Health Center Security & Compliance System Implementation Guide

VERSION 1.0 - 2019

HITEQ Center

Table of Contents

1 Introduction

There are ever-increasing cybersecurity guidelines and protection measures that Health Centers must navigate and digest. Newer and rurally located Health Centers can especially benefit from guidance and decision support that assists them in determining how to implement systems in a manner that meets compliance requirements and doesn't expose information to undue security risk. Identifying and managing these types of risk can be especially important when procuring new Health IT (e.g. EHRs, Medical Devices, Data Warehouses) for the Health Center. This toolkit provides a framework for Health Centers to evaluate compliance and security concerns as they purchase, adopt, and implement technology solutions.

Every time a Health Center adopts and implements newly procured technology, they could be exposing themselves to compliance gaps and security risks. Often these topics are addressed after the solution is implemented and are an after-thought. Unfortunately, the later in the adoption process that security is considered, the costlier it becomes to address as it may require redesign or reconfiguration of software, systems, and processes.

Especially important for covered entities, like Health Centers, is for this process to meet the regulations outlined within HIPAA. Throughout this document, the related HIPAA requirements are highlighted within each section so as to better understand where this process sits within broader security risk assessment (SRA) practices. In the Appendix of this guide is an EHR/Health IT Systems checklist that can be used as an implementation interview guide when procuring new resources.

This guide can help organizations identify security concerns and design the appropriate solution starting at the design and vendor-selection phase, thereby increasing the likelihood that security will be considered fully throughout the implementation process.

2 System Overview

The first step in understanding requirements and design for security of the system is to understand the scope of the system being implemented. If the system's role within the Health Center is clearly defined, it is much easier to determine areas to address for security. For example, if the organization is implementing an EHR, then it will be important to understand who will actively be using the system and for what types of activities.

Whereas if the Health Center is implementing a new networked printer then a different set of security risks will need to be defined. It is critical for each of these scenarios to determine appropriate access controls, where data will flow, and what potential risks are included.

Organizations can start by asking key stakeholders the following questions:

- What problem is being solved with this system?
- Who or what business unit within operations owns the IT/system?
- Who will be supporting, managing, and maintaining the IT/system?
- Who will be using the IT/system and for what purposes?
- How will the IT/system be accessed? Are there requirements for remote or mobile access?
- With what other IT/systems or organizations will this system interact?

3 Information Classification & Inventory

Reference: HIPAA Security Rule 164.308(a)(7)(ii)(E) Application and Data Criticality Analysis

Understanding the information that is stored in the system and how it will be used is critical to determining appropriate security controls. For example: Will the system store electronic Protected Health Information (ePHI)? If so, to where will it be transmitted and what third parties will have access? If there is no ePHI, perhaps strict security controls are not as appropriate.

Here are some sample questions to answer as you evaluate the information stored in and used by your system:

- What information will be stored? ePHI? Personally-Identifiable Information? Financial data? Employee confidential data?
- If the organization has a classification policy, how will the information be classified?
- Inventory where the information will be stored including resources such as:
    - Databases
    - File-based data
    - Data exports and backups
    - Cloud-based repositories
    - Training, Test, and Staging systems
- Inventory where the information will be transmitted and how it will be transmitted including resources such as:
    - Vendors such as IT, Application vendor, or backup provider
    - Cloud-based backups
    - Remote access by third parties
    - All Business Associates
    - Other healthcare providers

4 Business Associate Agreements and Contracts

Reference: HIPAA Security Rule 164.308(b)(4)(A) Business Associate Contract or Other Arrangement

Based on the information gathered in the Information Classification and Inventory section, determine who the Business Associates (BAs) are. This should include any third party that "*performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity*."

As you address this area, evaluate the following questions:

- Are all vendors, including Business Associates, monitored on an ongoing basis as part of the organization's vendor management process?
- If Business Associate Agreements (BAAs) are required, are they in place?[1]
- Do the BAAs require review by legal counsel?
- Evaluate BAAs for:
    - Permitted Uses and Disclosures
    - Permissible Requests by the Covered Entity
    - Termination
        - Can the BA terminate without cause?
        - Who owns the data when the contract is terminated?
        - For cloud providers, does the organization have a right to download/export data on termination?
    - Is the BA required to report all successful and unsuccessful security incidents to the Covered Entity?

5 Risk Analysis

Reference: HIPAA Security Rule 64.308(a)(1) Risk Analysis

The HIPAA Security Rule requires that organizations conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization. In addition, the

[1] Sample BAA contracts can be found here: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

HIPAA Security Rule requires that organizations update their security controls as the environment changes. Therefore, it is extremely important that threats, vulnerabilities, and risks be evaluated as the system is implemented. This resource, while not a replacement for a proper Security Risk Analysis, can serve as a useful tool to help evaluate these areas as systems are implemented. Consider threats to confidentiality, integrity, and availability as part of your risk analysis.

As part of your Risk Analysis of the new Health IT or system consider:

- Threats
  - Insider, Trusted Third-Party, Outsider
  - Malicious vs Accidental
  - Environmental threats such as weather, flooding, or fire
  - Technical, Physical, and Administrative threats
- Vulnerabilities
  - Technical Vulnerabilities (can be assessed through vulnerability scans and penetration testing)
  - Information-related (what information is being handled and by whom?)
  - Operational or Environmental
- Impact
  - What would be the impact to the organization or its patients in the event of a failure in confidentiality, integrity, or availability of the information?
- Security Controls
  - What security controls are in place to address the identified threat-vulnerability pairs?

6 Identity Management

Reference: HIPAA Security Rule 164.308(a)(4)(ii) Information Access Management
HIPAA Security Rule 164.312(a)(2) Access Control

Understanding the users and responsibilities for managing identities within the system is critical to protecting the system from unauthorized access.

When implementing the system, address the following questions:

- Does the system integrate into the organization's existing identity management system (e.g. Active Directory, Google)?
- Who are the users?
- How can the users be separated into groups with different access needs?
- Who requires administrative access?

- What is the process for requesting and approving new users or users with changes in roles?
- How are changes to permissions approved, documented, and monitored?
- How are users getting removed when they no longer require access (e.g. on termination or role change)?
- How are users authenticated? Is multi-factor authentication available for remote access or privileged access?

The identity management solutions and processes should be reviewed in relation to existing policies and procedures to ensure they align.

7 Encryption

Reference: HIPAA Security Rule 164.312(a)(2) Encryption and Decryption
HIPAA Security Rule 164.312(e)(2) Transmission Security

The HIPAA Security Rule requires that data be encrypted at rest and in transit where deemed reasonable and appropriate. In addition, if information is compromised, for example with a lost or stolen laptop, hard drive, or backup tape, organizations can avoid breach notification if the information is appropriately encrypted (https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html).

Using the information gathered in the *Information Classification and Inventory*, evaluate for each location where ePHI is stored or transmitted:

- Is encryption technology available? If so, it should be enabled barring extenuating circumstances.
- Does the encryption technology meet the standards outlined in the referenced HHS Guidance?
- How are encryption keys managed? Where are they stored? Who has access to them? Where are they backed up?
- If encryption is not deemed reasonable or appropriate:
    - What compensating controls can be put in place? For example, strong physical security, enhanced monitoring and tracking.
    - Document the reasoning as part of the risk assessment. Revisit this decision each time the risk assessment is reviewed and updated.

8 Auditing and Logging

Reference: HIPAA Security Rule 164.312(b) Audit Controls
HIPAA Security Rule 164.308(a)(1)(ii)(D) System Activity Review

Auditing and Logging are critical to the detection and investigation of security events. Even when organizations have audit logs, very often they fail to use them to proactively detect security events. The HIPAA Security Rule requires that organizations maintain audit logs and take proactive steps to review system activity to detect unauthorized activity.

When implementing a system, ensure the following questions are addressed:

- What audit logs are available and where are they stored?
- Can they be integrated into an existing log management system?
- How long will they be retained and where will they be backed up?
- How will the logs be used to detect unauthorized activity? Will this include manual review, automated tools, or both?
- What does unauthorized activity look like?
    - Snooping – Family, coworkers, neighbors, VIPs. Reports and alerts can be created for sensitive charts
    - Excessive chart accesses or downloads
    - Unauthorized prescriptions
    - Access from a new or unknown location
    - Off-Hours login by an individual who would not normally be logging in during those hours

9 Contingency Plan

Reference: HIPAA Security Rule 164.308(a)(7)(ii) Contingency Plan

Plan for the unexpected, because issues will occur at some point. Consider the following:

- How will the system be backed up?
- How will it be restored?
- How much data may be lost in the event of failure? For example, if daily backups are occurring, up to one day's worth of data could be lost.
- How long does it take to recover? Is this acceptable to the operations?
- What procedures are in place for when the system is unavailable?
- Schedule a test restore during system implementation

10 Workstation Requirements

Reference: HIPAA Security Rule 164.310(b) Workstation Use
HIPAA Security Rule 164.310(c) Workstation Security

Compromised workstations are often an attacker's initial foothold into an organization. Efforts should be taken to understand what workstations (that includes laptops, tablets, and smartphones) will be used to access the system and what security controls are in place.

The following questions should be considered:

- What types of devices will be used to access the system?
- What Operating Systems will be used?
- What are the organization's policies for security controls on the workstations?
- What supporting software and what version of that software is required (e.g. Java, Flash, .Net Framework)?
    - Do those versions have any known vulnerabilities?
- How is the workstation software updated?

11 Patching

Reference: https://www.hhs.gov/hipaa/for-professionals/faq/2014/does-the-security-rule-mandate-minimum-operating-system-requirements/index.html

System implementation planning should consider what happens beyond the initial roll-out. Ensure plans are in place to address the following:

- How is the third-party software updated? Is this performed by the vendor or the health center?
- Will release notes be provided to the organization in advance so that changes to workflows or user training can be incorporated?
- Is there a Test or Training environment available to try out updates before they are released to production?
- What Operating Systems are used on servers and devices? For example, does a medical device have an underlying operating system that needs to be patched or is it connected to a dedicated vendor-managed laptop? Who is responsible for patching these devices?

12 Security Testing

Reference: HIPAA Security Rule 164.308(a)(8) Evaluation
HIPAA Security Rule 164.308(a)(1)(ii)(A) Risk Analysis

Security Testing usually takes the form of vulnerability and penetration testing. Vulnerability Testing is generally an automated process that involves running a vulnerability scanning tool against a set of IP addresses and reviewing the results. This can be an extremely quick and easy way to determine if your system has any glaring vulnerabilities. These scans can be performed on external Internet-facing systems or on the local network. It used to be that these types of scans were reserved for large organizations or highly-sensitive systems, but through automation and Software-as-a-Service (SaaS) scanning services available, these types of scans can be a quick and affordable way to monitor systems for known vulnerabilities.

Penetration Tests are generally more involved and require an experienced tester to evaluate systems' security to determine paths of entry. This can involve technical testing against Internet-facing systems, but also social engineering and physical testing. These types of tests are generally more expensive and not as common. One simple test that many organizations are starting to perform, though is Phishing Tests where employees are sent a phishing email to both test and train them on what to look for. This is a great value since many current attacks, including Ransomware, come in through phishing.

When implementing a system, consider the following:

- What systems will be Internet-facing?
- Is it reasonable to set up regular automated vulnerability scans?
- Consider performing security testing prior to go-live
- Will the organization perform penetration testing?
- How does the vendor perform security testing prior to release?

13 Vendor and Developer Access

Reference: HIPAA Security Rule 164.308(a)(3)(ii) Workforce Security
HIPAA Security Rule 164.308(a)(4)(ii) Information Access Management

Third party access to systems can be a risk to organizations. Whether it be malicious intent on the part of a vendor's employee, compromised vendor systems leading to access to an organization's systems (See Target breach), or unauthorized maintenance on a system causing unexpected downtime, there are numerous threats that can be exercised through vendor access.

When implementing the system, consider the following:

- Will the vendor or developers have access to production systems?
- If so, how will this be controlled and/or monitored?
- Is the access perpetual (i.e. always on), or enabled as needed?
- Is there a process for requesting and approving vendor/developer access?

- Will there be multi-factor authentication (this may have saved Target)?
- How is access terminated for vendor employees who leave the organization?

14 Physical Security

Reference: HIPAA Security Rule 164.310(a)(2) Facility Access Controls

Physical access to data is important to evaluate as the system is being designed and implemented. For each type of data identified in the inventory, physical security controls should be considered.

Organizations should address the following:

- Who has a need to have physical access? Is access restricted to only these individuals?
- What are the security controls protecting access to the data?
- Are physical power protections in place to facilitate the required availability of information?
- How is information protected from environmental threats such as fire and flood?
- Where are removable media such as USB drives or backup tapes stored?

15 Network Segmentation

When implementing sensitive systems such as medical devices, consider placing devices on dedicated, private network segments that protect the devices from general-use systems such as workstations, laptops, phones, and even servers. Limit Internet connection as appropriate.

Systems that are especially sensitive such as medical devices should be placed on a dedicated private network segment. This is one of the best ways organizations can protect against the spread of malware such as Ransomware and prevent attackers from pivoting from workstations to more critical systems.

Ask the following questions as you consider placement of new systems and devices on the network?

- What does the system need to communicate with internally and externally?
- Can the network be segmented into logical segments by system type (e.g. server, data storage, workstation, mobile, printer, medical device) or by role (e.g. EMR, HR, medical device)?

Appendix A: Implementation Checklist

2. System Overview

Question	Response
What problem is being solved with this system?	
Who or what business unit within operations owns the system?	
Who will be supporting, managing, and maintaining the system?	
Who will be using the system and for what purposes? Develop use cases.	
How will the system be accessed? Are there requirements for remote or mobile access?	
With what other systems or organizations with this system interact?	

3. Information Classification and Inventory

Question	Response
What information will be stored? ePHI? Personally-Identifiable Information? Financial data? Employee confidential data?	
If the organization has a classification policy, how will the information be classified?	
Inventory where the information will be stored.	

Inventory where the information will be transmitted and how it will be transmitted.	

4. Business Associate Agreements and Contracts

Question	Response
Are all vendors, including Business Associates, tracked as part of the organization's vendor management process?	
If Business Associate Agreements (BAAs) are required, are they in place?	
Do the BAAs require review by legal counsel?	
Do BAAs contain required content?	

5. Risk Analysis

Question	Response
Has a Risk Analysis been performed or updated for the new system?	

6. Identity Management

Question	Response
Does the system integrate into the organization's existing identity management system (e.g. Active Directory, Google)?	
Who are the users?	
How can the users be separated into groups with different access needs?	
Who requires administrative access?	

What is the process for requesting and approving new users or users with changes in roles?	
How are changes to permissions approved, documented, and monitored?	
How are users getting removed when they no longer require access (e.g. on termination or role change)?	
How are users authenticated? Is multi-factor authentication available for remote access or privileged access?	

7. Encryption

Question	Response
Is encryption technology available? If so, it should be enabled barring extenuating circumstances.	
Does the encryption technology meet the standards outlined in the referenced HHS Guidance?	
How are encryption keys managed? Where are they stored? Who has access to them? Where are they backed up?	
If encryption is not deemed reasonable or appropriate	
If encryption is not deemed reasonable or appropriate, has this been documented and are compensating controls in place?	

8. Auditing and Logging

Question	Response
What audit logs are available and where are they stored?	
Can they be integrated into an existing log management system?	
How long will they be retained and where will they be backed up?	
How will the logs be used to detect unauthorized activity? Will this include manual review, automated tools, or both?	
What does unauthorized activity look like?	

9. Contingency Plan

Question	Response
How will the system be backed up?	
How will it be restored?	
How much data may be lost in the event of failure? For example, if daily backups are occurring, up to one day's worth of data could be lost	
How long does it take to recover? Is this acceptable to the operations?	
What procedures are in place for when the system is unavailable?	
Schedule a test restore during system implementation	

10. Workstation Requirements

Question	Response
What types of devices will be used to access the system?	
What Operating Systems will be used?	
What are the organization's policies for security controls on the workstations?	
What supporting software and what version of that software is required (e.g. Java, Flash, .Net Framework)? Do those versions have any known vulnerabilities?	
How is the workstation software updated?	

11. Patching

Question	Response
How is the third-party software updated? Is this performed by the vendor or the health center?	
Will release notes be provided to the organization in advance so that changes to workflows or user training can be incorporated?	
Is there a Test or Training environment available to try out updates before they are released to production?	
What Operating Systems are used on servers and devices? For example, does a medical device have an underlying operating system that needs to be patched or is it connected to a dedicated	

vendor-managed laptop? Who is responsible for patching these devices?	

12. Security Testing

Question	Response
What systems will be Internet-facing?	
Is it reasonable to set up regular automated vulnerability scans?	
Consider performing security testing prior to go-live	
Will the organization perform penetration testing?	
How does the vendor perform security testing prior to release?	

13. Vendor and Developer Access

Question	Response
Will the vendor or developers have access to production systems?	
If so, how will this be controlled and/or monitored?	
Is the access perpetual (i.e. always on), or enabled as needed?	
Is there a process for requesting and approving vendor/developer access?	
Will there be multi-factor authentication?	
How is access terminated for vendor employees who leave the organization?	

14. Physical Security

Question	Response
Who has a need to have physical access? Is access restricted to only these individuals?	
What are the security controls protecting access to the data?	
Are physical power protections in place to facilitate the required availability of information?	
How is information protected from environmental threats such as fire and flood?	
Where are removable media such as USB drives or backup tapes stored?	

15. Network Segmentation

Question	Response
What does the system need to communicate with internally and externally?	
Can the network be segmented into logical segments by system type (e.g. server, data storage, workstation, mobile, printer, medical device) or by role (e.g. EMR, HR medical device)?	

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $535,717 with 0 percent financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.