Definitions (Revised May 21, 2014):

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.

Cloud Computing-is a method of delivering data storage capacity and computing resources to a large community of end recipients. End users access cloud services through web browsers, mobile applications and desktop clients. A user's data and computing resources are stored on a server at a remote location, and the user must rely on the remote enterprise's privacy, security and disaster recovery protocols. Examples of cloud computing applications are Drop Box, Google Docs and iCloud.

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 and student information, information concerning 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. Confidential Information includes information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

Data custodians are individuals who have the primary responsibility for the accuracy, privacy, and security of the UAMS Data under their purview, providing specific data management and maintenance responsibilities.

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

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons outside of UAMS or outside the covered components of the UAMS hybrid entity.

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 cards and flash drives; 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 (ePHI) means individually identifiable health information that is:

- Transmitted/Received 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. The encryption mechanism must be FIPS 140-2 validated.

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

Hybrid Entity is an organization with both Covered and Noncovered components under HIPAA.

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(s) 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.

Legal Representative means the person authorized by law to act on behalf of the patient, such as the parent of a minor, a court-appointed guardian or a person appointed by the patient in a Power of Attorney document.

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 such as USB flash drives and memory cards, CD-ROMS and DVDs, digital cameras and portable hard drives.

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

Photography means, for purposes of this policy, a recording of a patient's likeness, even if the patient's face is not included, by a number of visual means, including still photography, videography, digital imaging, scans, and others. Photography does not mean radiological images such as X-rays and MRI.

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.

Privacy Board is a review body that may be established to act upon requests for a waiver or an alteration of the Authorization requirement under the Privacy Rule for uses and disclosures of PHI for a particular research study. At UAMS, the IRB serves as the Privacy Board.

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 and health information regarding a person who has been deceased for more than 50 years.

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. For purposes of compliance with HIPAA, "Required by Law" does not automatically include a subpoena issued or signed by a non-governmental entity since certain subpoenas require that a signed HIPAA Authorization accompany the subpoena. See UAMS Use and Disclosure Policy 3.1.28 for more information regarding compliance with subpoenas and persons who are authorized to sign a HIPAA Authorization.

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 mean security policies, procedures, standards and controls.

Social Networking (also known as social media) is a means of public and private Internet communication that moves beyond legacy interaction methods such as e-mail and Internet Relay Chat (IRC). Social networking allows for real time interactive dialoguing among groups of end users utilizing text, images and video. The privacy and security of what is shared or transmitted is the responsibility of the end user. Examples of Social Networking applications are Facebook, Twitter, Skype, LinkedIn and Pinterest.

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).

Student Shadower means an individual interested in pursuing a career in the healthcare field, who (a) has completed the training and forms required by this policy, (2) has been approved by a Department, and (3) has been assigned an employee or Faculty member to shadow. Student Shadower does not include students enrolled in an academic program at UAMS, volunteers, patients, or family members or friends visiting or accompanying patients. Student Shadower does not include any health care provider, such as a visiting nurse or physician, regardless of their credentials.

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

Treatment is providing, coordinating or managing health care and related services by one or more providers, including such coordination or management by a provider with a third party; consultation between providers relating to a patient or the referral of a patient for health care from one provider to another.

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

UAMS Workforce means for the purpose of this Policy, physicians, employees, volunteers, resident/fellows, students 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.

Unsecured Protected Health Information (PHI) means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology.

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.

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.