Security Management Process

Statement of Policy

To ensure Papaya TPA conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Papaya TPA. Papaya TPA shall conduct an accurate and thorough risk analysis to serve as the basis for Papaya TPA's RELEVANT AUTHORITY REQUIREMENT Security Rule compliance efforts. Papaya TPA shall re-assess the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business Papaya TPAs and technological advancements.

Procedure

a. Security Officer Responsibilities

The Security Officer shall be responsible for coordinating Papaya TPA's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.

b. Risk Analysis Process

i. Document Current Information Systems

a) Information Systems Inventory

- Update/develop information systems inventory
- List the following information for all hardware and software:
    - Hardware (network devices, workstations, printers, scanners, mobile devices)
    - Software (operating system, various applications, interfaces)
    - Information to include: date acquired, location, vendor, licenses, maintenance schedule, and function
- Update/develop network diagram illustrating organization's information system network configuration

b) Facility Layout

Update/develop facility layout showing location of:

- Information systems equipment
- Power sources
- Telephone jacks
- Telecommunications equipment
- Network access points
- Fire and burglary alarm equipment
- Storage for hazardous materials

c) Application Licensee Documentation

For each application identified:

- Identify each licensee (authorized user) by job title
- Describe authorization granting process

d) Application Analysis

For each application identified:

1. Data Description
    - Describe associated data
2. Data Source Analysis
    - Determine if data is created internally or received from third party
    - If from third party: identify party, purpose, and receipt method
3. Data Transmission Analysis
    - Determine if data is maintained internally or transmitted to third parties
    - If transmitted: identify party, purpose, and transmission method
4. Criticality Assessment
    - Define as high, medium, or low
    - Based on impact if application/data were unavailable
5. Sensitivity Assessment
    - Define as high, medium, or low
    - Based on potential harm from breach/security incident
6. Security Controls
    - Identify existing security controls
    - Locate related policies and procedures

e) Threat Assessment

Identify and document threats to ePHI confidentiality, integrity, and availability:

1. Natural Threats
    - Earthquakes
    - Storm damage
2. Environmental Threats
    - Fire and smoke damage
    - Power outage
    - Utility problems
3. Human Threats

    - Accidental acts
        - Input errors and omissions
        - Faulty programming/processing
        - Software/security update failures
        - Resource inadequacies
    - Inappropriate activities
        - Conduct violations
        - Privilege abuse
        - Workplace violence
        - Asset waste
        - Harassment
    - Illegal operations
        - Eavesdropping
        - Snooping
        - Fraud
        - Theft
        - Vandalism
        - Sabotage
        - Blackmail
    - External attacks
        - Malicious cracking
        - Scanning
        - Demon dialing
        - Virus introduction

4. Vulnerability Assessment

    - Identify system vulnerabilities
    - Conduct self-analysis using standards and specifications
    - Document findings

f) Risk Evaluation

1. Probability Assessment

    - "Very Likely" (3): Probable chance of occurrence
    - "Likely" (2): Significant chance of occurrence
    - "Not Likely" (1): Modest/insignificant chance of occurrence

2. Criticality Assessment

    - "High" (3): Catastrophic impact, significant records affected
    - "Medium" (2): Significant impact, moderate records affected
    - "Low" (1): Modest impact, some records affected

3. Risk Scoring

    - Multiply probability and criticality scores
    - Prioritize higher risk scores

g) Security Measures

- Identify appropriate security measures
- Document safeguards for key vulnerabilities
- Focus on high-risk items and Security Rule requirements

h) Implementation Strategy

1. Timeline development
2. Cost assessment and funding
3. Responsibility assignment
4. Implementation adjustments
5. Completion documentation

i. Effectiveness Evaluation

- Evaluate implemented measures
- Make necessary adjustments

c. Follow-up Evaluations

Security Officer Responsibilities

- Identify evaluation timing
- Coordinate evaluations
- Select evaluation team members

Evaluation Triggers

Conduct evaluations upon:

- Changes in Security Regulations
- New laws/regulations affecting ePHI security
- Technology/environmental/business process changes
- Serious security incidents

Evaluation Components

1. Administrative and Physical Safeguards
    - Employee compliance interviews
    - After-hours security inspections
    - Policy/procedure review
    - Log analysis
2. Technical Controls
    - Network assessment
    - Operating system evaluation
    - Application security review

- Vendor engagement as needed