



# University of Connecticut Health Center

## GLOSSARY

For the purposes of UCHC HIPAA Security Policies, the following terms have been defined.

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

**Access Control** – The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use.

**Access Control Mechanisms** – Hardware, software, or firmware features and operating and management procedures in various combinations designed to permit authorized, and detect and prevent unauthorized access to a computer system.

**Access Rights** – Also called “permissions” or “privileges”, these are the rights granted to users. Access rights determine the actions users have been authorized to perform (e.g., read, write, execute, create and delete).

**Accounting of Disclosures** – See UCHC HIPAA Privacy Policies glossary.

**Administrative Safeguards**- Security measures taken to protect and manage electronic protected health information.

**Application** – A computer program or set of programs that processes records for a specific function.

**Application Controls** – These refer to the transactions and data relating to computer-based applications whose purpose is to ensure the completeness and accuracy of records and the validity of the entries in the records. Applications controls may be manual or programmed, and the records and entries may result from both manual and programmed processing. Examples of application controls include, but are not limited to, data input validation, agreement of batch totals and encryption of data transmitted.

**Audit** – A methodological examination and review of UCHC’s implementation of HIPAA Security Policies and Procedures.

**Authentication** – The corroboration that a person is the one claimed. Authentication is the act of verifying the identity of a user and the user’s eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It also can refer to the verification of the correctness of a piece of data.

**Availability**- Data or information that is accessible and useable upon demand by an authorized person.

**Backup** – Exact copies of files and data, and the necessary equipment and procedures available for use in the event of a failure of applications or loss of data, if the originals are destroyed or systems are not functioning.

**Biometrics**- In computer security, the use of unique characteristics to provide positive personal identification. A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., retinal scan,, fingerprint patterns, and hand written signatures.)

**Business Associate** – A person or organization that performs, or assists in the performance of a function or activity on behalf of a covered entity, any function or activity involving the use or disclosure of ePHI, or any other function or activity regulated by HIPAA, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services of ePHI.

**Business Continuity Plan** – Also known as contingency plan. A document describing how an organization responds to an event to ensure critical business functions continue without unacceptable delay or change.

**Business Continuity Planning** – Business continuity is the ability to maintain the constant availability of critical systems, applications, and information across the enterprise.

**CIO** – Chief Information Officer.

**Confidentiality**-The status accorded to data or information indicating that it is sensitive, and therefore needs to be protected against theft or improper use and is not made available or disclosed to unauthorized persons or processes.

**Covered Entity (CE)** – A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

**Data aggregation**- The collection and analysis of information from different data sources.

**Data Owners** – Individuals employed by UCHC who have been given the responsibility for the integrity, accurate reporting, and use of computerized data.

**De-Identified Data**- A record in which identifying information has been removed.

**Department Manager** – The definition of a department manager by UCHC is the first level outside of a bargaining unit.

**Disaster Recovery Plan** – A documented plan that provides detailed procedures to facilitate recovery of capabilities at an alternate site.

**Disaster Recovery Planning** – Disaster recovery refers to the immediate and temporary restoration of critical computing and network operations after a natural or man-made disaster within defined timeframes. The Disaster Recovery Plan documents how UCHC will respond to a disaster and resume the critical business functions within a predetermined period of time; minimize the amount of loss; and repair, or replace, the primary facility to resume data processing support.

**Electronic Media**-Electronic storage media includes 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. See also Information Technology Resources.

**Electronic Protected Health Information (ePHI)** – Information that is individually identifiable health information that is transmitted by electronic media or maintained in electronic media.

**Encryption** – A technique (algorithmic process) used to transform plain intelligible text by coding the data so it is unintelligible to the reader.

**Firewall**- A dedicated computer equipped with safeguards that acts as a single, more easily defined Internet connection.

**Health Care Clearinghouse** – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value added” networks and switches, that either processes or facilitates the processing of health information.

**HIPAA** – The Health Insurance Portability and Accountability Act of 1996 and the rules and regulations promulgated thereunder.

**Information Security** – Administrative, physical and technical controls that seek to maintain confidentiality, integrity and availability of information.

**Information Technology (IT) Resources** – IT resources are tools that allow access to electronic technological devices, or are electronic technological devices themselves that service information, access information or is the information itself stored electronically. These resources include all computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; peripheral devices such as printers, scanners and cameras; pagers, radios, voice messaging, computer generated facsimile transmissions, copy machines, electronic communication including email and archived messages; electronic and removable media including CD-ROMs, tape, floppy and hard disks; external network access such as the Internet; software, including packaged and internally developed systems and applications; and all information and data stored on UCHC equipment as well as any other equipment or communications that are considered IT resources by UCHC.

**Information Security Officer** – The designated individual responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule.

**IT Information Security-** The unit within the Information Technology Department responsible for overall information security functions for the UCHC. Information security functions include policy administration, security audits and assessments, security tools, security operations, security investigations, security awareness training, and risk management pertaining to the potential loss or unauthorized disclosure of IT resources and electronic information.

**Integrity -** Relevant to computer and system security. A security principle that keeps information from being modified or otherwise corrupted either maliciously or accidentally. Data integrity refers to the accuracy and completeness of the data.

**Limited Data Set -** A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: Names; Postal address information, other than town or city, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; and Full face photographic images and any comparable images.

**Logical Access Control –** The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data.

**Malicious Software –** Software, for example, a virus, designed to damage or disrupt a system.

**Mitigation -** Any action taken to permanently eliminate or reduce the long-term risk to human life, property, and function from hazards.

**Need to Know Principle-** A security principle stating that a user should have access only to the data he or she needs to perform a particular function.

**Password –** A protected, generally computer-encrypted string of characters that authenticate an IT resource user to the IT resource.

**Physical Security-** 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. The measures used to provide physical protection of resources against deliberate and accidental threats.

**Preventive Controls –** Controls designed to prevent or restrict an error, omission or unauthorized intrusion to IT resources.

**Risk -**The aggregate effect of the likelihood of occurrence of a particular threat with the degree of vulnerability to that threat and the potential consequences of the impact to the organization if the threat did occur.

**Risk Analysis** – An assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of IT resources.

**Risk Management** - The process of identifying, measuring, controlling and minimizing or eliminating security risks that may negatively affect information systems.

**Role Based Access-** With Role Based Access Control (RBAC) the attempt is made to map the organization's security policy to a relatively low-level set of technical controls (typically, access control lists) where each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

**Safeguards-** (also called security controls). The protective measure and controls that are prescribed to meet the security requirements specified for systems. Safeguards may include, but are not limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints, ;personnel security; and physical structures, areas, and devices.

**Security Incident** – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

**Security or Security Measures-** Encompass all of the administrative, physical and technical safeguards in an information system.

**Security Policies-**The framework with which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system.

**System Administrator** -A person assigned responsibility for managing, maintaining and ensuring an information system. The person responsible for addressing and managing system functionality, and access to the system.

**Technical Safeguards-**Processes put in place to protect electronic protected health information and control access to it.

**Threat** -An action or event that poses a possible danger to a computer system. The potential for exploitation of a vulnerability.

**Token** -A physical item that is used to provide identity. Typically, an electronic device that can be inserted in a door or a computer system to gain access.

**User** – A person or entity with authorized access.

**Unique User Identifier** – A unique set of characters assigned to an individual for the purpose of identifying and tracking user identity.

**Virus-** Due to industry terminology and widespread use of calling all malicious software a virus, “virus” refers to all malicious software in the context of countermeasure products.

**Vulnerability-**A weakness in a system that can be exploited to violate the system's intended behavior.

**Workforce Member -** Employees (including faculty and staff), volunteers, students and residents, temporary staff, agency and contracted staff, credentialed staff, and members of the Board of Directors, and other persons whose conduct, in the performance of work, is under the direct control of UCHC, whether or not they are paid by UCHC.

**Workstation-** Means an electronic computing device such as a laptop or desktop computer, or any other device that performs similar functions.