University of Arkansas for Medical Sciences

UAMS ADMINISTRATIVE GUIDE

NUMBER: 2.1.32 **DATE: 02/02/2002**
REVISION: 11/06/2008; 02/28/2011; 03/06/2013; 01/06/2016; 04/28/2021; 03/11/2024 **PAGE: 1 of 5**

SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: IT SECURITY INCIDENT IDENTIFICATION & HANDLING POLICY

PURPOSE

To establish and outline the University of Arkansas for Medical Sciences ("UAMS") procedures designed to protect the integrity, availability and confidentiality of Confidential Information, including ePHI, to prevent loss of service, and to comply with applicable legal requirements.

SCOPE

The UAMS workforce.

DEFINITIONS

UAMS Workforce shall mean 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.

IT Security Incident shall mean any activity that harms or represents a threat to the whole or part of UAMS's computer and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, software or data, unauthorized exposure, change or deletion of ePHI or non-public personal information, or a crime or natural disaster that destroys access to or control of these resources. IT Security Incident includes the loss of ePHI or non-public personal information through the theft or loss of a mobile device (including but not limited to laptop computer, smartphone, tablet, external disk drive, CD-RW, and USB flash drive), compromised UAMS logon credentials resulting from phishing scams or negligent sharing of passwords, and direct attacks by cyber hackers to infiltrate or damage data stores.

Go to the UAMS HIPAA Office website at hipaa.uams.edu to access any other terms or definitions referenced in this policy.

POLICY

UAMS IT Security deploys automated scanning, endpoint detection and response software, anti-virus software, log file analyzers, and other tools to help identify, respond, and address security incidents. These tools are intended to identify, respond and address IT Security Incidents in a timely manner. The timeliness to identify, respond, and address IT Security Incidents depends on several factors, such as the type of IT Security Incident, the criticality of the resources and data that are affected, the severity of the IT Security Incident, the time and day of the week, and other IT Security Incidents being handled. Generally, the highest priority is identifying, responding to, and addressing IT Security Incidents that are likely to cause the most damage to UAMS or to other organizations. (See Reference Section)

PROCEDURES

UAMS IT Security will identify, address, and respond to IT Security Incidents in accordance with the procedures set forth below. Such procedures are consistent with best practices, recommendations and guidelines set forth in the NIST publication referenced below.

A. Reporting IT Security Incidents – Intrusions or Vulnerabilities

Each user of UAMS computing and information systems has a responsibility to report IT Security Incidents or violations of UAMS IT Security policies. All IT Security Incidents will be reported to the IT Security Team as soon as an incident comes to the attention of the user or it is identified by automated tools. Any IT Security Incident should be immediately reported to IT Security at (501) 686-8555.

B. Handling IT Security Incidents

The IT Security – Technical team will oversee the handling of all IT Security Incidents. UAMS IT Security will respond to IT Security Incidents by performing analysis of systems in question to validate the incident in a timely manner. IT Security – Technical team shall perform scans of the UAMS network to test for and identify any potential vulnerability (virus, external intrusion or hacker attack, broadcast storm, etc.) present on workstations, servers, and other networked devices, taking into consideration the operational functions and number of end users affected.

1. If a potential vulnerability is identified, the IT Security – Technical team shall notify the appropriate person(s) via phone and/or email. Depending upon the nature and severity of the incident, a follow-up to the event may be performed.

2. Any IT Security Incident identified as having taken place on the UAMS campus shall be classified as one of the following severity levels and the corresponding actions taken:

   - **Level 1 (Critical):** Device is infected, compromised, or a high-risk vulnerability is detected, or a chance credentials have been compromised
   - **Action:** Device will be removed from the network and repaired (see below), and extended notification procedures implemented
   - **Level 2 (Warning):** Medium risk vulnerability detected
   - **Action:** Device must be corrected or disconnected from the network within 72-hours
   - **Level 3 (Information):** Low risk vulnerability detected
   - **Action:** Notification only, updates are optional

3. If a Level 1 IT Security Incident (Critical) occurs on the UAMS network:

    - Device will be removed from the network and repaired, as may be possible.
    - All identified Network Administrators or backup personnel will be informed of the incident.
    - The UAMS Technical Support Center ("TSC") will be informed of the incident and advised as to its impact upon personnel and equipment attached to the UAMS network. The TSC shall also be instructed on what steps to take and how to inform users to lessen the impact of the incident.
    - If the incident could potentially involve ePHI, the UAMS HIPAA Campus Coordinator and HIPAA Security Officer will be notified immediately and an Incident Response Committee will be established as an advisory committee to the UAMS HIPAA Campus Coordinator. The Incident Response Committee will include as necessary, key representatives of UAMS IT, administrators of affected schools and hospital, Campus Police, General Counsel, and Communications and Marketing.
    - Incidents involving the possible loss of user logon credentials will follow the extended notification procedures, notifying appropriate departments or staff by direct email and phone when appropriate.

4. Network, workstations, servers, and/or networked devices may be removed from the network, if required to protect the integrity of the network, until the threat has been removed from the device. Under no circumstances shall the device be reconnected until the threat has been eliminated unless reconnection is approved by the Assistant Vice Chancellor for Technical Operations/UAMS Chief Technology Officer ("CTO") or the Associate Vice Chancellor for Information Services/UAMS Chief Information Officer ("CIO"). They may be contacted with Priority 1 call to the UAMS Help Desk at 501-686-8555. Any personally owned devices, such as tablets, smart phones, wireless devices, or other electronic transmitters which have been used to store or access ePHI or non-public personal information and are determined to contribute to an IT Security Incident, may be subject to seizure and retention by UAMS until the IT Security Incident has been remediated, unless the custody of these devices is required as evidence for a court case.

5. Appropriate local, state, and federal law enforcement agencies, regulatory agencies and oversight agencies will be notified of the IT Security Incident as may be required by law. Appropriate logs and notes will be submitted to such agencies in accordance with applicable laws, rules, and regulations. It will be the decision of the UAMS HIPAA Campus Coordinator, with the advice of the Incident Response Committee, to notify law enforcement and/or regulatory and oversight agencies if the data involves ePHI.

6. If required by law, individuals affected by the IT Security Incident will be notified. The HIPAA Campus Coordinator, with the advice of the Incident Response Committee, will determine whether notification is required for IT Security Incidents involving ePHI, and will coordinate notification of affected individuals. For notification of individuals other than when ePHI is involved, the system owner shall be responsible for notification.

7. All communications with the media regarding the IT Security Incident involving ePHI will require coordination with the HIPAA Campus Coordinator, who will consult with the Incident Response Committee. Communications and Marketing will communicate directly with the media.
8. When applicable, other organizations and entities outside of UAMS shall be notified to take appropriate precautionary or remedial steps.

9. All IT individuals involved with the IT Security Incident shall keep a log from start to finish of their own activities involved in remedying the situation. These logs shall be audited and maintained by IT Security as may be necessary. All network related IT Security Incidents may be reviewed with the appropriate committee in accordance with the duties and responsibilities of such committee. All potential evidence related to the IT Security Incident and all IT Security Incident reports will be retained by IT Security for a minimum of six years for those IT Security Incidents involving PHI and one year for all others.

C. Request for Investigation by IT Security

1. Departments, division, offices and other areas may request that IT Security conduct an investigation to resolve or collect evidence of employee non-compliance with UAMS policies, and/or state, local, or federal laws, rules or regulations. As a result of such an investigation, IT Security may identify an IT Security Incident. Such requests are made by contacting the UAMS Help Desk at 501-686-8555 or helpdesk@uams.edu. Division level approval is required before any action is taken by IT Security to monitor, collect or report on any employee's internet usage, local profile, or email. Additional procedures must be followed to access and monitor electronic communications, such as emails, of others. See Administrative Guide Policy 2.1.31, *Email Access and Usage.*

2. Network bandwidth monitoring is an exception to the general procedure above. The bandwidth usage at UAMS will be monitored by the IT Security – Technical team through the use of an automated process that creates a top twenty (20) list of high usage workstations. Workstations on this list are reviewed periodically to verify the legitimacy of the high bandwidth usage in relation to appropriate UAMS business use. When the high bandwidth usage is found to be non-compliant, a report including the user information is made to the CIO who distributes it to the proper division level officer for distribution to lower management to use in any necessary employee discipline. The primary purpose of this procedure is to ensure that there is enough bandwidth for mission critical applications at UAMS.

D. Sanction

Violation of this policy will result in disciplinary action as set forth in the Administrative Guide Policy 4.4.02, Employee Discipline, and Administrative Guide Policy 2.1.42, HIPAA Sanctions Policy.

REFERENCES

National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-61, Revision 2 for best practices regarding identifying, responding to, and addressing IT Security Incidents.

Signature: __________________ **Date: March 11, 2024**