HIPAA SECURITY SERVICE

Overview

The Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect the privacy and security of patient information. It is a healthcare organization's responsibility to implement safeguards that ensure patient information is properly protected.

Infinity Partners Group, LLC has put together a HIPAA Security Service that helps healthcare organizations identify and implement the proper safeguards to protect patient data and to comply with the HIPAA regulations. The HIPAA Security Service consists of the following:

1. Creation of 18 custom HIPAA security policies and procedures

2. Perform and document a detailed HIPAA Security Risk Assessment

3. Provide online training and compliance testing to all employees

4. Access to the HIPAA Compliance Portal (12 months)

1. Policies and Procedures

The HIPAA Security Service provides 18 policies and procedures that address the HIPAA security administrative, physical, and technical safeguards. Each policy and procedure is a separate Microsoft Word document. The policies and procedures are customized with the name of the organization. Most organizations do not require additional changes or customizations. Additional changes and customizations are available if required but are outside the scope of this proposal.

Administrative policies and procedures

The administrative policies and procedures address the following:

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedure
- Contingency Planning
- Evaluation

- Business Associate Contracts

Physical policies and procedures

The physical policies and procedures address the following:

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Control

Technical policies and procedures

The technical policies and procedures address the following:

- Access Control
- Audit Control
- Person or Entity Authentication
- Transmission Security

2. Security Risk Assessment

A detailed Risk Assessment is required under the HIPAA Security Rule.

> The Security Management Process standard in the Security Rule requires organizations to “implement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. § 164.308(a) (1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a) (1) (ii) (A) states:
>
> RISK ANALYSIS (Required).
> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the [organization].

Infinity Partners Group will perform an administrative, physical, and technical assessment against the HIPAA Security Regulations. The Risk Assessment follows the methodology described in NIST Special Publication (SP) 800-30.

Risk Assessment Process

1. Identify and document all electronic protected health information (ePHI) repositories. Evaluate every system that stores, receives, maintains, or transmits ePHI.

2. Identify and document potential threats and vulnerabilities to each repository. Threats include fire, flood, stolen laptops, etc.

Risk Assessment Process

3. Assess current security measures. Review the current security measures (safeguards / controls) that are currently in place that are used to mitigate identified risks. Examples of current safeguards include: employee security awareness training, encryption, data backups, disaster recovery, etc.

4. Determine the likeliness of threat occurrence. For each threat and vulnerability to ePHI that has been identified in step 2 of the Risk Assessment procedure, calculate the likelihood of the threat occurring. Existing security measures as identified in step 3 of the Risk Assessment procedure may lower the likeliness of a threat. Existing vulnerabilities as identified in step 2 of the Risk Assessment procedure may raise the likeliness of a threat. Likeliness is expressed in terms of low, medium or high.

5. Determine the potential impact of threat occurrence. For each threat and vulnerability to ePHI, calculate the associated impact of the threat. Impact is expressed in terms of low, medium, or high impact.

6. Determine the level of risk. For each threat and vulnerability to ePHI, calculate the level of risk of the associated threat. The level of risk is calculated by using the likeliness of a threat, as calculated in step 4 of the Risk Assessment procedure and the resulting impact of a threat, as calculated in step 5 of the Risk Assessment procedure. Risk is expressed in terms of low, medium, or high risk.

7. Determine additional security measures needed to lower level of risk. Based on the determination of the level of risk as defined in step 6 of the Risk Assessment procedure, additional security measures (safeguards / controls) may be need to lower the risk.

8. Document the findings of the Risk Assessment. The final step in the Risk Assessment process is to document and publish all of the findings in each of the steps of the Risk Assessment procedure.

The output of the Risk Assessment consists of a 10-15 page Executive Summary as well as a 50+ page detailed report. The Executive Summary is an easy to understand overview that discusses the current state of the overall risk to systems that contain ePHI as well as recommendations to lower the risk to each system. The detailed report looks at each system that contains ePHI and documents the threats to the system, the vulnerabilities to the system, the current safeguards in place to protect the system, and the additional recommended safeguards to lower the risk to the system.

The Risk Assessment report will give a good understanding of the risks to ePHI and provide specific steps and actions that should be taken to lower the risk.

3. HIPAA Security Training and Compliance Testing

Employee training on security and protecting patient information is a requirement under HIPAA regulations.

> STANDARD § 164.308(a) (5) Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
>
> Security training for all new and existing members of the covered entity's workforce is required by the compliance date of the Security Rule. In addition, periodic retraining should be given whenever environmental or operational changes affect the security of EPHI. Changes may include: new or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the Security Rule.
>
> Source: Department of Health and Human Services Security Standards: Administrative Safeguard

The HIPAA security service provides in-depth training on the HIPAA Security Rule as well as advice for best practices in protecting ePHI and patient information. The training is provided in an online format which is both engaging and convenient to staff members.

Training usually takes around 1 hour to complete. Staff members can start a training session stop and resume the session from where they left off. They can take the training during work hours or complete the training at home after hours.

Once staff members have completed the online training, they will take a short 15-20 question online quiz to demonstrate their knowledge regarding the HIPAA Security Rule. If they receive a score of 80% or higher, they will receive a certificate with their name that acknowledges that they have successfully completed the HIPAA Security Training. If they do not receive an 80% score on the quiz they can retake it as many times as they need to.

When the entire staff has completed training, a report can be accessed that lists each of the staff members, the date they took the training and the highest score they received on the training quiz.

4. HIPAA Compliance Portal

The HIPAA Compliance Portal makes it easy to manage all aspects of HIPAA security compliance. The compliance portal will store the 18 HIPAA security policies and procedures. Employees will be able to access the policies and procedures, read summaries of each of the policies and procedures, and watch short entertaining videos that describe each policy and procedure.

In addition, the HIPAA compliance portal has the ability to upload other policies and procedures and important documents such as HIPAA privacy policies and procedures, disaster recovery procedures, HR policies and procedures, etc. Employees can access all the policies and procedures via the HIPAA compliance portal.

Administrators of the HIPAA compliance portal can utilize the functionality to perform the following functions:

1. Access the HIPAA security risk assessment documents.

2. Track and maintain all business associates including uploading any business associate agreements.

3. Track electronic protected health information (ePHI) that enters or leaves the organization.

4. Capture and record any security incidents that affect patient data or ePHI.

5. Provide HIPAA security training to new employees.

6. Track repairs or maintenance to critical area such as server rooms and other areas that store sensitive ePHI.

7. Access employee HIPAA security training reports.

LIMITATION OF LIABILITY

The HIPAA Security Service does not guarantee compliance with the HIPAA Security Rule. The service provides education and tools to help implement the HIPAA Security Rule. The HIPAA Security policies and procedures are a foundation for implementing the Security Rule. It is the organization's responsibility to ensure that all employees comply with the policies and procedures. In addition, the HIPAA Security risk assessment identifies areas that the organization need to concentrate on to further protect electronic protected health information (ePHI, or better known as patient information). It is the organization's responsibility to use the risk assessment and implement the recommendations to further protect ePHI. It should also be noted that the HIPAA Security Service is not legal advice. Consult with legal counsel to ensure a full legal interpretation of the law.