Applying the Data Access Policy

UAB's Data Access Policy governs the access to and use of UAB institutional data that is classified as Sensitive or Restricted. This document provides guidance to UAB constituents on how to apply and abide by the Data Access Policy and, in so doing, take measures that protect both UAB's data and the constituents themselves. Failure to properly apply the Data Access Policy can significantly increase the risk that Sensitive or Restricted data could be compromised and the constituents responsible for protecting the data could be held accountable for the compromise.

Proper application of the Data Access Policy is a shared responsibility for the following groups:

- **Data Stewards:** the owners of the Sensitive or Restricted data who are ultimately responsible for authorizing access to the data and making sure that it is secured,
- **Trusted Designee:** an individual who is granted the ability by a data steward to authorize access to the data; data stewards, however, are always ultimately responsible and accountable for the use and security of their data and cannot assign that responsibility to a trusted designee,
- **Data Custodians:** individuals or groups who accept, process, store, and/or transmit Sensitive or Restricted data during the course of conducting approved UAB business processes, and
- **Data Users:** individuals authorized to access UAB data tied to approved UAB business processes.

Each group is charged with protecting Sensitive or Restricted data to which they have access, but again, the data steward is ultimately responsible and accountable for the security of the Sensitive or Restricted data. So, how is data classified at UAB and what is defined as Sensitive or Restricted data? Detailed answers to those questions can be found in UAB's Data Classification Rule. To summarize that document, data at UAB falls into one of three classifications:

- **Public Data:** Data that may be disclosed to the general public without harm.
    - Examples: public phone directory, course catalogs, public research findings, enrollment figures, public web sites, general benefits data, press releases, newsletters, etc.
- **Sensitive Data:** Data that should be kept confidential. Access to these data shall require authorization and legitimate need-to-know. Privacy may be required by law or contract.
    - *Examples:* FERPA, budgetary plans, proprietary business plans, patent pending information and data protected by law.
- **Restricted Data:** Sensitive Data that is highly confidential in nature, carries significant risk from unauthorized access, or uninterrupted accessibility is critical to UAB operation. Privacy and Security controls are typically required by law or contract.
    - *Examples:* HIPAA PHI, Social Security numbers, credit card numbers (PCI DSS), GLBA data, Export Controlled data, FISMA regulated data, log-in credentials, and information protected by non-disclosure agreements.

Per UAB's Data Access Policy, data that is classified as Public can be accessed by and distributed to any entity. However, access to and the use of Sensitive and Restricted data require authorization from the data steward (or his/her trusted designee) before it can be used by data custodians or data users. With that in mind, this document will guide stewards, trustees, custodians, and users through both the proper process of requesting authorization to use critical UAB institutional data, thus ensuring that the data sets are protected and the risk tied to all accountable parties is minimized to an acceptable level.

Start by building a use case to present to the data steward

Data custodians or users who want to use UAB institutional Sensitive or Restricted data for a legitimate UAB use case or business process should begin by reviewing the appropriate UAB policies, defining a specific data set that is needed for that use case/process, and preparing to present that use case to the appropriate data steward or his/her trusted designee. In general, custodians/users should follow these steps to prepare a use case (a use case should include why the data set is needed, what will be included in the data set, how it will be used, who will require access and/or use the data, and whether the data will be shared with internal/external parties):

- Define the minimum data set that will be needed to fulfill the use case or business process. For example, if your data set only needs the number of employees in each UAB department, the total number of years they've been employees, and whether they are alumni, don't also ask for names, addresses, phone numbers, or other data that isn't required to meet your needs.
    - **Note:** Also define a retention period that states how long this data set will need to be retained. From both a storage and a security point, there's no need to store data for five years if you only need to access it for six months. Once the retention period ends, be prepared to securely delete the data since it no longer has value to you.
- At a minimum, review the following UAB policies and standards to understand how they will shape your use case:
    - Data Access Policy
    - Data Custodian Responsibilities
    - Data Classification Rule
    - Data Protection Rule
- Based on the Data Classification Rule, determine whether the desired data set to be requested is classified as Public, Sensitive, or Restricted. If the data set is classified as Public, you can contact the data steward or trusted designee to request authorization to obtain and use the data set.
    - **Note:** If you are unsure as to whether the data set should be classified as Public, Sensitive, or Restricted, contact UAB's Enterprise Information Security Office (EISO) at riskmgt@uab.edu for additional guidance.
- If the data set is classified as Sensitive or Restricted, determine if the data can be downgraded from Sensitive or Restricted to Public via deletion, tokenization, or de-identification.
    - For example, if social security numbers are included as part of the data set, first ask whether SSNs actually are needed? If not, delete them and there's a good chance Restricted data has now been reduced to Public data. If SSNs are used as unique identifiers, determine whether they can be replaced by another non-Restricted data field that can be used as a unique key, such as a BlazerID, student (B00) number, or employee (Oracle) number.
    - For additional guidance on how you can reduce the classification of your data to an acceptable risk level, please visit UAB's Data Reduction site.
- If Sensitive or Restricted data cannot be downgraded via deletion, tokenization, or de-identification, the custodian/user seeking authorized access to the data must review UAB's Data Protection Rule to determine specific methods required to secure the data should authorized access be granted for the required use case. For example, Restricted data must be stored in UAB Central IT's data center.

- **Note:** If the data set is classified as Sensitive or Restricted, there likely are additional security requirements tied to regulations or laws that must be met. Be sure you are aware of such requirements. For example, credit card data must meet requirements set forth by the Payment Card Industry Data Security Standard (PCI DSS). Patient health information is governed by Health Insurance Portability and Accountability Act (HIPAA) requirements, and access to UAB/UABHS-owned HIPAA data must be approved by the UAB Health System.
- If you are unsure as to whether there are additional security requirements tied to your use case, contact EISO at riskmgt@uab.edu for additional guidance. You also can refer to UAB's Applying the Data Classification and Protection Rules document for guidance.

- Identify the data steward that can grant authorization to use the Sensitive or Restricted data in question. The following chart provides information as to which UAB group owns specific types of UAB institutional data:

Data Type	Data Steward
Student Education Records	Provost and VP of Student Affairs
Administrative Records	VP for Financial Affairs & Administration
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

Table 1: UAB Institutional Data Stewards by Data Type, as defined by UAB's Data Access Policy

- **Note:** Remember, access to UAB/UABHS-owned HIPAA data must be approved by the UAB Health System.

- At this point, formally prepare to present to the data steward/trusted designee your use case/business process, a sample of the desired minimum data set needed, the retention requirements, and a description of how the data set will be protected and how it will meet the requirements set by the UAB Data Protection Rule and any applicable regulations and/or laws.

- **Note:** If the custodian's/user's use case involves sharing Sensitive and/or Restricted data with an external third party, an exception request must be filed for EISO to review. This review process must be completed and official approval granted by EISO before the Sensitive/Restricted data can be shared with an approved external party. Also, an individual contract agreement or memoranda of understanding (MOU) must be signed by the third party and approved by the University contract office.

Present the use case and formally request access to the data

At this point, the custodian/user should reach out to the appropriate data steward/trusted designee to formally request access to the required data set. The custodian/user should present the explanation of the proposed use case/business process, the minimum required data set, the defined retention period, and a description of how the Sensitive or Restricted data will be protected.

The steward/designee is responsible for reviewing the elements presented by the custodian/user before granting or denying access to the requested data. As part of this evaluation process, the custodian/designee should consider whether he/she understands:

- The use case and whether the minimum data set has been requested,
- How the data will be secured and used,
- Who will have access to the data,
- How the data will be shared with internal or external parties (if applicable),
- How long the data will be retained,
- How it will be securely deleted, and
- Whether all of these factors sufficiently minimize the risk of the data being compromised to a level that is acceptable to the data steward/trusted designee.

The steward/designee may immediately grant approval and coordinate with the custodian/user for secure transfer of the data set to the custodian/user. If the steward/designee deems the risk to the data is still too high, he/she can require the custodian/user to implement additional security controls and improve the associated processes tied to the use case to reduce the risk to an acceptable level. The steward/designee always has the right to deny access to the data, too.

Authorization and the Data Lifecycle

Once authorization to use the Sensitive or Restricted data is granted by the steward/designee, he/she must work with the custodian/user to securely transfer the data to the custodian/user. As a reminder, the custodian/user must implement all of the security controls they designed to protect the data and workflow processes that store, transmit, or process that data. The custodian/user also must follow the guidance UAB provides regarding the data custodian responsibilities.

It is of paramount importance that all parties involved understand that the approved data set can only be used by the authorized custodian/user to fulfill the original use case presented to the steward/designee. Possession of the approved data set by the custodian/user does not entitle him/her to use that data set with other use cases or business workflow processes without first securing permission from the steward/designee. Any new use cases that can leverage that data set also must be presented for approval by the steward/designee. Also, approval to use the data set does not grant

custodians/users the right to pass that set along to other unauthorized parties who might want to use the data.

Once the use case or workflow process has been completed and the data retention point is expired, the custodian/user must securely delete the Sensitive or Restricted data. He/she also should notify the associated steward/designee that the data set has been destroyed. Since the data steward is always responsible and accountable for the security of the Sensitive and Restricted data that he/she owns, the steward should implement a business process that notifies him/her or the trusted designee to confirm from custodians/users that all Sensitive or Restricted data that have been provided to custodians/users are securely deleted at the end of their term of use, thus ending the data's lifecycle for that particular use case.

Related UAB documents

- Data Classification Rule
- Data Protection Rule
- Data Custodian Responsibilities
- Data reduction strategies
- Applying the Data Classification and Protection Rules
- Risk Level Assignment for UAB Restricted and Sensitive Data