Applying the Data Classification and Protection Rules

Sources Cited:

- Data Classification Rule
- Data Protection Rule

Objective

This knowledge base article provides guidance regarding issues that fall under the purview of UAB's Data Classification and Data Protection rules. It leverages information from those rules that can be used to assess and address issues that involve risk management and compliance matters.

First, the "Data Classification Levels" section of this document covers the three classification tiers applied to data at UAB and provides examples of each classification level. Each classification can be mapped to its own table of minimum security requirements that describe how the data should be properly handled and protected. Those requirements are enumerated in the "Data Protection Requirements" section.

Data Classification Levels

Per the Data Classification Rule, all UAB data that is stored, processed, or transmitted must be classified in accordance with the rule itself. Based on those classifications, users are required to implement appropriate security controls. The three classifications appear in the following table:

Classification Level	Definition	Examples of Data
Public data	Data that may be disclosed to the general public without harm.	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.	FERPA, budgetary plans, proprietary business plans, patent pending information, export controls information and data protected by law.
Restricted/PHI data	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.	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.

These classifications provide context to any issues that deal with raw data or systems that process, transmit, or store data. They can be used with the Data Protection Requirements detailed in the next section to provide guidance for users as to how the various types of data can be appropriately handled.

Data Protection Requirements

Per the Data Protection Rule, the Data Protection Requirements define the minimum security requirements for each category of data when being used or handled in a specific context (such as Sensitive Data sent in an email message or the storing and processing of Restricted Data). By mapping the Classification Level of the data to the Protection Requirements, one can quickly gauge what type (or types) of controls need to be put in place to protect the classified data.

For example, if a user inquires about emailing patient information across campus, this should set off a red flag. Per the Data Classification Rule, patient information is classified as Restricted/PHI data. By looking at the Data Protection Requirements table regarding email and electronic messaging for Restricted/PHI data, one will find the following:

Email and other electronic messaging	• Not permitted without express authorization or unless required by law. • Messages with Restricted data shall be transmitted in either an encrypted file format or only through secure, authenticated connections or secure protocols. • Restricted data may be shared through approved UAB services. • SSNs may not be shared through email or other electronic messaging. • Credit card data may not be shared through email or other electronic messaging.

Note that there are a number of restrictions on emailing Restricted/PHI data. Based on the requirements, the Restricted/PHI data would have to be sent via email in an encrypted file attachment or in an encrypted email, using S/MIME and certificate-based encryption, for example. If the requirements cannot be met, then the user must not be allowed to email unencrypted patient information across campus. An alternative method of secure delivery must be used.

For convenience, the minimum protection requirements for Public, Sensitive, and Restricted/PHI data are provided in tables on the following pages. Afterward, there is an appendix that provides brief descriptions of the following types of Sensitive and Restricted data:

- PCI/Credit Card Data
- HIPAA/PHI Data
- GLBA Data
- FERPA Data

Public Data	
Collection and Use	• No protection requirements
Granting Access or Sharing	• No protection requirements
Disclosure, Public Posting, etc.	• No protection requirements
Electronic Display	• No protection requirements
Open Records Requests	• Data can be readily provided upon request. However, individuals who receive a request must coordinate with University Relations Office before providing data.
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	• No protection requirements
Storing or Processing: Server Environment	• Servers that connect to the UAB network must comply with the Minimum Security for Computing Devices Rule.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	• Systems that connect to the UAB network must comply with the Minimum Security for Computing Devices Rule.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	• No protection requirements
Electronic Transmission	• No protection requirements
Email and other electronic messaging	• No protection requirements
Printing, mailing, fax, etc.	• No protection requirements
Disposal	• No protection requirements

Sensitive Data	
Collection and Use	• Limited to authorized uses only. • Units/Colleges that collect and/or use Sensitive Data should participate in the Information Security Program by reporting servers to the Enterprise Information Security Office. • In addition, any/all servers that process or store Sensitive Data must meet all requirements associated with applicable laws and/or standards. • Additionally, sensitive institutional data must be stored and managed in unit or higher systems.
Granting Access or Sharing	• Access shall be limited to authorized University officials or agents with a legitimate academic or business interest and a need to know as outlined by UAB policies. • All access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable. • Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved through the UAB contract process.
Disclosure, Public Posting, etc.	• Sensitive Data shall not be disclosed without consent of the data owner. • Sensitive Data may not be posted publicly. • Directory information can be disclosed without consent. However, per FERPA, individual students can opt out of directory information disclosure.
Electronic Display	• Only to authorized and authenticated users of a system.
Open Records Requests	• Sensitive Data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with the University Relations Office.
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	• A contractual agreement (or MOU if governmental agency) outlining security responsibilities shall be in place and approved through the UAB contract process before exchanging data with the third party / service provider. • UAB Box.com – no special requirements.
Storing or Processing: Server Environment	• Servers that process and/or store sensitive institutional data must comply with the Minimum Security for Computing Devices Rule, as well as applicable laws and standards. Additionally, sensitive institutional data must be stored and managed in unit or higher systems.

Sensitive Data	
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	• Systems that connect to the UAB network must comply with the Minimum Security for Computing Devices Rule, as well as applicable laws and standards. • In addition, any/all systems that process or store Sensitive Data must be encrypted volume and endpoint must require PIN and/or password for access to device.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	• Sensitive Data shall only be stored on removable media in an encrypted file format or within an encrypted volume.
Electronic Transmission	• Sensitive Data shall be transmitted in either an encrypted file format or over a secure protocol or connection.
Email and other electronic messaging	• Messages shall only be sent to authorized individuals with a legitimate need to know. • Messages with Sensitive Data shall be transmitted only to other uab.edu or uabmc.edu email recipients. • Sensitive Data may be shared through approved UAB services.
Printing, mailing, fax, etc.	• Printed materials that include Sensitive Data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. • Access to any area where printed records with Sensitive Data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry. • Do not leave printed materials that contain Sensitive Data visible and unattended.
Disposal	• Follow the UAB Secure Media Destruction process for the secure disposal of discs, CDs, DVDs, tapes and hard drives. • Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use - Physically destroy. • Follow the Destruction of University Records Procedure for printed materials.

Restricted/PHI Data	
Collection and Use	• Limited to authorized uses only. • Units/Colleges that collect and/or use Restricted data should participate in the Information Security Program by reporting servers to the Enterprise Information Security Office. • In addition, any/all servers that process or store Restricted data must meet all requirements associated with applicable laws and/or standards. • Restricted/PHI data must be stored on servers located in the UAB data center and managed by Central IT. • SSNs may not be used to identify members of the UAB community if there is a reasonable alternative. • SSNs shall not be used as a username or password. • SSNs shall not be collected on unauthenticated individuals. • All credit/debit card uses must be approved by the VP of Financial Affairs and Administration Office.
Granting Access or Sharing	• Access shall be limited to authorized University officials or agents with a legitimate academic or business interest and a need to know as outlined by UAB policies. • All access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable. • Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved through the UAB contract process.
Disclosure, Public Posting, etc.	• Not permitted unless required by law.
Electronic Display	• Restricted data shall be displayed only to authorized and authenticated users of a system. • Identifying numbers or account numbers shall be, at least partially, masked or redacted.
Open Records Requests	• Restricted data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting Restricted portions of records. Individuals who receive a request must coordinate with the University Relations Office.

Restricted/PHI Data	
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	• A contractual agreement (or MOU if governmental agency) and/or Business Associate Agreement (BAA) outlining security responsibilities shall be in place and approved through the UAB contract process before exchanging data with the third party / service provider. • UAB Box.com – Subject to any applicable laws.
Storing or Processing: Server Environment	• Servers that process and/or store sensitive institutional data must comply with the Minimum Security for Computing Devices Rule, as well as applicable laws and standards. Additionally, restricted/PHI data must be stored on servers located in the UAB data center and managed by Central IT. • Storing Credit/Debit card PAN data is not permitted.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	• Any/all systems that process or store Restricted data must be encrypted volume and endpoint must require PIN and/or password for access to device. • Storing Credit/Debit card PAN data is not permitted. • Storing Restricted data on personally-owned devices is not permitted. • Devices storing or processing Restricted data must be physically secure at all times. • Avoid storing Restricted data on portable devices.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	• Not permitted unless required by law. • If required by law, Restricted data stored on removable media shall be encrypted and the media shall be stored in a physically secured environment. Storing Restricted data on personally-owned media is not permitted.
Electronic Transmission	• Secure, authenticated connections or secure protocols shall be used for transmission of Restricted data.
Email and other electronic messaging	• Not permitted without express authorization or unless required by law. • Messages with Restricted data shall be transmitted in either an encrypted file format or only through secure, authenticated connections or secure protocols. • Restricted data may be shared through approved UAB services. • SSNs may not be shared through email or other electronic messaging. • Credit card data may not be shared through email or other electronic messaging.

Restricted/PHI Data	
Printing, mailing, fax, etc.	• Printed materials that include Restricted data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. • Access to any area where printed records with Restricted data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry. • Do not leave printed materials that contain Restricted data visible and unattended. • Social Security Numbers shall not be printed on any card required to access services. • New processes requiring the printing of SSN on mailed materials shall not be established unless required by another state agency or a federal agency.
Disposal	• Follow the UAB Secure Media Destruction process for the secure disposal of discs, CDs, DVDs, tapes and hard drives. • Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use - Physically destroy. • Follow the Destruction of University Records Procedure for printed materials. • Restricted data that is no longer necessary for University business should be disposed of to minimize risk of data breach.

Appendix: Specific Types of Sensitive and Restricted Data

PCI/Credit Card Data — Restricted

When the term "credit card data" is used, many people immediately think of a credit card number, an expiration data, and a cardholder's name. These are examples of Restricted credit card data, as defined by the Payment Card Industry Data Security Standard (PCI DSS). But they are not the only types of Restricted credit card data that must be protected. The PCI DSS defines the following elements as either cardholder data or sensitive data that are classified as Restricted under UAB's Data Classification Rule:

- Primary account number (PAN)
- Cardholder name
- Expiration date
- Service Code
- PINs or PIN blocks
- Full track data (magnetic stripe data or the equivalent residing on a card's chip)
- CAV2, CVC2, CVV2, or CID codes appearing on the back of the card

HIPAA or PHI Data — Restricted

The Health Insurance Portability and Accountability Act (HIPAA) mandates that Protected Health Information (PHI) must be protected in both physical and digital form. Such information, which is classified as Restricted/PHI by UAB, is defined as individually identifiable health information that relates to the mental or physical health/condition of an individual. Examples of HIPAA/PHI data that must be protected include:

- Names
- Postal address information (any address information smaller than state of residence)
- Dates
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images

GLBA Data — Restricted

The Gramm-Leach-Bliley Act (GLBA) is a law enacted in 1999 that requires financial institutions to protect the privacy of consumer information. It also mandates that companies provide consumers with privacy statements that describe in detail the companies' information-sharing policies and practices. The GLBA's Privacy Rule is designed to protect the non-public personal information (NPI) of consumers. NPI is defined as any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.

Examples of NPI protected by GLBA include:

- Any information an individual gives the institution in order to get a financial product or service (for example, name, address, income, Social Security Number, or other information on an application)
- Any information an organization receives about an individual from a transaction involving a financial product or service (for example, the fact that an individual is a consumer or customer of the company, account numbers, payment history, loan or deposit balances, and credit or debit card purchases)
- Any information the company gets about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

FERPA Data — Sensitive

The Family Educational Rights and Privacy Act of 1974, commonly known as FERPA, is a federal law governing the privacy of educational records. It grants specific rights to students and puts restrictions on how schools may handle educational records. In general, UAB divides educational records into two areas: Non-directory information and directory information.

Non-directory information is considered to be private information, and should NOT be disclosed. Examples of non-directory information include:

- Class schedule
- Religious affiliation
- Citizenship/nationality
- Disciplinary status
- Ethnicity
- Gender
- Grade point average (GPA)
- Marital status
- Social Security Number/student ID
- Grades/exam scores
- Test scores (SAT, ACT, GRE, final exams, etc.)

UAB considers the following data to be “directory information,” which is not considered to be protected data and can be released without consent of the student. Note, however, that FERPA allows individual students to opt out of directory information disclosure:

- Name
- Address (local and permanent)
- Telephone number
- University e-mail address
- CampusCard photo
- Date of birth
- Major field of study
- Participation in officially recognized activities and sports
- Dates of attendance (enrollment verification)
- Degrees and awards received
- Institution most recently previously attended