NUMBER: 2.1.33 **DATE:** 04/30/2002
REVISION: 10/05/2011; 08/07/2013; 07/10/2019; 05/09/2023 **PAGE:** 1 of 2

SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: GENERIC ACCOUNTS

PURPOSE

To establish provisions for the creation and management of Generic Accounts on IT workstations, the provision of Generic Access to information systems, and to ensure that proper security methodology is followed at the University of Arkansas for Medical Sciences ("UAMS").

SCOPE

The UAMS Workforce.

DEFINITIONS

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.

Electronic Protected Health Information (ePHI) means individually identifiable health information that is:

- Transmitted by Electronic Media
- Maintained in Electronic Media

Generic Accounts, **Generic Access**, generic identification, generic logon terms refer to definition and implementation of user authentication information (such as user ids and passwords) and procedures which are designed so that they do NOT require specific information associated with a unique individual but accept some nonspecific identification information to enable access.

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.

To access any other terms or definitions referenced in this policy:
https://hipaa.uams.edu/wp-content/uploads/sites/136/2019/02/DEFINITIONS-HIPAA.pdf

POLICY

UAMS will allow Generic Accounts to be utilized on certain workstations and devices on the UAMS network within the parameters set forth by the following procedures.

PROCEDURE

(1) Generic Accounts may be utilized by UAMS in cases where multiple users must access one workstation to perform given duties.
(2) Generic Access to workstations should occur only in protected areas where public access is supervised and/or restricted.
(3) Generic Accounts will not require users to sign in and out of Microsoft Windows and may allow unrestricted access to Intranet resources and non-patient applications and products as needed.
(4) Requests for Generic Accounts will be reviewed and approved or disapproved as appropriate by the IT Security Office. Such reviews will take into account the area where the Generic Account requested will be used to ensure appropriate physical safeguards are in place.
(5) Generic Accounts will be audited regularly for appropriateness of access and ongoing need.
(6) All clinical and patient care applications containing PHI installed on generic workstations will be accessed through non-generic, individually password protected logons.
(7) Confidential Information, including PHI, must never be stored on a generic workstation.
(8) These above procedures may not apply to publicly accessible library workstations (which will be implemented on a virtual LAN) or to other workstations where a clear need can be defined and other security methods are implemented, such as logging of access and changing of passwords. Internet access may be available from generic logons on these workstations.

SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with UAMS Administrative Guide Policy 4.4.02, *Employee Discipline* and UAMS Administrative Guide Policy 2.1.42, *HIPAA Sanctions Policy*.

Signature:  **Date:** **May 9, 2023**