

## **Definitions (Revised 11/16/2011):**

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

**Anti-virus software** means software that detects or prevents malicious software.

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

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

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

**Confidential Information** includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

**Data custodian** refers to those who conduct data processing services for the organization's software applications, data, networks, operating systems, etc.

**Disaster** means an event that causes harm or damage to information systems. Disasters include but are not limited to: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.

**Disclosure** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

**Electronic media** means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as CD-ROM, DVD, floppy disks, magnetic tape or disk, optical disk, or digital memory card; 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), 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.

**Electronic Protected Health Information** means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

**Electronic signature** is an electronic sound, symbol, or process attached to or logically associated with an electronic record or document and executed or adopted by a person with the intent to sign a record or document.

**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.

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

**Information system owner** means the workforce member(s) with overall or final responsibility for an information system.

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

**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.

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

**Mobile devices** are defined as Personal Digital Assistants (PDAs), tablets, cellular phones, text pagers, laptop computers, and any other types of mobile devices or media that receive, record or store information and data.

## **Network**

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

**Pre-Research or Review Preparatory to Research** means the review of information or records prior to obtaining patient authorization and consent or prior to obtaining an IRB Waiver of Authorization in which the review is solely to prepare a research protocol, to determine if a research project is feasible, or for similar purposes preparatory to research.

**Protected Health Information (PHI)** means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted

in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

**Required by Law** means a mandate contained in law that compels UAMS to make a use or disclosure of information and that is enforceable in a court of law. “Required by Law” includes, but is not limited to, court orders and court-ordered warrants, grand jury subpoenas, a governmental or administrative body authorized by law to require the production of the information being sought, Medicare or Medicaid conditions of participation, and statutes or regulations that require the production of the information. “Required by Law” does not mean a subpoena issued or signed by a non-governmental attorney. See UAMS Use and Disclosure Policy 3.1.28 for more information regarding subpoenas.

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

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

**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 and disclosure of ePHI and loss of data integrity.

**Risk** means the likelihood of a given threat exercising a particular vulnerability and the resulting impact of that event.

**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.

**Security measures** means security policies, procedures, standards and controls.

**spam** - The term spam refers broadly to unsolicited bulk e-mail (or junk e-mail), which can be either commercial (such as an advertisement) or noncommercial (such as a joke, chain letter, or Trojan virus).

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

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

**UAMS workforce** means for the purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

**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.

**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.

**Workforce member** means employees, volunteers, 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. This includes full and part time employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the covered entity.

**Workstation** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and the electronic media in its immediate environment.

**Worm** means a piece of code, usually disguised, that spread 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.