Data Classification and Handling
HIPAA Policy: Security 12

Summary: Classifying data in HIPAA covered entities and setting baseline security measures

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish a framework for classifying data in the possession of University of Mississippi (UM) and its workforce members and to define the baseline security controls for handling and safeguarding information assets.

The resulting data classification categories determine which UM data requires special protection safeguards, security controls, and risk reduction measures.

The purpose of this policy is to establish the minimum security controls for handling, labeling and storing UM's data in order to protect the data from unauthorized disclosure or misuse.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy.

This policy applies to all electronic data that is generated or used as part of UM's covered entity business operations.

This policy covers all UM data regardless of where the information is stored, including UM owned or managed systems or on a third party-hosted service.

All workforce members, including third parties, who may have access or exposure to UM data are required to comply with this policy.

Policy

A. Classification of Data

   1. All UM data is classified into one of three sensitivity levels (tiers).

2. Data owners may assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements is used to classify the entire body of data as a whole.

B. Tier 1: Confidential Data

1. Data is classified as confidential data when the unauthorized disclosure, alteration or destruction of that data causes a significant level of risk. Confidential data is always sensitive.
2. The highest level of security controls apply to confidential data. Access to confidential data must be controlled from creation to destruction. Access is only granted to those persons who require such access in order to perform their job ("need-to-know") in accordance with the principle of least privilege. Access to confidential data may be authorized to groups of persons based on job classification or responsibilities ("role-based" access).
3. Access to confidential data must be authorized by the data owner who is responsible for the data.
4. Based on state, federal, and contractual requirements, protected health information (PHI) covered under HIPAA is defined as confidential data and must be protected.
5. Based on state, federal, and contractual requirements, personally identifiable health information (PII) covered under HIPAA is defined as confidential data and must be protected.
6. Payment Card Information (PCI) covered under PCI DSS (Data Security Standard) is defined as confidential data and must be protected. Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:
    - Cardholder name
    - Service code
    - Expiration date

- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

C. Tier 1: Confidential Data Examples

1. Data protected by state or federal regulations including:

   - Protected Health Information (PHI)
   - Personally Identifiable Information (PII)
   - Social Security Numbers (SSN)
   - Payment Card Information (PCI or Credit/Debit Card Data)
   - Financial Account Data
   - Data as identified in the Mississippi Data Breach Notification Law

2. Data protected by confidentiality agreements, including:

   - Employee personnel records
   - Non-Disclosure Agreements (NDA).

3. Internal UM information that must be protected from unauthorized internal or external disclosure, including:

   - Merger / acquisition sensitive info
   - Financial reports and budget information
   - Sensitive Executive Officer correspondence or information
   - Intellectual property
   - Credentialing information (e.g., credentials, password data) that grants access to systems storing sensitive data
   - Legal products, including legal correspondence and data that is subject to attorney-client privilege

4. Legal hold data that are the subject of (or are anticipated to be the subject of) any type of investigation and/or legal proceeding.

D. Tier 2: Internal Use Only Data

1. Data is classified as internal use only data when the unauthorized disclosure, alteration or destruction causes a low-to-moderate level of risk. Internal use only data is not for release to the general public. Internal use only data is always sensitive.
2. A reasonable level of security controls apply to internal use only data.
3. By default, all data that are not explicitly classified as confidential data or public data are to be treated as internal use only data.
4. Access to internal use only data must be authorized by the data owner who is responsible for the data. Access to internal use only data may be authorized to groups of persons based on job classification or responsibilities ("role-based" access).
5. Tier 2: Internal Use Only Data Examples:
   - Internal company newsletters
   - Training program materials
   - Project plans / documentation
   - Operations meeting notes
   - Operations policies and procedures

E. Tier 3: Public Data

1. Data is classified as public data when the unauthorized disclosure, alteration or destruction of that data results in little or no risk. Public data is not sensitive but does require a data owner. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.
2. As public data is not considered sensitive, access may be granted to any requester or published with no restrictions. The integrity of public data is protected and the data owner takes measures to ensure public data remains accurate over time.

3. Tier 3: Public Data Examples:
    - Provider directory information
    - Public event information
    - Research publications

F. Data Handling, Labeling, and Storage Requirements

1. All UM data is handled, labeled, and stored in accordance with this policy based upon its data classification.
2. Procedures for handling, processing, communication and storage of information (including information media awaiting disposal) are established to protect data from unauthorized disclosure or misuse including:
    - Physical and technical access restrictions commensurate with the data classification level
    - Handling and labeling of all media according to its indicated classification (sensitivity) level
    - Periodic review (at a minimum annually) of distribution and authorized recipient lists
    - Monitoring the status and location of media containing unencrypted confidential information

    Note: Any data covered by federal or state laws or regulations or contractual agreements must also meet the security requirements defined by those laws, regulations, or contracts in addition to the requirements of this policy.

G. Minimum Security Controls

The following table specifies the minimum security controls for UM's confidential data, internal-use-only data, and public data:

Data Classification and Handling
HIPAA Policy: Security 12

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
Access Controls	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data owner or designee grants permission for access. Authentication and authorization required for access. Non-Disclosure Agreement required.	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data owner or designee grants permission for access. Authentication and authorization required for access.	No restrictions for viewing. Authorization by data owner or designee required for modifications; supervisor approval required if not a self-service function.
Auditing	Logins, access and changes.	Logins	Not required
Backup/Disaster Recovery	Daily backups required. Off-site storage of backup media in a secure location recommended.	Daily backups required. Off-site storage of backup media recommended.	Backups required; daily backups recommended.
Copying/Printing (applies to both paper and electronic forms)	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and who have signed a Non-Disclosure Agreement.	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know. Data must not be left unattended on a	No restrictions.

Data Classification and Handling
HIPAA Policy: Security 12

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
	Data must not be left unattended, such as on a printer/fax, desktop, or any public location. Copies must be conspicuously labeled "Confidential". If sent via internal mail, must be must be marked "Confidential".	printer/fax, desktop, or any public location. May be sent via Internal Mail.	
Data Storage	Storage on a secure server required. Storage in secure Data Center required. Should not permanently store on an individual workstation or Mobile Computing Device (e.g., a laptop computer). If stored on a workstation or Mobile Computing Device, that device must use whole-disk encryption. Encryption on Backup Media required.	Storage on a secure server recommended. Storage in a secure Data Center recommended. Should not store on an individual's workstation or a mobile device.	Storage on a secure server recommended. Storage in a secure Data Center recommended.

Data Classification and Handling
HIPAA Policy: Security 12

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
	Paper/hard copy: do not leave unattended where others may see it; store in a secure location.		
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	Shred paper. Re-use or destroy electronic media at end of life according to the *Secure Disposal Policy*.	Recycle paper. Wipe/erase electronic media.	No restrictions.
Mobile Computing Devices	Password protected, locked when not in use, encryption required.	Password protected, locked when not in use.	Password protection recommended, locked when not in use
Network Security	Protection with a Network Firewall using "default deny" (Deny All, Permit by Exception [DAPE]) rule set required. IDS or IPS protection recommended. Protection with router ACLs optional. Servers hosting the data must not be visible to the	Protection with a Network Firewall required. IDS or IPS protection required. Protection with router ACLs optional. Servers hosting the Data must not be visible to the entire Internet. May be in a shared Network server subnet	May reside on a public Network. Protection with a Firewall recommended. IDS or IPS protection recommended. Protection only with router ACLs acceptable.

Data Classification and Handling
HIPAA Policy: Security 12

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
	entire Internet, nor to unprotected subnets like the guest wireless networks. Logical and/or physical Network partitioning of Confidential Data from other types strongly recommended. The Firewall rule set must be reviewed periodically.	with a common Firewall rule set for the set of servers.	
Physical Security	Computing Devices must be locked or logged out when unattended. Hosted in a secure Data Center required. Physical access to Data Center must be monitored, logged, and limited to authorized individuals 24x7.	Computing Devices must be locked or logged out when unattended. Hosted in a secure location required; a secure Data Center is recommended.	Recommend that computing devices be locked or logged out when unattended. Host-based software firewall recommended.
Remote Access to systems hosting the data	Access restricted to local network or secure VPN group. Remote Access by Third Party for technical	Access restricted to local Network or VPN. Remote Access by Third Party for technical support limited to	No restrictions.

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
	support limited to authenticated, temporary access via secure protocols over the Internet. Two-factor authentication required.	authenticated, temporary access via secure protocols over the Internet.	
System Security	Must follow UM- specific and Operating System (OS)-specific best practices for system management and security. Host-based software Firewall required. Host-based software IDS/IPS recommended.	Must follow UM- specific and OS-specific best practices for system management and security. Host-based software Firewall recommended. Host-based software IDS/IPS recommended.	Must follow general best practices for system management and security. Host-based software Firewall recommended.
Training	General security awareness training required. Data security training required. Applicable policy and regulation training required.	General security awareness training required. Data security training required.	General security awareness training recommended.

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
Transmission	Encryption required in accordance with the *Encryption Policy*. Cannot transmit via email unless encrypted.	No requirements.	No restrictions.
Virtual Environments	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Should not share the same virtual host environment with guest virtual servers of other security classifications.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.

Policy Compliance

Enforcement

The CISO, or designee, has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UM reserves the right to add, delete, or revise any provision of this Policy (approval by committee) at any time without prior notice to users.

Data Classification and Handling
HIPAA Policy: Security 12

Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM's computing environment is subject to loss of network privileges and any other disciplinary actions deemed appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy.

Exceptions

Exceptions to this policy must follow the approved exception process as outlined in the *Information Security Waiver Policy*. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice.

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory References**: HIPAA §164.308(a)(1)(ii)(A), HIPAA §164.308(a)(1)(ii)(B), HIPAA § 164.308(a)(3)(ii)(A), HIPAA § 164.310(b), HIPAA § 164.310(c), HIPAA § 164.310(d)(1), HIPAA § 164.310(d)(2)(iv), HIPAA § 164.312(c)(1)
- **HITRUST References**: 07.d Data Classification Guidelines, 09.q Information Handling Procedures
- **PCI References**: PCI DSS v3 3.2, PCI DSS v3 3.2.1, PCI DSS v3 3.2.2, PCI DSS v3 3.2.3, PCI DSS v3 3.3, PCI DSS v3 9.5, PCI DSS v3 9.6, PCI DSS v3 9.6.3, PCI DSS v3 9.7

Related Documents:

- Information Technology Access Control Policy
- Glossary
- Information Asset Management Policy
- Information Security Roles and Responsibilities
- Password Policy for Client-Facing Deliverables
- Record Retention Policy

Data Classification and Handling
HIPAA Policy: Security 12

Approval

Chief Information Security Officer	<date>