

DEFINITIONS

1. *Access* means the ability or the means necessary to read, write, modify, or communicate data or otherwise use any system.
2. *Anti-virus software* means software that detects or prevents malicious software.
3. *Auditable event* means any change to the security state of a system, any attempted or actual violation of the system access control or accountability security policies, or both (e.g., authentication attempts, access of highly sensitive EPHI such as mental health records, information system start up or shutdown, use of privileged accounts such as a system admin account).
4. *Authentication* means the corroboration that a person or entity is the one claimed.
5. *Authorize* means to grant authority or permission.
6. *Availability* means the property that data or information is accessible and useable upon demand by an authorized person.
7. *Backup data* means a retrievable, exact copy of data to be backed up, including applications, operating systems, database software, and other software supporting packages and tools, as well as the contents of databases and files.
8. *Biometric identification system* means a system in which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.
9. *Business associate* means a person or organization that performs a function or activity involving the use or disclosure of protected health information for or on behalf of the covered entity. A person or organization who only assists in the performance of the function or activity is also a business associate. This includes a person or organization that receives PHI *from* the covered entity, and one who obtains PHI *for* the covered entity. This includes, for example: data analysis, processing or administration; web site hosting; utilization review; quality assurance; billing; collections; benefit management; practice management; legal services; actuarial services; accounting and auditing; consulting; management and administrative services; accreditation; financial services; or any other service in which the person or organization obtains PHI from or for the covered entity. Members of the workforce are not considered business associates. The exchange of protected health information between providers of health care, for purposes of providing treatment to a patient, does not create a business associate relationship.
10. *Checksum* means a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it is assumed that the complete transmission was received. This number can be regularly verified to ensure that the data has not been improperly altered.
11. *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.
12. *Context-based* refers to the circumstances, conditions, setting, or environment of the workforce member's employment, e.g., patient records room, benefits office.

13. *Covered component* means those schools or units of New York University as a hybrid entity that, from time to time, are designated by NYU as covered by HIPAA and the HIPAA regulations.
14. *Cryptographic key* means a variable value that is applied using an algorithm to data to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the data.
15. *Cryptography* means encrypting ordinary text into undecipherable text then decrypting the text back into ordinary text.
16. *Data steward* refers to those individuals entrusted with overall responsibility and management of data and information, including electronic data, at the University ("University Data"). Data stewards have decision-making authority related to the development, implementation, and maintenance of policies and procedures related to University Data and may delegate responsibilities as they deem appropriate in specific functional areas.
17. *Data user* refers to individuals responsible for the creation of the data used or stored in organizational computer systems, as well as users of New York University data processing services, such as application software, networks, databases, datastores, and operating systems.
18. *Digital signature* means a cryptographic code that is attached to a piece of data. This code can be regularly verified to ensure that the data has not been improperly altered.
19. *Disaster* means an event that causes harm or damage to New York University information systems or communications network. Disasters include but are not limited to: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.
20. *Electronic communications network* means any series of nodes interconnected by communication paths that are outside (e.g., the Internet) or inside the New York University network. Such networks may interconnect with other networks or contain sub networks.
21. *Electronic media* means:
 - a. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card, computers (i.e., servers, desktops, laptops), Storage Area Networks (SANS), floppy diskettes, backup tapes and cartridges; or
 - b. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.
22. *Electronic Protected Health Information* or *EPHI* means all electronic protected health information that New York University creates, receives, maintains, or transmits that is transmitted by or maintained in electronic media.
23. *Emergency* means a crisis situation.

24. *Encryption* means the conversion of data into secret, unreadable code. To read encrypted data, a person or system must have access to a secret key or password that enables them to decrypt (decode) the data.
25. *EPHI Systems* means all New York University's information systems, repositories, and conduits that contain EPHI.
26. *Erase tool* means hardware or software that is capable of substantially removing all recorded material from electronic media.
27. *Facility* means the physical premises and the interior and exterior of a building(s).
28. *Hash (or hash value)* means a number generated from a string of text. A sender of data generates a hash of the message, encrypts it, and sends it with the message itself. The recipient of the data then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they are the same, there is a very high probability that the message was transmitted intact.
29. *HIPAA Security Regulations* means the regulations published in the Federal Register by the Department of Health and Human Services on February 20, 2003 as the "Health Insurance Reform: Security Standards; Final Rule," as amended or superseded from time to time.
30. *Information system* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
31. *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.
32. *Malicious code* means an executable application (e.g. Java applet or Active X control) designed to damage or disrupt an information system.
33. *Malicious software* means software designed to damage or disrupt an information system, and includes viruses, worms, Trojan Horses, Remote Program Calls, file extensions (e.g., .exe, .vbs, .scr, and .bat), and other malicious code.
34. *Message authentication code* means a one-way hash of a message that is then appended to the message. This is used to verify that the message is not altered between the time the hash is appended and the time it is tested.
35. *Password* means confidential authentication information composed of a string of characters.
36. *Protected health information* means individually identifiable health information, as defined in the Privacy Regulations promulgated pursuant to HIPAA, transmitted or maintained in any form or medium. Protected health information excludes (i) individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, (ii) records described at 20 U.S.C. § 1232g(a)(4)(B)(iv), and (iii) employment records held by New York University in its role as employer.
37. *Restoration* means the retrieving of files previously backed up and returning them to the condition they were at the time of backup.

38. *Re-use* means the use of electronic media containing EPHI for something other than its original purpose.
39. *Risk* means the likelihood that a specific threat will exploit a certain vulnerability, and the resulting impact of that event.
40. *Risk analysis* means a systematic and analytical approach that identifies and assesses risks to the confidentiality, integrity or availability of a covered entity's EPHI. Risk analysis considers all relevant losses that would be expected if specific security measures protecting EPHI were not in place. Relevant losses include losses caused by unauthorized use and disclosure of EPHI and loss of data integrity.
41. *Role-based* refers to the duties and responsibilities of a workforce member in his/her employment, e.g., physician, receptionist.
42. *Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
43. *Security measures* mean security policies, procedures, standards and controls.
44. *Security Officer* means that person designated by New York University responsible for the overall security of NYU's EPHI and EPHI Systems, including development and implementation of policies and procedures relating to HIPAA Security Regulations.
45. *Security token system* means a system in which a small hardware device along with a secret code (e.g., password or PIN) is used to authorize access to an information system.
46. *Threat* means something or someone that can exploit a vulnerability intentionally or accidentally.
47. *Token* means a physical device that together with something that a user knows will enable authorized access to an information system.
48. *Trojan horse* means a program in which malicious or harmful code is contained inside apparently harmless programming or data.
49. *User-based* refers to the specific workforce member who comes in contact with PHI, e.g., any computer user.
50. *Virus* means a piece of code, typically disguised, that causes an unexpected and often undesirable event. Viruses are frequently designed to spread automatically to other computers. They can be transmitted by numerous methods: as e-mail attachments, as downloads, and on floppy disks or CDs.
51. *Vulnerability* means a flaw or weakness in a system security procedure, design, implementation, or weakness in system security procedures, design, implementation, or internal controls that can be exploited by a threat and result in misuse or abuse of EPHI.
52. *Workforce member* means employees, volunteers, and persons other than those deemed business associates 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, and who have access to EPHI. This includes full and part time employees, students, volunteers, and third parties other than those deemed business associates who provide service to the covered entity.

53. *Workstation* means 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.
54. *Worm* means a piece of code, usually disguised, that spreads itself by attacking and copying itself to other machines. Some worms carry destructive payloads that delete files or distribute files; others alter Web pages or launch denial of service attacks.