PURPOSE

To inform departments within the University of Arkansas for Medical Sciences ("UAMS") of the procedure to be followed while accessing and using e-mail.

SCOPE

This policy applies to all use of electronic mail systems within UAMS where the mail either originated from or is forwarded to the UAMS computer network. It applies to all e-mail users including, but not limited to, faculty, staff, students, volunteers, and official visitors if UAMS information is involved regardless whether UAMS computer resources are used or not.

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.

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.

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

POLICY

UAMS shall provide email services to UAMS faculty, employees, students, contract personnel, vendors, volunteers, and official visitors for the express purpose of conducting UAMS business.

Use of UAMS email services must be consistent with UAMS's mission and comply with local, state and federal laws and university policies.

PROCEDURES

A. PRIVACY, CONFIDENTIALITY AND PUBLIC RECORDS CONSIDERATIONS

The UAMS electronic mail (e-mail) system is available to authorized users for the expressed purpose of conducting UAMS business. Reasonable efforts will be made to maintain the integrity and effective operation of its electronic mail systems (e-mail), but users are advised that those systems should not be regarded as a secure medium for the communication of sensitive or Confidential Information. Any e-mails sent outside of the UAMS network containing Confidential Information, including ePHI, must be encrypted. Refer to Section D below.

B. PERMISSIBLE USES OF ELECTRONIC MAIL

1. Authorized Users: Only UAMS faculty, staff, and students and other persons who have received permission under the appropriate UAMS authority are authorized users of UAMS electronic mail systems and resources.
2. Purpose of Use: The express purpose of UAMS electronic mail resources is for UAMS business, including academic, clinical and research pursuits.

C. PROHIBITED USES

E-mail is the property of UAMS. Prohibited uses of electronic mail include, but are not limited to:

1. Using for personal monetary gain or for commercial purposes that are not directly related to UAMS business.
2. Sending copies of documents in violation of copyright laws.
3. Including the work of others in electronic mail communications in violation of copyright laws.
4. Unapproved capturing or opening of another individual's electronic mail except as required as part of assigned job duties for authorized employees to diagnose and correct delivery problems.
5. Using electronic mail to harass or intimidate others or to interfere with the ability of others to conduct University business (this includes inappropriate or offensive content, chain-letters and/or "spamming" - sending non-approved / non-solicited advertisements to other individuals on campus.)
6. Using electronic mail systems for any purpose restricted or prohibited by state and federal laws and regulations or by UAMS Policy.
7. Using your UAMS email for communication on social media, dating, and sites considered to be obscene or indecent.
8. "Spoofing" - constructing an electronic mail communication so it appears to be from someone else.

9. Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.
10. Broadcasting messages to "Everyone" within UAMS without prior permission from the UAMS e-mail administrator (see Section I below).
11. Using custom backgrounds, special formats, or colors within your email. Refrain from this practice and use plain, white backgrounds and professional formats. The only exceptions to this are special emails crafted to be official UAMS business invitations, announcements, advertisements, or pamphlets.
12. Use of quotations or sayings within your message or signature block. This practice has great potential to offend so quotations must not be used and any that exist must be removed. Again, the exceptions would be special official UAMS business emails crafted for specific purpose.

D. CONFIDENTIAL INFORMATION AND ePHI IN E-MAILS/ELECTRONIC COMMUNICATIONS

1. E-mail is secured automatically inside the UAMS network. Any e-mails sent outside of the UAMS network containing Confidential Information, including ePHI, must be encrypted.

    a. The UAMS workforce may utilize encryption methods of their own choosing.
    b. It is recommended that the UAMS workforce utilize the enterprise secure e-mail gateway solution.

        (1) This is easily accomplished by clicking on the "mark secure" button provided on the standard toolbar in Outlook, or
        (2) The word [secure] typed with the brackets into the subject line will also encrypt the message
        (3) Communication with other organizations in many cases will be set up for automatic encryption and a list of these organizations will be provided.

2. The patient's e-mail address is part of the patient's Protected Health Information and must be protected as any other PHI in accordance with all applicable laws, regulations and UAMS policies.
3. For PHI that is subject to the minimum necessary requirements of the HIPAA regulations, reasonable efforts must be made to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. *Administrative Guide Policy 2.1.10, Minimum Necessary Policy*
4. UAMS takes the steps necessary to make sure that your e-mail and other computer messages are secure, but no one can guarantee the security and privacy of e-mail messages. Therefore, it is best not to use e-mail to send highly sensitive information.

5. Confirm the e-mail address before sending any e-mail containing Confidential Information or ePHI.
6. Caution must be taken when using distribution lists or forwarding e-mails that contain Confidential Information and ePHI.
7. UAMS e-mail may not be auto-forwarded to any non-UAMS account, including but not limited to personal and commercial e-mail accounts such as Gmail, Yahoo, iCloud, or MSN, with the exception that UAMS e-mail may be auto-forwarded to VA and Arkansas Children's Hospital e-mail accounts.
8. ePHI contained within the content or in attachments of UAMS email should be deleted after use especially in the case of larger attachments containing multiple patients' PHI.

E. PROVIDER COMMUNICATIONS WITH PATIENTS VIA E-MAIL

1. The decision to correspond with patients via e-mail is left to the discretion of the physician or clinic. It is the responsibility of the clinic to determine additional e-mail communication guidelines, such as (a) how often e-mail will be checked; (b) instructions for when and how to escalate to phone calls and office visits; and (c) the types of transactions that are appropriate for e-mail.
2. Any ePHI originated by UAMS must be encrypted when being sent via e-mail.
3. UAMS takes the steps necessary to secure e-mail and other computer messages, but no one can guarantee the security and privacy of e-mail messages. Use caution when sending highly sensitive information.
4. E-mail communication is a convenience for the patients and should not be used for emergencies or time-sensitive situations.
5. Keep in mind that the patient's e-mail address is part of the patient's Protected Health Information and must be protected as any other PHI in accordance with all applicable laws, regulations and UAMS policies.
6. Before sending the e-mail containing Confidential Information or ePHI, confirm the e-mail address to ensure it does not contain any typographical errors.
7. E-mail messages must include (a) information in the subject line, such as prescription refill, appointment request or other information generally describing the purpose of the e-mail; and (b) patient name, telephone number and patient identification number in the body of the message.
8. Clinically relevant messages and responses will be documented in the patient's medical record.
9. Upon a patient's receipt of e-mail, patients will be provided guidelines of using e-mail for communicating with their provider.

F. UAMS ACCESS AND DISCLOSURE OF COMMUNICATIONS

To the extent permitted by law, UAMS reserves the right to access and disclose the contents of faculty, staff, students, and other users' electronic mail without the consent of the user. UAMS will do so when it believes it has a legitimate business need including, but not limited to, those listed in section F 6. (below), and only after explicit authorization is obtained from the appropriate UAMS authority (see Section G below).

1. Faculty, staff, and other non-student users are advised that UAMS' electronic mail systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on UAMS business or with the use of UAMS resources may be made available for review by any authorized UAMS official for purposes related to UAMS business.
2. Electronic mail of students may constitute "education records" subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). UAMS may access, inspect, and disclose such records under conditions that are set forth in the statute.
3. Any user of UAMS electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate UAMS authority.
4. UAMS will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law as UAMS deems necessary for purposes of maintaining the integrity and effective operation of UAMS electronic mail systems.
5. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring: To the extent permitted by law, the contents of electronic mail communications, properly obtained for UAMS purposes, may be disclosed without permission of the user. UAMS will attempt to limit disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation. Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail Communications: Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must obtain approval in advance of such activity from the appropriate UAMS authority. The request for approval shall take into consideration ways to minimize the time and effort required to submit and respond to requests, the need to minimize interference with UAMS business, and protection of the rights of individuals. The request for granting access to electronic communications is provided in Section L below.
6. UAMS will inspect and disclose the contents of electronic mail in accordance with the established approval process (see section G below). Such action will be taken as necessary; to include:

    a. To respond to legal processes or fulfill UAMS obligations to third parties,
    b. in the course of an investigation triggered by indications of misconduct or misuse,
    c. as needed to protect health and safety,
    d. as needed to prevent interference with the academic, clinical or research missions of the organization,
    e. as needed to locate substantive information required for UAMS business, or
    f. as required under the Arkansas Freedom of Information Act.

G. PROCEDURE FOR GRANTING APPROVAL TO ACCESS ELECTRONIC COMMUNICATIONS OF OTHERS

1. The following information will be required prior to approval of access to electronic communications addressed to others:

    a. Name and title of the person whose communications will be accessed;
    b. Name and title of the person who is requesting access;
    c. Name and title of the person who will do the accessing;
    d. Detailed description of why the access is needed;
    e. Required duration of the access or dates within which access is desired;
    f. What will be done with the accessed messages? With whom will they be shared?

2. Anyone may request access of messages through the UAMS Technical Support Center. The following approvals are required.

    a. Department Chairpersons and Unit Directors are the first level of approval;
    b. Deans or Vice Chancellors are the final level of approval.

3. The IT Security Office will obtain appropriate approval and will maintain copies of all requests.

4. The person requesting the access will be given the following advice and reminders:

    a. A reminder that concerns about fiscal misconduct or criminal activity should not be investigated by individuals or departments but should be referred to University Police, Hospital Compliance, or Internal Audit staff.
    b. A reminder that to the extent permitted by law, the contents of electronic communications obtained after appropriate authorization may be disclosed without the permission of the employee. At the same time, UAMS will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

H. RETENTION & STORAGE OF E-MAIL

UAMS utilizes a hosted email solution from Microsoft that ensures email services will be highly available. Specific emails are not able to be recovered once deleted.

I. E-MAIL ARCHIVE

The UAMS hosted email system includes services designed for archiving email. Retrieval of this archived email can be done through Microsoft Outlook version 2016, 2019, or M365 Apps for Enterprise as well as through Outlook on the web. Mailbox folders are set, by default, to delete email older than 6 months from the Inbox, per the UAMS 3.2.01 Record

Retention policy. Users must manage their email, moving what needs to be saved to other folders or to the individual's Archive Mailbox. UAMS email based archive application is to be used for long term storage of email in accordance with the policies and procedures contained within this document.

J. E-MAIL SITE MESSAGES

Site messaging is a tool used for campus e-mail alerts and notifications that are directed to the entire campus or a select group (i.e., Department Heads, Business Managers). These notifications are restricted and may ONLY be sent by the e-mail administrator. Messages must also have prior approval before delivery of the site message is transmitted by the e-mail system. To request sending of a site message:

1. The party requesting an e-mail site message should contact the UAMS IT Technical Support Center (TSC) by calling (501) 686-8555 or sending an e-mail message to 'Tech Support Center' utilizing the "Campus-Wide Email Request" web site http://intranet.uams.edu/announcements.htm
2. Except in emergency situations, the requested Site Message text must be received by the UAMS Technical Support Center no later than two days prior to the requested send event.
3. Technical Support Center logs the call and assigns call to Communications and Marketing.
4. Communications and Marketing will contact requesting party for verification of message and targeted individuals or group.
5. Communications and Marketing formats messages and forwards to the IT Enterprise Operations Unified Communications group.

    a. Non-UAMS function announcements will not be approved.
    b. Emergency site messages are processed by the IT EO Unified Communications group.

K. E-MAIL ETIQUETTE

When you send e-mail, remember these points:

1. Don't say anything in an e-mail that you wouldn't say in a letter on your office letterhead. E-mail should contain appropriate language and be rational, reasonable and respectful.
2. Communication should be done within a framework that does not constitute negligence or willful disregard of harmful consequences that might ensue to the institution and its employees.
3. Be aware of the difference between reply and reply-all. Assure that your communication is sent to the proper individual(s) - not inadvertently sent to someone that has no need for the information, or is adversely affected by the communication.
4. E-mail is not a forum to discuss significant events, opinions affecting health care in the institution, lengthy debates or arguments.

L. VIRUS AND ATTACHMENT BLOCKING

One of the industry-wide guidelines for reducing risk of virus infection to organizational networks and workstations is to "block" high-risk attachments at the firewall level. The block prevents virus-type attachments from becoming widely available. UAMS will utilize automatic tools to block high risk attachments within email.

1. Virus protection on the local workstations will block messages that contain malware from internal users.
2. Infected messages coming to UAMS recipients from external sources or the Outlook web client will be cleaned or dropped at the email gateway.
3. High risk attachments (exe, bat, com, scr, vbs, pif) will be stripped from all messages both internally and externally. The user will receive the email with an "alert.txt" attached.
4. In the event of a major trojan, phish, or virus breakout that utilizes a particular file extension for propagation, such extension will be blocked until a patch is available to negate it.
5. Network access will be disabled for workforce members that become infected until their accounts can be cleaned.

M. SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with *Administrative Guide Policy 4.4.02, Employee Discipline*.

Signature: _____ **Date:** **August 25, 2021**

REQUEST TO ACCESS ELECTRONIC COMMUNICATIONS OF OTHERS

Our department requests authority to access electronic communications sent to an individual as described below:

Name, Title, and Department of person whose communications would be accessed:

_____ _____
Name & Title Department

Name, Title, and Department of person requesting access:

_____ _____
Name & Title Department

Name, Title, and Department of person who will do the accessing (if different than above):

_____ _____
Name & Title Department

Reason for access request:_____

_____

_____

How long should the special access last? _____

_____

What will be done with the accessed messages? With whom will they be shared?

_____

_____

_____ _____
Signature of Requesting Person Date

_____ _____
Signature of Department Head Date

_____ _____
Signature of Approving Dean or Vice Chancellor Date

Upon approval, this form is to be delivered to the following person as authorization for them to implement the requested special access: Steve Cochran, Director of Information Technology Security, Slot 802