University of Alabama at Birmingham

DATA ACCESS POLICY

June 1, 2017 (Target)

Related Policies, Procedures, and Resources

- Data Protection and Security Policy
- Data Classification Rule
- Data Protection Rule
- HIPAA Core Policies – Information Systems and Network Access
- UABHS Interdisciplinary Policies – Information Systems and Network Access

1.0 Introduction

The University of Alabama at Birmingham (UAB) shall approve access to Sensitive and Restricted/PHI Institutional Data in order to ensure that such access is authorized and based on the principles of least privilege and need to know, that Sensitive and Restricted/PHI data is used appropriately, and that authorized access complies with UAB policies, standards and rules and relevant state and federal laws.

2.0 Scope and Applicability of Policy

This policy outlines requirements for granting and revoking access to Sensitive and Restricted/PHI Institutional Data. This policy applies to access to Sensitive and Restricted/PHI Data maintained by the University or party(ies) acting on the behalf of the University.

Data that is classified as Public can be accessed by and distributed to any entity.

Requests for records by the public are outside of the scope of this policy and shall be handled by University Relations and facilitated by the System Legal Office. This policy also does not apply to situations in which the University is legally compelled to provide access to information.

3.0 Policy Statement

3.1 Data Stewards Approve Access to Sensitive and Restricted/PHI Institutional Data

Access to Sensitive and Restricted/PHI Institutional Data is approved by UAB-designated Data Stewards, whose roles and responsibilities are defined by Section 3.1 of UAB's Data Protection Rule.

- Data Stewards shall grant access in compliance with the UAB Data Security and Protection Policy and all relevant regulations (e.g. FERPA, HIPAA and GLBA).
- Data Stewards shall grant access only to those employees, affiliates, and systems that need the access to perform their job duties or mission and have a legitimate need to know.
- In the event that a Data Steward is not designated, the data in question is owned by the dean, vice president, or head of the unit that creates/owns the data.

3.2 Vice Presidents Retain the Right to Approve All Access to SSN Data

Per the UAB Data Classification Rule, Social Security Numbers (SSNs) are classified as Restricted/PHI Data. Therefore, access to SSN data shall not be granted unless approval has been provided by a University Vice President or a Vice President's designee.

3.3 UAB Hospital Retains the Right to Approve All Access to HIPAA/PHI Data

Appropriate access is provided/controlled according to established policies and procedures within UAB/UABHS HIPAA covered entities. Access shall be granted based on the need-to-know and the minimum necessary standards.

3.4 Data Stewards are Responsible for Procedures for Requesting, Approving, and Revoking Access

Data Stewards shall ensure that procedures for access to Sensitive and Restricted/PHI Institutional Data are documented and implemented. Procedures may vary per Data Steward or Data Users group. However, all procedures shall include sufficient tracking for requests, approvals, and revocations, and such tracking must be auditable.

3.5 Only Authorized Users Shall Access Sensitive and Restricted/PHI Institutional Data

All access by individuals to Sensitive and Restricted/PHI Institutional Data shall be controlled by reasonable measures to prevent access to and/or distribution of said data to unauthorized users.

3.6 Data Users Shall Use Sensitive and Restricted/PHI Institutional Data Responsibly

Data Users must maintain the confidentiality and integrity of data in accordance with all applicable laws, the UAB Data Protection and Security Policy, the Data Classification Rule and Data Protection Rule. Data Users must responsibly use data for intended purposes and respect the privacy of members of the University community.

3.7 Data Stewards May Delegate Approval Responsibilities to a Trusted Designee

A Data Steward may delegate the ability to approve access to Sensitive and Restricted/PHI Institutional Data to individuals in designated roles. Approved documented procedures must exist that allow a trusted designee to grant access for employees that have certain pre-approved roles and responsibilities based on their job requirements and need to know. Data Stewards retain the responsibility for ensuring that all access to Sensitive and Restricted/PHI Institutional Data is authorized, appropriate, and complies with relevant legal requirements and University policies, standards, and rules. The responsibility for owning and protecting the data does not transfer to designees.

4.0 External Third-Party Access to Restricted/PHI Institutional Data Shall be Governed by Contractual Agreement

Individual contractual agreement or memoranda of understanding (MOU), if the third party is a governmental organization, shall govern access to Sensitive and Restricted/PHI Institutional Data by external parties. Such contractual agreements shall be approved through the University contract office.

5.0 Exception

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, complete the Information Security Exception Request Form.

6.0 Non-Compliance

Confirmed violations of this policy will result in consequences commensurate with the offense. Intentional unauthorized release of Sensitive and/or Restricted/PHI Data or egregious violations of this policy may result in termination of employment, appointment, student status, or other relationships with UAB.

7.0 Maintenance

This policy will be reviewed by UAB's Information Security Office periodically, or as deemed appropriate.

8.0 Implementation

The Vice President for Information Technology is responsible for the oversight and implementation of this policy, including the overall procedures related to its implementation and management.

APPENDIX A

UAB Institutional Data Stewards by Data Type
(Designations based on UAB Records Retention Schedule)

Data Type	Data Steward
Student Education Records	Provost and VP of Student Affairs
Administrative Records	UAB Archives
Athletics	VP for Financial Affairs & Administration
Legal	Office of Counsel
Financial Data	VP for Financial Affairs & Administration
Employee Data	VP for Financial Affairs & Administration
Public Relations Data	Chief Communications Officer
Sponsored Research	VP for Research & Economic Development
Patient Records (Electronic Patient Health Information)	Student Health Services: VP of Student Affairs Academic: Provost HIPAA Data: Senior-most VP/Director/Manager
Personally Identifiable Information (PII)	Students: Provost Faculty & Staff: VP for Financial Affairs & Administration
Departmental Records	Administrative: Senior-most VP / Provost
Financial Aid Records	VP of Student Affairs
Facilities Information	VP for Financial Affairs & Administration
Alumni and Development Data	VP of Development and Alumni
Payment Card Information	VP for Financial Affairs & Administration
Police Records	VP for Financial Affairs & Administration