

Policy 1.430 Graduate Medical Education Committee
Section Educational Administration
Subject Social Networking/Personal Electronic Communication System Usage
Policy Requirements ACGME Common: IV.A.5, IV.B.1.a), VI.B. UAMS Administrative Policy: 2.1.01, 2.1.02, 2.1.13, 2.1.23, 2.1.26, 2.1.42, 3.1.48, 4.4.01, 7.2.11, 13.1.01 Academic Affairs Policy: 2.1.1, 2.1.2 GMEC Policy: 1.420, 1.500
Version History Date developed: 11/2009 Revisions Approved: 5/2014, 2/2018, 8/2020 Legal Review: 7/2013, 2/2018, 8/2020

Purpose

To communicate potential problems and liabilities associated with the use of the Internet and electronic communication systems.

Social networks and other electronic communication systems are great tools for connecting, engaging, and communicating to patients, students, faculty, staff, parents, alumni, fans, and friends. These tools allow the university to broadcast relevant news and to build goodwill with our community.

There is the potential for significant risks associated with inappropriate use. Residents and fellows who use these websites and applications must be aware of the critical importance of privatizing these websites and applications so that only trustworthy “friends” have access to the sites. They must also be aware that posting certain information is illegal. Violation of existing statutes and administrative regulations may expose the offender to criminal and civil liability, and punishment for violations may include fines and imprisonment. Offenders also may be subject to adverse academic actions that range from a letter of reprimand to probation to dismissal from the University of Arkansas for Medical Science (UAMS).

Definitions

Electronic communication systems – websites or web-based services that users may join, view, and/or post information to, including but not limited to weblogs (blogs), internet chat rooms, online bulletin boards, and social networking sites including but not limited to Facebook, Instagram, LinkedIn, Snapchat, Twitter, and YouTube.

Confidential Information – 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) – 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.

Policy

The following policies are intended to provide you with a quick reference to policies and practices at UAMS. Please see UAMS Compliance 360 for any updated information.

1. Individuals may not share confidential information in violation of Health Insurance Portability and Accountability Act (HIPAA) or Family Educational Rights and Privacy Act (FERPA) related to UAMS business on electronic communication systems, including but not limited to, personnel actions, internal investigations, research material, or patient/student/faculty information. This includes sharing photos or partial information even when names of patients, students, or faculty are not used. This includes any activity that would cause UAMS to not comply with state or federal law.
2. All laptops and any other mobile device storing or manipulating data containing confidential information or PHI must use encryption. Submit a ticket with the UAMS Information Technology Department for assistance.
3. Individuals assume personal liability for information they post on electronic communication systems, including but not limited to personal commentary, medical advice, photographs, and videos. UAMS does not endorse or assume any liability for resident or fellows’ personal communications.
4. Individuals should not use UAMS email addresses to register on social media or other electronic communication systems utilized for personal use.
5. Individuals should exercise appropriate discretion in sharing information, with the knowledge that patients, faculty, students, other residents, and potential employers may observe such communications.
6. Individuals should not post defamatory information about others, activities or procedures at UAMS or other institutions through which they rotate.
7. Individuals should not represent or imply that they are expressing the opinion of UAMS or other institutions through which they rotate.
8. Individuals should not misrepresent their qualifications or post medical advice.
9. Individuals should refrain from using social media while on work time and using UAMS equipment, unless it is work-related as authorized by your program director.

10. Since information posted on the Internet is public information, UAMS may review electronic communication systems for content regarding residency applicants and current residents.
11. Employers, organizations, and individuals may monitor and share information they find posted on electronic communication systems.
12. If known or suspected material has been posted, the person who discovered the material should report the incident using the official processes outlined by the UAMS HIPPA office.
13. Disciplinary actions may occur in compliance with Graduate Medical Education Committee (GMEC) policy 1.420 Academic & Other Disciplinary Actions.
14. All major forms of communication that carry the name or logo of UAMS, including social media accounts, whether intended to reach internal or external audiences, will be developed in consultation with the UAMS Office of Communications & Marketing (OCM).

References

UAMS Compliance 360 <http://inside.uams.edu/compliance/uams-policies/>

UAMS HIPPA Office <https://hipaa.uams.edu/>

UAMS Office of Communications & Marketing (OCM) <https://creativeservices.uams.edu/>

GMEC policy 1.420 Academic & Other Disciplinary Actions <https://gme.uams.edu/wp-content/uploads/sites/24/2018/05/1.420-Disciplinary-ActionsFINAL.pdf>

GMEC policy 1.500 Appropriate Treatment of Residents in an Educational Setting <https://gme.uams.edu/wp-content/uploads/sites/24/2019/07/1.500-Treatment-of-Residents-FINAL.pdf>

UAMS Social Media Guidelines <http://inside.uams.edu/social-media/>