SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: PHISHING AND FRAUD

PURPOSE

To promote the UAMS mission (education, patient care, research, and outreach) by implementing procedures to assure the protection of staff, faculty, students, and patients from fraudulent activities.

SCOPE

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.

Phishing is the attempt by criminals to acquire sensitive information (such as usernames, and passwords or credit card, social security or bank account numbers) from Internet users by pretending to be trusted entity or business (such as a UAMS department), and then use the information to steal business or personal income or data, access financial accounts or infect computers with viruses or malware.

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, 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.

UAMS Workforce means for the purpose of this Policy, physicians, employees, volunteers, residents, students, trainees, visiting faculty, 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.

Other terms or definitions referenced in this policy are available on the UAMS HIPAA Office website at hipaa.uams.edu.

POLICY

Phishing is the leading method to get to UAMS Confidential Information, circumventing all other protections. UAMS will not be held responsible for Workforce members who release Confidential Information in response to a Phishing scheme delivered through the UAMS email system, smart phone text messages, phone calls, or any other technology or from face-to-face scam artists. Each Workforce member will be responsible for any personal financial loss incurred (including wages or salaries earned at UAMS) as a result of providing Confidential Information in response to a Phishing scheme. If an employee's response to a Phishing scheme results in a breach of PHI, the employee will be subject to disciplinary action under the UAMS HIPAA policies.

PROCEDURE:

Annual Training

Each Workforce member must complete an annual training reminder about Phishing and other malware, the consequences of succumbing to such, and other pertinent security controls as necessary. The training reminder will come by email notification annually and be recorded in the appropriate system. Those who do not complete the training within 90 days will face disciplinary action from UAMS Human Resources.

Technical Protections

Phishing scams have similar signs: Misspellings (although not always), generic or no greetings, urgent appeals, account status issues, fake or spoofed web links, and requests for personal or business information. The criminals try to appeal to basic human nature, focusing on matters of trust, life, and curiosity. UAMS IT will provide technical processes and systems to prevent/block the majority of Phishing and malware attacks.

- SPAM and malware filters will be utilized on the email servers to prevent the majority of attacks.
- UAMS Workforce members must report Phishing or malware immediately when receiving it to the UAMS Technical Support Center at (501)686-8555.
- Countries and organizations that spawn huge amounts of SPAM and malware will be blocked and whitelists created for legitimate communications.
- Certain email attachments that are utilized to install malware will be queued and manually verified before release to the recipient.

MISCELLANEOUS:

Questions. Any questions about this policy should be directed to UAMS Compliance or IT Security.

Protect Your Personal Information and UAMS Confidential Information. Go to the following link to learn steps you can take to prevent Phishing.
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

SANCTIONS

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

REFERENCE

1) Administrative Guide Policy 2.1.31, Email Access and Usage
2) Administrative Guide Policy 2.1.02, Mobile Device Management
3) Administrative Guide Policy 2.1.01, Confidentiality policy
4) Administrative Guide Policy 2.1.23, Safeguarding Protected Health Information
5) Administrative Guide Policy 2.1.32, IT Security Incident Identification and Handling Policy

Signature:  **Date: February 23, 2024**