Third Party Risk Management
HIPAA Policy: Security 03

Summary: Outlines methods for dealing with business associates and other third parties

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish the methods by which University of Mississippi (UM) manages security risks that are introduced by third parties. The intent is to ensure that the security of UM information and information assets are not reduced when sharing information with third parties or by the introduction of third party products or services into the UM environment.

This policy also describes what processes must be in place before protected health information (PHI) can be released to Business Associates, and the mechanism for developing and maintaining contractual agreements with Business Associates regarding their responsibilities under HIPAA regulations.

Policy Scope

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

This policy applies to all third party arrangements, including those with business associates.

Definitions

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

Policy Statement

A. Third Party Risk Management Policy

1. UM shall establish a third party risk management function with the purpose of governing security risks of third party organizations that have access to enterprise data, or provide products or services for UM.
2. Responsibilities for the third party risk management function shall include:
    a. Identifying all UM Business Associates, according to the HIPAA Security and Privacy rules.
    b. Vetting the security controls of third parties before establishing a third party contract relationship.
    c. Ensuring an approved and up-to-date UM Business Associate Agreement (BAA) is in place and has been signed by every third party.

d. Maintaining a current and accurate listing of all UM business associates.

e. Monitoring third parties for adherence to provisions within BAAs (where applicable), Service Level Agreements (SLAs), and contractual security requirements.

f. Performing continual reviews of security measures implemented by third parties.

g. Ensuring the adherence to all other provisions within this policy.

B. Third Party Risk Identification

1. The potential risks to UM information assets from business processes involving third parties shall be identified, and appropriate controls shall be implemented to mitigate these risks before granting access.

2. Third parties shall only be granted access to UM' information assets after due diligence has been conducted, and appropriate controls have been implemented.

3. UM shall ensure third parties are aware of their obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.

4. Due diligence by UM to determine risk may include interviews, and reviews of documents, checklists, and certifications.

C. Third Party Security Requirements

1. If appropriate, a risk assessment shall be conducted of the third party to determine the specific security requirements necessary to secure their systems to a level of risk acceptable to UM.

2. All identified third party security requirements shall be addressed and validated before granting third party access to UM information or information assets.

D. Third Party Agreements

1. Agreements with third parties involving accessing, processing, communicating or managing UM information assets, or adding products or services to information

assets must cover all relevant security requirements and shall include all required security and privacy controls in accordance with UM's security and privacy policies.

2. The specific limitations of access, arrangements for compliance auditing, penalties, and the requirement for notification with respect to relevant third party personnel transfers and terminations shall be identified in the third party agreements.
3. A standard BAA shall be defined and made available to appropriate workforce members.
4. The BAA shall include provisions for breach notification and termination upon breach.
5. The BAA shall define the disposition of PHI on termination of the agreement.

E. Third Party Access Control Requirements

1. UM shall only allow third parties to create, receive, maintain, or transmit PHI on its behalf after the organization obtains satisfactory written assurance that the third party shall appropriately maintain the privacy and security of the enterprise data, including, where relevant, protecting PHI via a BAA.
2. Third party access shall be based on the principles of need-to-know and least privilege.
3. Third party access shall be granted only for the duration required.
4. Remote access connections between UM and third parties must be encrypted.
5. Remote access connections with third parties shall be monitored on an ongoing basis.

F. Third Party Service Delivery

1. UM shall ensure that the security controls, service definitions, and delivery levels included in the third party agreement are implemented, operated and maintained by the third party.
2. SLAs, or contracts with an agreed service arrangement, shall address liability, service definitions, security controls, and other aspects of services management as appropriate.
3. UM shall develop and update at least annually a list of current service providers.

4. UM shall address information security and other business considerations when acquiring systems or services including maintaining security during transitions and business continuity following a failure or disaster.

G. Third Party Monitoring and Review

1. The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the third party agreements.

2. Network connections with third parties shall be periodically audited to ensure that third parties have implemented any required security features and that third parties meet all requirements agreed to with UM.

H. Third Party Change Management

1. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking into account the criticality of business systems and processes involved and re-assessment of risks.

2. Third parties shall be required to coordinate, manage and communicate changes that shall have an impact to UM information, systems or processes.

3. Third party changes shall be evaluated to identify the potential impacts before implementation.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO) 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 (with committee approval) at any time, or any other Information Security Policy without prior notice to users.

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

Exeption 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 References

HIPAA Regulatory References: HIPAA § 164.308(a)(3)(ii)(A), HIPAA § 164.308(a)(3)(ii)(B), HIPAA § 164.308(b)(1), HIPAA § 164.308(b)(3), HIPAA § 164.314(a)(1), HIPAA § 164.314(a)(2)(i), HIPAA § 164.314(a)(2)(ii), HIPAA § 164.314(b)(1), HIPAA § 164.314(b)(2)(i), HIPAA § 164.314(b)(2)(ii), HIPAA § 164.314(b)(2)(iii), HIPAA § 164.314(b)(2)(iv), HIPAA § 164.404(b), HIPAA § 164.410(a)(1), HIPAA § 164.410(a)(2), HIPAA § 164.410(b), HIPAA § 164.410(c)(1), HIPAA § 164.410(c)(2), HIPAA § 164.414(b)
HITRUST References: 05.i Identification of Risks Related to External Parties, 05.j Addressing Security When Dealing with Customers, 05.k Addressing Security in Third Party Agreements, 09.e Service Delivery, 09.f Monitoring and Review of Third Party Services, 09.g Managing Changes to Third Party Services
PCI Regulatory References: PCI DSS v3 12.8.2, PCI DSS v3 12.8.3, PCI DSS v3.1 2.4, PCI DSS v3.1 12.8.3, PCI DSS v3.1 12.8.5, PCI DSS v3.1 12.9

Third Party Risk Management
HIPAA Policy: Security 03

Related Documents

Business Associate Agreement (BAA)
Template Business Associates Policy
Glossary
Standard Service Level Agreement (SLA)
Template Third Party Risk Management Procedures