiers related to an individual or of relatives, employers, or household members of the individual, but retains geographic subdivisions larger than the postal address, elements of dates including month and day as well as other unique identifying numbers, characteristics or codes not previously listed as a direct identifier and cannot reasonably be used to identify an individual. Limited data sets may only be used for research, public health or for health care operations; and only in conjunction with a data use agreement. |
| ***Malware*** | Short for malicious software. Software the is intended to damage or disable computers and computer systems. Malware includes computer programs known as viruses, worms, Trojans, ransomware and spyware. |
| ***Marketing:*** | A communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Using protected health information for marketing purposes requires an authorization from the patient, unless the communication is: a face-to-face communication made by a covered entity to an individual; or a promotional gift of nominal value. |
| ***Minimum Necessary:*** | A standard that requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to certain uses or disclosures such as those requests by a health care provider for treatment purposes, disclosures to the individual who is the subject of the information or pursuant to an individual's authorization. |
| ***Mobile Computing Device or Mobile Device:*** | A small device, typically small enough to be handheld, that is capable of collecting, storing, transmitting, or processing electronic data or images. These may include a cellular telephone, mobile phone, smart phone, PDA, non-laptop based tablet (e.g. iPad, kindle, android), or USB-device. IU includes laptop and notebook computers in its definition of "mobile device". |
| ***Notice of Privacy Practices:*** | The Rule requires health plans and covered health care providers to provide adequate notice that provides a clear, user friendly explanation of the individual's legal rights with respect to their personal health information and the privacy practices of the covered entity. |

## GLOSSARY OF HIPAA RELATED TERMS

| Term | Definition |
|---|---|
| ***Observer:*** | An individual who has:<br>1. Completed the forms required by this Guidance Document<br>2. Been approved by a Unit: and<br>3. Been assigned to a Supervisor within a Unit to shadow an employee or healthcare provider.<br>It is highly recommended that Observers be at least 18 years of age to do an on the job shadowing experience with a healthcare provider. |
| ***Phishing*** | The activity of defrauding an online account holder by posing as a legitimate company or person. |
| ***Phishing Schemes*** | A form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email IM or other communication channels. |
| ***Physician-Patient e-mail:*** | Computer-based communication between physicians or associated medical personnel and patients within a professional relationship in which the physician has taken on an explicit measure of responsibility for the patient's care. [844 IAC 5-1-1]<br><br>These guidelines do not apply to communication between caregivers and consumers in which no on-going professional relationship exists. E-mail communications does not include communication via social networking sites or cell phone short messaging services (texting). |
| ***Payment:*** | Activities undertaken by a health care provider to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. |
| ***Personally Identifiable Information (PII):*** | Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information. |
| ***Physical Safeguards*** | Physical measures, policies and procedures to protect a covered entity's paper records and electronic information systems and related building and equipment from natural and environmental hazards and unauthorized intrusion. |
| ***Protected Health Information (PHI):*** | Individually identifiable health information held or transmitted by a covered entity or its business associate in any form or medium, whether electronic, on paper or oral. |
| ***Recording:*** | The action or process of storing sounds and images on electronic media or paper so they can be heard and/or seen again. Includes all methods of recording photographs, images, videos, audio and other digital or electronic media by which the identity of the recorded individual may be determined. |

## GLOSSARY OF HIPAA RELATED TERMS

| Term | Definition |
|---|---|
| ***Safeguards:*** | Specific actions which are designed to protect the privacy and security of an individual's health information. These actions may include: administrative measures such as policies, procedures, training and written agreements; physical measures such as locked doors or keycard access; and technical measures such as firewalls, password/passphrase and encryption. |
| ***Sanitizing electronic media:*** | A process by which data is irreversibly removed from media or the media is permanently destroyed. It includes removing all classified labels, markings, and activity logs. |
| ***Secure Destruction:*** | The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover. |
| ***Security Incident Response Team:*** | A group of individuals created to assist with an incident investigation. The incident response team will be activated at the discretion of the Information Security Office (ISO). The core IU Health incident response team members will be decided with each incident by the ISO. This team may typically consist of General Counsel representatives, IS representatives, a Media Relations Office representative, and a Compliance Office representative. |
| ***Security Incident:*** | The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. |
| ***Site:*** | The location where an Observer will watch an employee or Faculty member at work. The healthcare facility or practice that occupies the Site will be responsible for the administration of the shadowing experience in accordance with this policy or the facility's policy. For purposes of this policy, the term site may include but not be limited to a school clinic, department, practices, clinics or hospitals affiliated with Indiana University. |
| ***Social Networking Sites:*** | Internet sites that provide a variety of ways for users to interact, such as e-mail instant messaging, posting informational web pages and picture exchange services. Common Internet social networking sites are Facebook, Twitter, Instagram, LinkedIn, Pinterest, Google Plus+, Tumblr, VK, Flickr, Vine and Myspace. |
| ***Social Networking:*** | Online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail instant messaging and picture exchange services. |
| ***Supervisor:*** | An individual employed by or affiliated with the respective Health Science School or affiliated healthcare facility participating in the job shadowing experience and is responsible for determining when access to confidential information is appropriate. |
| ***Technical Safeguards*** | The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. |

## GLOSSARY OF HIPAA RELATED TERMS

| Term | Definition |
|---|---|
| ***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. |
| ***Use:*** | With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. |
| ***User:*** | A person who uses a computer or network service. At IU this includes faculty, staff, students, affiliates, temporary workers, retired faculty, retired staff and any individuals or entities that use or have authorized access to IU's network. |
| ***Unit:*** | A clinical or non-clinical department within one of IU's Health Science Schools. |
| ***Workforce member:*** | Employees, volunteers, trainees (including students, residents and fellows), and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. |