DEFINITIONS

The following definitions apply to all of NYU patient privacy and security policies and procedures.

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. *Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR 164.402 which compromises the security or privacy of the protected health information.
   (1) Breach excludes:
      (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity (covered or support component) or a business associate, if such acquisition, access, or use was made in good faith and within the course and scope of authority and does not result in further access, use or disclosure in a manner not permitted under 45 CFR 164.402.
      (ii) Any inadvertent disclosure by a person who is otherwise authorized to access protected health information at a covered entity (covered or support component) or business associate to another person authorized to access protected health information at the same covered entity (covered or support component) or business associate, or organized health care arrangement in which the covered entity (covered or support component) participates, and the information received as a result of such disclosure is not further accessed, used or disclosed in a manner not permitted under 45 CFR 164.402 .
      (iii) A disclosure of protected health information where a covered entity (covered or support component) 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.

   (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR 164.402 is presumed to be a breach unless the covered entity (covered or support component) or business associate, as

applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.

10. *Business associate* means a person or organization that creates, receives, maintains, or transmits protected health information in any form or medium, including electronic media, in fulfilling certain functions or activities for a HIPAA-covered entity (covered or support component) and that performs a function or activity involving the use or disclosure of protected health information for or on behalf of the covered entity (covered or support component). 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 (covered or support component), and one who obtains PHI *for* the covered entity (covered or support component). 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 (covered or support component). 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.

11. *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.

12. *Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

13. *Context-based* refers to the circumstances, conditions, setting, or environment of the workforce member's employment, e.g., patient records room, benefits office.

14. *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. The College of Dentistry and the Student Health Center are *covered components*. The NYU School of Medicine also is a *covered component.* The School of Medicine follows HIPAA-related policies and procedures created specifically for their environment; School of Medicine compliance with HIPAA is coordinated through Langone Medical Center.

15. *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.

16. *Cryptography* means encrypting ordinary text into undecipherable text then decrypting the text back into ordinary text.

17. *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.

18. *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.

19. *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.

20. *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.

21. *Discovered breach* means a *breach* is to be treated as discovered by a covered entity (covered or support component) or a *business associate* if any person, other than the individual committing the *breach*, that is an employee, officer or other agent of such entity or *business associate* knows or should reasonably have known of the *breach*. The time period for notification begins to run when the incident becomes known, not when it is determined that a *breach* as defined by the Rule has occurred.

22. *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.

23. *Electronic media* means:
    (1) Electronic storage material on which data is or may be recorded electronically, including, for example, 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
    (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), intranet, 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, if the information being exchanged did not exist in electronic form immediately before the transmission.

24. *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 as defined in the HIPAA Regulations.

25. *Emergency* means a crisis situation.

26. *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.

27. *EPHI Systems* means all New York University's information systems, repositories, and conduits that contain EPHI.

28. *Erase tool* means hardware or software that is capable of substantially removing all recorded material from electronic media.

29. *Facility* means the physical premises and the interior and exterior of a building(s).

30. *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.

31. *HIPAA* means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

32. *HIPAA Omnibus Rule means* the amendments to the *HIPAA Security Regulations* published in the Federal Register on January 25, 2013, entitled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule."

33. *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. These include the Omnibus Rule amendments, published in the Federal Register on January 25, 2013.

34. *HITECH* means the Health Information Technology for Economic and Clinical Health Act, enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

35. *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.

36. *Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.

37. *Malicious code* means an executable application (e.g. Java applet or Active X control) designed to damage or disrupt an information system.

38. *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.

39. *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.

40. *Password* means confidential authentication information composed of a string of characters.

41. *Protected health information* means individually identifiable health information, as defined in the Privacy Regulations (45 C.F.R. Section 160.103(i)) promulgated pursuant to HIPAA, transmitted or maintained in any form or medium. Protected health information excludes individually identifiable health information (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, (ii) in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv), (iii) in employment records held by New York University in its role as employer, and (iv) regarding a person who has been deceased for more than 50 years.

42. *Restoration* means the retrieving of files previously backed up and returning them to the condition they were at the time of backup.

43. *Re-use* means the use of electronic media containing EPHI for something other than its original purpose.

44. *Risk* means the likelihood that a specific threat will exploit a certain vulnerability, and the resulting impact of that event.

45. *Risk analysis* means a systematic and analytical approach that identifies and assesses risks to the confidentiality, integrity or availability of a covered entity's (covered or support component'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.

46. *Role-based* refers to the duties and responsibilities of a workforce member in his/her employment, e.g., physician, receptionist.

47. *Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system that contains or processes PHI.

48. *Security measures* mean security policies, procedures, standards and controls.

49. *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.

50. *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.

51. *Subcontractor* means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

52. *Support component* means the part(s) of the New York University's health component to the extent that the component performs activities that would make it a business associate of a component of the University that performs covered functions, if the two components were separate legal entities. The following are *support components*: Office of the Bursar, Controller's Division, including Accounts Payable, NYU Information Technology (NYU IT), Office of Insurance and Risk Management, Internal Audit, Office of Compliance and Risk Management, Office of General Counsel, Office of Sponsored Programs, University Relations and Public Affairs, Public Safety, Treasury Applications, and University Development and Alumni Relations.

53. *Threat* means something or someone that can exploit a vulnerability intentionally or accidentally.

54. *Token* means a physical device that together with something that a user knows will enable authorized access to an information system.

55. *Trojan horse* means a program in which malicious or harmful code is contained inside apparently harmless programming or data.

56. *Unsecured PHI* means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS in the guidance issued under section 13402(h)(2) of Public Law 111–5.

57. *User-based* refers to the specific workforce member who comes in contact with PHI, e.g., any computer user.

58. *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.

59. *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.

60. *Workforce member* means employees, volunteers, trainees, and persons other than those deemed business associates whose conduct, in the performance of work for a covered entity (covered or support component), is under the direct control of such covered entity (covered or support component), whether or not they are paid by the covered entity (covered or support component), 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 (covered or support component).

61. *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.

62. *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.