Academic Policy Series	1900.10

Employee and Student Data: Use and Security

The University of Arkansas (UA) houses and maintains student and employee data in many systems and locations. Such data are utilized to support University operations and to facilitate the ethical and scholarly conduct of research by members of the UA community. The University is committed to using student and employee data in a judicious and responsible manner while working to protect the privacy and confidentiality of all individuals represented in the data. Subject to all applicable UA policies, the University of Arkansas seeks to protect personal and private information in every location or format, including data in any warehouse or comparable site aggregated for access by campus users.

This policy describes the University's general approach to the use and security of employee and student data; other policies may apply to specific types of data or databases. Unless specifically limited, statements in this policy refer to both educational/research and administrative use of individually identifiable information.

In general, requests by UA officials for non-aggregated student or employee data for bona fide administrative or non-research educational purposes shall be considered by administrators for approval to the extent the requests are consistent with the Family Educational Rights and Privacy Act (FERPA), codified at 20 U.S.C. § 1232g, and other federal or state provisions designed to protect the privacy of personal information. Requests for non-aggregated student or employee data for bona fide research purposes shall be considered for approval by the UA Institutional Review Board (IRB) using appropriate protocols. IRB protocols take into account the requirements of (FERPA) and other federal or state provisions designed to protect the privacy of personal information.

Obtaining Access to University of Arkansas Student Data

University of Arkansas faculty and staff must be authorized by the Registrar or Director of Institutional Research, or other appropriate University officials as described below, in order to access UA student data. Any access to student education records must be in compliance with FERPA and Universitywide Administrative Memorandum 515.1, UA Policy Concerning Student Educational Records. Department or unit heads are responsible for monitoring use of information within the department and any failure to comply may result in immediate loss of access to UA student data and may be considered for purposes of job performance evaluation. To the extent applicable, the U of A will not release any "individually identifiable health information" as described in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) except as expressly permitted by HIPAA and its implementing regulations. Likewise, student social security numbers will not be released except for IRB-approved research or for non-research purposes, to the extent permitted by federal law, as approved by the Registrar, the Director of Institutional Research, the Provost, or the Vice Chancellor for Finance and Administration [e.g., for student loan administration or pertaining to student

employment]; otherwise the University Personal Identification number (UID) shall be used if needed.

Student data shall be released only to properly trained appointed employees with a job-related, educational or administrative need to know and consistent with a signed confidentiality agreement approved by the college dean or non-academic department director or director's agent. Student users, both graduate and undergraduate and administrative and research users, shall only be permitted to access information under the supervision of a full-time faculty or staff member who is responsible for monitoring use and consistent with a signed confidentiality agreement. Non-aggregated student information shall only be released with a signed confidentiality agreement that specifies data shall be handled as follows:

1. Data shall be destroyed at the completion of the intended research project or administrative use, rendered anonymous or, in the case of longitudinal data, personally identifiable information will be kept separate from the data in a secured area consistent with the written policy and procedures of the unit.
2. Data shall be used solely for the approved research project or administrative purpose.
3. Data shall be used solely in accordance with FERPA and its implementing regulations, located at 34 CFR § 99, and any other applicable federal or state law.
4. Data shall not be used in any way that permits the identification or contact of any student or his/her parents outside the scope of the approved research project or administrative purpose.
5. Data shall not be disclosed to any unauthorized party.

Obtaining Access to University of Arkansas Employee Data

Employee data shall be released only to properly trained employees with a job-related need to know, and solely to the extent permitted by applicable federal or state law. To the extent applicable, the UA shall not release any "individually identifiable health information" as described in Health Insurance Portability and Accountability Act of 1996 (HIPAA) except as expressly permitted by HIPAA and its implementing regulations. Employee social security numbers shall not be released except for IRB approved research or for non-research access approved by the Director of Institutional Research, the Vice Chancellor for Finance and Administration, or the Provost; otherwise, the University Personal Identification number (UID) shall be used if needed. Non-aggregated employee information shall only be released with a signed confidentiality agreement that specifies non-aggregated data shall be handled as follows:

1. Data shall be destroyed at the completion of the intended research project or administrative use, rendered anonymous or, in the case of longitudinal data, personally identifiable information shall be kept separate from other data in a secured area consistent with the written policy and procedures of the unit.

2. Data shall be used solely for the approved research project or administrative purpose.
3. Data shall be used solely in accordance with any applicable federal or state law.
4. Data shall not be used in any way that permits the identification or contact of any employee or his/her family outside of the scope of the approved research project or administrative purpose.
5. Data shall not be disclosed to any unauthorized party.

Resources
FERPA: www.ed.gov/offices/OII/fpco/ferpa/

HIPAA: www.uark.edu/depts/healinfo/AnnouncePage0802a.shtml
www.hrsa.gov/website.htm

IRB: UA Research and Sponsored Programs – Research Compliance
www.uark.edu/admin/rsspinfo/compliance/human-subjects/irb/index.html

Universitywide Memorandum 515.1, UA Policy Concerning Student Educational Records

Provost's Office 8/1/04