

Student Records Privacy: FERPA Basics for Faculty & Staff

Overview

The Family Educational Rights and Privacy Act of 1974, more commonly known as “FERPA”, affords students in higher education certain rights with respect to their education records. FERPA accomplishes this by 1) allowing students to inspect, review and request amendment to their education records, and 2) allowing students to restrict the release of certain personally identifiable information (PII) except to the extent that FERPA authorizes disclosure without consent. FERPA is separate from HIPAA, and records that fall under the auspices of HIPAA *generally* do not fall under FERPA (and vice versa).

FERPA and the Classroom

Whether the classroom is in-person or online, FERPA applies to the way records and student data are handled. Beyond the obvious no-no’s, such as posting student grades outside the instructor’s office door without significant de-identification, remember the not-so-obvious land mines. These might include the seemingly innocuous social media post by the instructor, a public congratulations to a student for academic performance (e.g., “Great job, Sally, for being the only student to ace the last module exam!), or an email message containing sensitive student information that is sent to an audience that includes unnecessary or unintended recipients.

Student Education Records

Student education records generally include any information recorded in any way (e.g., grades, conduct records, meeting minutes, etc.), including, but not limited to, handwriting; print; tape; film; electronic, including computer records; and microform (yes, we still have lots of that here at UAMS), and which is directly related to a student and is maintained by the University or any of its campuses, or by a person acting for the University. There are some exceptions to records that are considered student education records, including *some* “sole possession” records, law enforcement records, employment records, treatment records and alumni records. Refer to UAMS Academic Affairs Policy 2.1.2 for details about exclusions.

Data Security and Record Retention

It is the responsibility of all UAMS employees to protect the privacy student education records and PII. Similar to HIPAA, paper files must be securely transported and electronic files must be encrypted. It is recommended that data files be shared via secured shared folders rather than sent via email. Data storage systems should be protected by strong passwords, filing systems locked, sensitive information never left in open view on a desk, and computers locked whenever the user is not present. Records that are no longer required to be maintained should be archived or destroyed in accordance with departmental and University record retention policy (see UAMS Administrative Guide Policy 3.2.01). Records that have exceeded their retention disposal dates, but which are still on file, are still part of the

student’s education record, and are therefore still subject to the provisions of FERPA.

Directory Information

Directory Information includes specifically outlined data elements that are generally not considered harmful or an invasion of privacy if disclosed. This information usually includes a student’s primary name, home address, phone number, UAMS email and major/field of study. Additional elements are included in the list of Directory Information, and can be found in the UAMS Academic Affairs Policy 2.1.2 and online at <http://registrar.uams.edu/ferpa>. Directory Information is subject to change by UAMS policy amendment, and may be disclosed without student consent under certain conditions only if the student has NOT submitted a request to restrict the release of such information. This process is also outlined in the UAMS policy document.

FERPA Breaches

While breaches are thankfully rare, they must be reported so that UAMS can follow specific procedures to ensure data can be re-secured and the appropriate officials are notified per FERPA guidelines. In the event of *any* unintentional data release or if a release is *suspected*, the incident must be reported immediately to the college’s academic associate dean and to the UAMS FERPA Officer, Clinton Everhart. Timing is critical, and it is always best to report the incident immediately to safeguard data and ensure UAMS remains in compliance with federal law.

Resources and Training

The Office of the University Registrar and UAMS General Counsel work closely to coordinate FERPA policy, compliance and training. University of Arkansas System Administrative Memorandum 515.1 addresses FERPA at the system level, and you can visit <http://registrar.uams.edu/ferpa> for UAMS information, including links to the UAMS Academic Affairs Policy 2.1.2 and the student “Directory Hold” form. Additional FERPA training is in development at this time.

UAMS FERPA Officer / Contact

Clinton Everhart, Ed.D., Assistant Provost for Enrollment Services and University Registrar
Office of the University Registrar ~ 4301 W. Markham, #767 ~
Little Rock, AR 72205
501-686-5113 (Direct) ~ 501-526-5600 (Office of the University Registrar)
everhart@uams.edu
<http://registrar.uams.edu/ferpa>