Data Security Policy – Business Associate and Third Party Risk Management

PURPOSE

To provide principles and guidelines for business associate and third party risk management, including vendors, service providers, and suppliers.

SCOPE

The Business Associate and Third Party Risk Management Policy and Procedure will cover Organization's:

- Definition of business associates and third parties
- Due diligence and third party/business associate selection
- Third Party Inventory
- Third Party Risk Management (TPRM)
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows processes for managing relationships, agreements, and day-to-day operations with business associates and third parties.

Business Associates and Third Parties

Third parties are contractors, service providers, vendors, suppliers, and any other businesses or partners the company engages with.

Business associates are a subset of third parties that create, process, store, handle, or otherwise maintain PHI or ePHI. The HIPAA Security Rule provides specific guidance for what must be included in Business Associate Agreements or "BAAs," including measures for safeguarding PHI or ePHI (164.314(a)). Business Associates must comply with the requirements of the HIPAA Security Rule and properly safeguard PHI or ePHI handled on Organization's behalf.

Organization documents and retains written agreements with business associates and third parties.

Due Diligence and Third Party Selection

Organization has adopted and follows a third party or business associate due diligence and selection process that incorporates cross-functional stakeholders.

Organization performs due diligence throughout the third party or business associate selection process, using internal requirements, industry standards, and questionnaires to screen potential candidates.

Rationale for selecting a third party or business associate is documented and retained as part of the Third Party Inventory, Repository, or Database. Organization can use the Vendor module in The Guard for this purpose.

Third Party Inventory

Organization has set up a Third Party Inventory that contains details and information about each third party or business associate the company does business with. The Third Party Inventory includes a risk rating for each organization based on the criticality of their services or products to our own operations.

Third Party Risk Management

Organization has set up processes to manage the third party or business associate relationship lifecycle. The company designates an “owner” to manage the relationship with the third party and ensure compliance with our security requirements and obligations.

Third Party Onboarding

Organization has set up a process for onboarding new third parties or business associates with the company, which includes designating a third party relationship owner and adding the organization to the Third Party Inventory.

Third Party Monitoring and Review

Organization has set up processes for monitoring or auditing the products or services provided by third parties or business associates, as well as their compliance with our security agreements.

Third party relationships are periodically reviewed, and any changes resulting from that review are reflected in the Third Party Inventory.

Third Party Noncompliance or Incident Reporting

Organization has set up processes for responding to third party issues or noncompliance. Workforce members should report suspected incidents through the standard incident reporting process or contact the Security Official directly.

Third Party Offboarding

Organization has set up processes for terminating third party or business associate relationships. Termination processes include removing third party access and updating the Third Party Inventory.

PROCEDURES

This Business Associate and Third Party Risk Management Policy and Procedure must be reviewed and updated at least annually. The reviewer will record the date that the review was completed.

Third Party and Business Associate Agreements (BAAs)

Organization retains written third party and/or business associate agreements for each third party vendor, service provider, or partner.

Business associate agreements must include commitments from the BA to:

- Set up policies and processes to address the HIPAA Security Rule's requirements
- Provide HIPAA security training to all employees
- Perform a regular, documented HIPAA risk analysis to determine if PHI and *ePHI* are appropriately protected
- Report and disclose security incidents or events that could impact Organization within 30 days of notification or sooner if reflected in the BAA, or as required by the HIPAA Breach Notification Rule
- Uphold and adhere to the requirements of the HIPAA Security Rule and other security measures outlined in the agreement

When possible, seek inclusion of MFA enforcement.

Due Diligence and Vendor Selection

Cross-functional stakeholders work together to determine the criteria and standards that third parties and business associates must meet to be selected. Some criteria that should be considered as part of the vendor selection process are:

- Financial considerations, including cost, upkeep, and budget
- Compliance risks, including adherence to the HIPAA Security Rule and third party or business associate agreements
- Industry standards and best practices
- Resources and capabilities available to the company
- Alternative solutions, products, or services

As part of due diligence, Organization obtains any attestations or certifications held by the third party, such as SOC 1 or SOC 2 Type II reports, ISO certifications, HITRUST certification, or others. We review these reports or certifications and incorporate any findings into the overall vendor selection process. Reviewers of third party reports and certifications must record their findings and justification for their recommendations and retain this documentation as part of the Third Party Inventory. It can be uploaded to the vendor record in the Vendor module of the Guard.

Due Diligence Questionnaires In the event that a third party does not have a relevant third-party attestation, report, assessment, or certification to indicate their compliance with an industry standard, the company may issue a custom “Due Diligence Questionnaire” that covers topics of interest to Organization. The Guard has a questionnaire available.

Third Party Inventory

Organization maintains a Third Party Inventory, Repository, or Database that lists all third party organizations, business associates, partners, vendors, suppliers, and contractors that the company does business with. Organization tracks this information in the Guard Vendor module or alternate tracking tool. The Third Party Inventory should contain or link to the following details and information about each organization:

- Third party name and description
- Third party relationship owner
- Third party contact information
- Signed contract or agreement
- Risk rating, based on the criticality of the third party’s products or services to **Organization’s** operations
- Review notes
- Due diligence documentation

The company may opt to track other parameters as well.

Third Party Risk Management

Organization’s Third Party Risk Management process and lifecycle includes third party onboarding, monitoring and review, and offboarding. These steps may occur simultaneously for different third parties.

Third Party Onboarding

When a new third party or business associate enters into an agreement with Organization, they are added to the Third Party Inventory.

If any access is required for third party users or services, the relationship owner will submit requests and follow the company’s Data Security Policy - Access Control on behalf of the third party.

The relationship owner facilitates access requests to the third party’s resources, applications, or services as needed.

Third Party Monitoring and Review

The company regularly monitors the performance of third parties, as well as their compliance with the written agreement.

At least annually, third party contracts, agreements, and relationships are reviewed, and any observations or changes resulting from that review are reflected in the Third Party Inventory.

Third Party Noncompliance or Incident Reporting

If a third party is found to be in noncompliance, Organization will first attempt to address the issue. Business associates that fail to comply with HIPAA requirements may be terminated, or have findings reported to the Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR) within 30 days of the incident.

If an Organization workforce member receives a report or complaint of third party or business associate noncompliance, that event should be reported promptly through defined incident reporting channels, or directly to the Security Official. The Security Official is responsible for responding to the situation and initiating Incident Response and Reporting procedures.

The third party relationship owner will work with the third party for support, troubleshooting, and customer service as needed.

Third Party Offboarding

When a third party or business associate needs to be offboarded or terminated for any reason, all access to Organization's information and assets must be removed upon notification. Changes to that third party's status are updated and reflected in the Third Party Inventory.

The third party relationship owner should work with cross-functional stakeholders, such as Accounting and Legal, to coordinate the termination of third party payments and ensure that all legal considerations are addressed.

ROLES AND RESPONSIBILITIES

Security Official: Receives complaints or reports related to third party or business associate noncompliance or failure to safeguard ePHI. Responds to third party security incidents or delegates responsibilities.

Third Party Relationship Owner: Maintains the company's relationship with designated third party organizations. Ensures third party compliance with contractual agreements and HIPAA Security Rule requirements. Monitors third party performance and reports incidents as needed.

VIOLATIONS

Business associates that fail to comply with HIPAA requirements may be terminated, or have findings reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) within 30 days of the incident.

FORMS/PLANS/DOCUMENTS

- Third Party Inventory. The Guard's Vendor Module can be used create this.
- Business Associate Agreement or Third Party Agreement Templates are available in the Guard document module.

RELATED POLICY

- *Data Security Policy - Security Management*

RELEVANT HIPAA REGULATIONS

- § 164.308(b)(1) *Business associate contracts and other arrangements*
- § 164.308(b)(3) *Written contract or other arrangement*

RELEVANT SOC 2 CRITERIA

- CC9.2.1 *Establishes requirements for vendor and business partner engagements*
- CC9.2.2 *Assesses vendor and business partner risks*
- CC9.2.3 *Assigns responsibility and accountability for managing vendors and business partners*
- CC9.2.4 *Establishes communication protocols for vendors and business partners*
- CC9.2.5 *Establishes exception handling procedures from vendors and business partners*
- CC9.2.6 *Assesses vendor and business partner performance*
- CC9.2.7 *Implements procedures for addressing issues identified during vendor and business partner assessments*
- CC9.2.8 *Implements procedures for terminating vendor and business partner relationships*
- CC9.2.9 *Obtains confidentiality commitments from vendors and business partners*
- CC9.2.10 *Assesses compliance with confidentiality commitments of vendors and business partners*
- CC9.2.11 *Obtains privacy commitments from vendors and business partners*
- CC9.2.12 *Assesses compliance with privacy commitments of vendors and business partners*