HIPAA SECURITY POLICIES
GLOSSARY FOR HIPAA SECURITY POLICY MANUAL

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

2. **Anti-virus software** - means software that detects and attempts to prevent installation of malicious software.

3. **Authentication** - means the corroboration that a person or entity is the one claimed.

4. **Availability** - means the property that data or information is accessible and useable upon demand by an authorized person.

5. **Authorize** - means to grant authority or permission to.

6. **Backup** - means creating a retrievable, exact copy of data stored in an information system.

7. **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.

8. **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. The term 'Breach' excludes:

    a. 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 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.
    b. Any inadvertent disclosure by a person who is otherwise 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 accessed, used or disclosed in a manner not permitted under 45 CFR 164.402.
    c. 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.

    Apart from the exceptions as provided in the paragraphs above 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 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.

9. **Business associate** - means a person or organization that performs a function or activity involving the use or disclosure of protected health information, 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's 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. **Covered entity** – means a health care provider that electronically transmits health information for any of the standardized transactions, a health plan, or a health care clearinghouse. Particular components of the University ((primarily health care provider areas) collectively constitute one covered entity for purposes of compliance with HIPAA. The Employee Health Plan is a distinct, separate covered entity.

13. **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.

14. **Cryptography** - means encrypting ordinary text into undecipherable text (ciphertext) then decrypting the text back into ordinary text (cleartext).

15. **Data custodian** - refers to those who conduct data processing services for the organization's software applications, data, networks, operating systems, etc. Data custodians perform these services on behalf of data stewards.

16. **Data steward** - refers to individuals with ultimate responsibility for the creation of the data used or stored in organizational information (computer) systems. Examples of data stewards are Senior Clinical Administrators (SCA) and Department or Business Unit heads i.e. the System Owners.This individual has overall and final responsibility for the information system.

17. **Data user** - means any individual who accesses data used or stored in organizational computer systems.

18. **Decryption** - refers to the process of converting encrypted data back into its original form, so it can be understood. See Encryption.

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 University of Miami information systems. Disasters include but are not limited to: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.

21. **Disclosure** - means the release, transfer, provision of, access to, or divulging in any other manner of protected health information (PHI) outside the covered entity holding the information.

22. **Electronic communications network** - means any series of nodes (electronic devices on the network) interconnected by communication paths which facilitate the transmission of data (e.g., the Internet). Such networks may interconnect with other networks or contain sub networks.

23. **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; or

    b. **Transmission media** used to exchange information already in electronic storage media.
        i. 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.

24. **Electronic protected health information** (EPHI) - individually identifiable health information that is:
    - Transmitted by electronic media
    - Maintained in electronic media

    See also Protected Health Information (PHI).

25. **Email**: The common term for "electronic mail", a method for writing, sending and receiving electronic text (and audio and/or video) over a computer network. A variation of email popular with mobile telephone users is the Short Messaging Service (SMS). Email differs to other messaging systems in that it is asynchronous in nature.

26. **Emergency** - means a crisis situation.

27. **Encryption** - means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key. In other words, encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized individuals.

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

29. **ESIRT** -means Enterprise Security Incident Response Team.

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

31. **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.

32. **Health care** – means care, services, or supplies related to the health of a patient. It includes, but is not limited to (1) 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 a patient or that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

33. **Health care clearinghouse** – means a public or private entity that either: (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; or (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.

34. **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.

35. **Information system owner** – see Data Steward.

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

37. **Keylogger** - A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via email).

38. **LSIRT** -means Local Security Incident Response Team. E.g. a business unit or dept. may have a "local" team composed of individuals within that unit/dept. which responds to security incidents on information systems under the control of that particular unit/dept.

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

40. **Malicious software** - means software, for example, a virus, designed to damage or disrupt an information system.

41. **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.

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

43. **Privacy rule** – means the federal privacy regulations issued pursuant to HIPAA and codified at 45C.F.R. parts 160 and 164, as amended from time to time.

44. **Protected health information or patient information** – means information transmitted or maintained in any form that is created or received by a health care provider, health plan, health are clearinghouse, or employer and: (1) relates to the past, present, or future physical or mental health or condition of a patient, the provision of health care to a patient, or the past, present, or future payment for the provision of health care to a patient; and (2) identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient. It does not include certain education records, health information of students, or employment records held by a covered entity in its capacity as an employer.

45. **Psychotherapy notes** – means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the patient's medical record. It excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

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

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

48. **Risk** - means the likelihood that a specific threat will exploit a certain vulnerability, as well as the resulting impact of that event.

49. **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 are not in place. Relevant losses include losses caused by unauthorized use, disclosure of EPHI and loss of data integrity.

50. **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.

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

52. **51. 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.

53. **SPAM**: Unsolicited bulk email, normally sent for a commercial or fraudulent purpose. SPAM is an effective means of advertising as the costs of distribution of SPAM email is very low. Thus even with a very low success rate, "Spammers" can afford to send millions of emails to generate a few positive responses.

54. **Spyware -** A general term for a class of software that monitors the actions of a computer user. This software falls into a number of categories: Software that may be installed legitimately to provide security or workplace monitoring, software with relatively benign purposes that may be associated with marketing data collection and software that is maliciously installed, either as a general violation of a user's privacy or to collect information to allow further attacks on their computer or online transactions (e.g. "keylogging" to gain passwords).

55. **Threat** - means something or someone that can intentionally or accidentally exploit vulnerability in an information system.

56. **Token** - means a physical device, which together with something that a user knows (for example a PIN or password), will enable authorized access to an information system.

57. **Treatment** –means 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.

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

59. **University or the University** –means the University of Miami health care component, as described in the HIPAA Privacy Policies.

60. **Unsecured PHI** – means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the secretary of HHS.

61. **Use** –means the sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains such information.

62. **Virus** - means a piece of code, typically disguised, that causes an unexpected and often undesirable event. Viruses are frequently designed to automatically spread to other computers. They can be transmitted by numerous methods: as e-mail attachments, as downloads, and on floppy disks or CDs.

63. **Vulnerability** - means a flaw 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.

64. **Workforce member** - means employees, volunteers, medical staff, faculty and other persons whose conduct, in the performance of work for the covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part-time employees, affiliates, associates, volunteers and students who have access to PHI in order to satisfy a clinical experience requirement for a program of study.

65. **Workstation** - means an electronic computing device, for example, a laptop or desktop computer, or any other device (e.g. Smart phone, tablet) that has the ability to perform similar functions with local processing capabilities as well as the ability to connect to networks and systems. This can include electronic media connected in the immediate vicinity of the workstation.

66. **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.