THE BEST GUIDE TO THE HIPAA SECURITY RULE YOU'LL EVER READ

LET HALOCK HELP YOU NAVIGATE THE LATEST VERSION OF THE HIPAA SECURITY RULE

HALOCK®
Purpose Driven Security

TABLE OF CONTENTS

Who Should Read This Guide?

If you have some responsibility in your organization for complying with the HIPAA Security Rule, then this guide is for you.

HALOCK Security Labs wrote *The Best Guide to the HIPAA Security Rule You'll Ever Read* in a style that is useful to a wide readership, including compliance professionals, technologists and non-technical managers.

What is the Purpose of this Guide?

The goal of this guide is to show you what you need to do in order to comply with the latest version of the HIPAA Security Rule. More specifically, the guide is designed to translate federal legalese into practical guidance in order to reveal a little-understood principle of the Security Rule which makes it more practical than is commonly believed. This guide was written to provide two benefits to its readers:

1. To be immediately useful in helping your organization understand the latest requirements of the HIPAA Security Rule.
2. To help you and your organization understand that your organization's unique risk profile creates the standard for your compliance program; not a checklist.

HALOCK has found that the first, most significant challenge that organizations face while addresing the HIPAA Security Rule is that they do not understand what the regulation is actually asking organizations to do. For instance, the Office for Civil Rights recently found that two-thirds of the organizations they audited did not understand that compliance was supposed to be based on their risks[1], and not on a checklist. This means that more times than not organizations are not setting the right compliance goals for themselves, and either fall short of compliance or over-extend themselves as a result.

Not that this is the fault of people who are trying to comply. The HIPAA Security Rule is not the easiest regulation to read and understand in its native format. The Security Rule is officially stated in a Code of Federal Regulations (45 CFR Part 160, and Part 164 Subparts A and C). If you think the citation is confounding, try reading the actual document[2]. It is a small-font, three columned tome that reads like a bureaucrat's history of drafts, comments, status of comments; then, at last, only the revised specifications of the regulation. Because of the regulations arcane format, readers who want to know all of the specifications of the Security Rule must read the previous versions of the CFR as well.

The HIPAA Security Rule is not the easiest regulation to read and understand in its native format.

[1]*Sanches, Linda. "HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis". PowerPoint PDF. Health Care Compliance Association, April 23, 2013, September 16, 2013*

[2]*Health Information Portability and Accountability Act, 45 CFR Parts 160 and 164, 2013*

And as if the document format was not enough of a challenge to the uninitiated reader, further confusion comes into play when you try to understand the degree to which you must implement the specifications. CFRs are notoriously difficult to interpret. Given that there have been two updates (also stated in CFR format), the public is left to read through three generations of revision commentary and outdated text to understand their obligations. But once you do understand the Security Rule, you'll find that it is easier to comply with than you may have originally thought.

Because HIPAA is officially only described in a CFR, the public looks instead for easy-to-read guides, explainers, crib notes and cheat sheets. In conducting our own research, we read through many of these publicly available documents and found that they provide the wrong guidance.

SURPRISING FACTS ABOUT THE HIPAA SECURITY RULE

- You can be too compliant.
- You can actually calculate "reasonable and appropriate."
- Only encrypt information that creates a risk.
- You can accept some ePHI risks.
- Risk assessments exist to make compliance easier.

The most common misunderstanding of the HIPAA Security Rule, even among the security community, is that it is a list of security requirements that must be achieved as-written in order to meet compliance. That is wrong. The HIPAA Security Rule is a requirement that tasks your organization with asking the question, "What damage could result if we don't care for the information we have?" and, "What is a reasonable thing for us to do to prevent that damage?" Then it requires that you answer the question with a list of reasonable and appropriate safeguards that you will implement, oversee and correct if they fail to be effective.

As information security consultants that have worked with covered entities, business associates and attorneys to help them understand and attain HIPAA Security Rule compliance we decided to translate the Security Rule's requirements for you with citations to the sources for your own fact-checking convenience.

We have broken down the Security Rule specifications into a revision of the table-format that Health and Human Services Office of Civil Rights (OCR) provides. We then added a column to the table, "What This Means," to advise you on how to apply the specification in a way that is compliant, and that you can manage. You will find that achieving these specifications is easier to accomplish when you address them as risk mitigation, rather than as checklist goals.

Why is HIPAA Easier than Commonly Thought?

Because many people mistake the HIPAA Security Rule for a checklist of compliance, they conduct gap assessments and audits to determine how compliant they are. Of course this kind of oversight is critical for running a security or compliance program, but if you are not analyzing compliance based on risk, then you are very likely giving yourself too much work to do.

The risk assessment requirement of the HIPAA Security Rule[3] is telling you to not only understand your compliance gaps with the security rule specifications, but to know why those gaps matter[4]. The risk assessment process causes you to ask the following question: "If I don't have appropriate security controls over this database or this patient data, what threat could compromise it? What would be the likelihood and impact of that event, and what safeguard would bring that likelihood and impact down to a reasonable level?"[5]

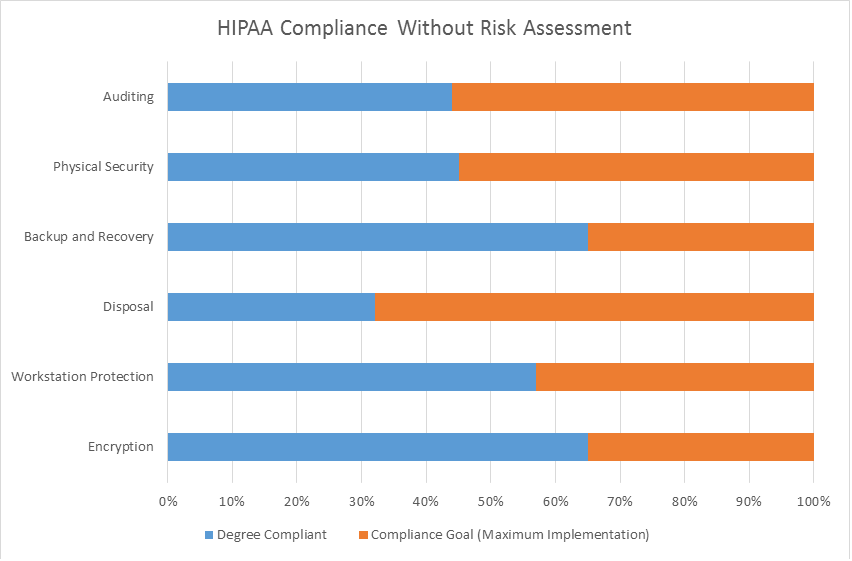
To some, this question may seem to be an unnecessary step to take on your way to implementing required security controls. But think of what this means. The answer to the question, "what safeguard would bring that likelihood and impact down to a reasonable level?" is not "everything possible." The answer is "something that is demonstrably reasonable."

Let's take a look at how an organization would approach HIPAA Security Rule compliance first without a risk assessment, then with a risk assessment.

In Figure 1 we see what a compliance audit looks like when the organization relies on gap assessments, rather than risk assessments. An assessor or auditor will read the straight language from the Security Rule, examine the organization's security practices, then use their judgment as to whether the security practices were sufficient.

As a result, the organization's target of compliance for a security specification is always 100% of a control. If they have some patient-related databases encrypted and others not, then they calculate their compliance based on the population of encrypted over unencrypted databases. There may be no determination as to why it matters that some patient-related databases are not encrypted, but there is the goal to get them all encrypted to be "compliant."

Figure 1



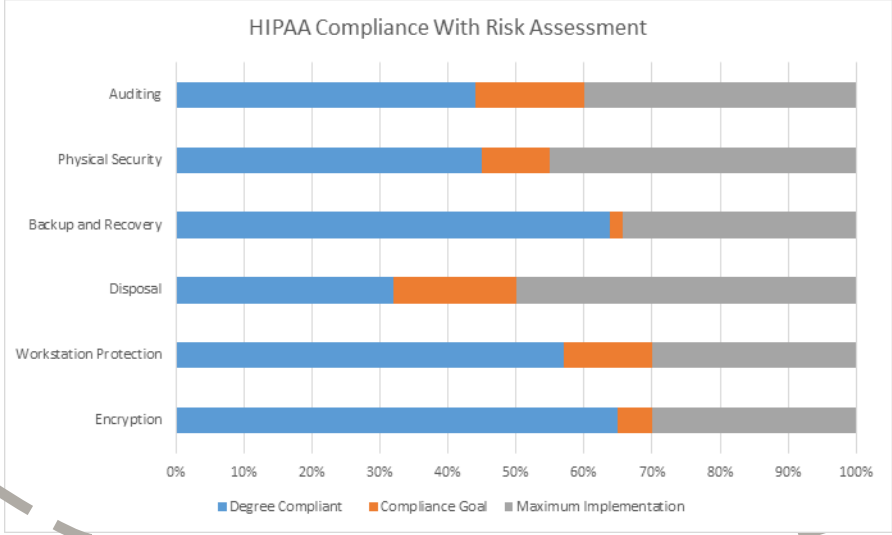
[3] 45 CFR 164.308(a)(1)(ii)(A) [4] 45 CFR 164.306(d)(3)(i) [5] Office of Civil Rights. "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" Department of Health and Human Services. Web. July 14, 2010, September 16, 2013

For the record, the compliance goal that this figure represents would likely be “too much.”

But when the organization conducts risk assessments, they will have calculated their “duty of care”: the degree to which they must protect ePHI (Electronic Protected Health Information). What that means for organizations is that they are able to demonstrate that their investments in security are responsible; that they applied “due care” over the ePHI. This of course means that security investments would be lower than the more common (and incorrect) approach, and it means that security investments are prioritized in all of the right places.

As a result, that organization’s target compliance requires less than 100% implementation of controls, as seen in Figure 2. Note that the “degree compliant” in Figure 2 doesn’t change from the first scenario. But the amount of required security investment changes significantly.

Figure 2



What Does The HIPAA Security Rule Ask Us To Do?

The HIPAA Security Rule is made up of standards and specifications. Standards are security principles that you need to address. Specifications are the safeguards and controls that you are being told to implement to meet those standards.

You will notice that the specifications are described as either “Required” or “Addressable.” In both of these cases, you must implement safeguards to satisfy the specification, but you know the degree to which you must implement the addressable specifications by conducting your risk assessment.

But even in the case of the required specifications, realize that you will implement them to a reasonable and appropriate degree. Take for instance the “Response and Reporting” specification. This is a required control as you must have an incident response plan in place to help you address breaches in a legally sound manner. But your plan would script your security responses with different degrees of care and thoroughness depending on the risk that a security event exposed you to. A server that fails because it suffers an availability incident will in most cases not require informing authorities. An exposure of 1,000 patient records would require disclosure.

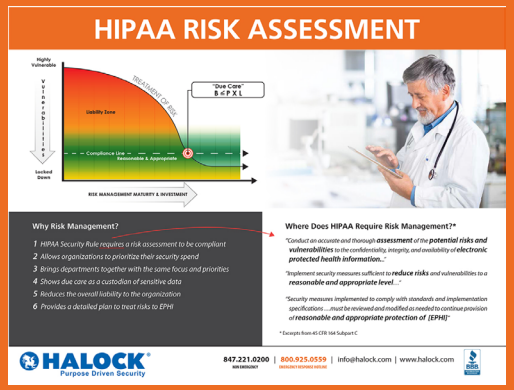
Similarly, you will have a Disaster Recovery Plan (also required) but it will only be applied to the degree that it addresses the need for recovery time and uptime as determined by your Applications and Data Criticality Analysis.

How To Use This Guide

As you review the specifications in the table below, you should be aware that most of the text is provided by the Department of Health and Human Services, and contains the most up-to-date requirements of the Security Rule (as of the release of the Omnibus Rule in March, 2013).

The right-most column of the table, “What This Means” is provided to you by HALOCK to help you understand how you would interpret the specification for your organization. You will notice that much of that content refers to your use of the risk assessment to interpret the specification. This is not by accident. Your goal should be to reach a “reasonable and appropriate” level of risk with your HIPAA Security Rule program. The only way to do that is by analyzing how each safeguard addresses risk in your environment.

WANT TO LEARN MORE ABOUT RISK ASSESSMENTS?



The risk assessment process we describe in this presentation conforms to NIST SP 800-30 and NIST SP 800-37, the risk assessment methodologies referenced by the Department of Health and Human Services, Office of Civil Rights in their risk assessment guidance document.

For further guidance from OCR on risk assessment for HIPAA compliance, visit: http://www.hhs.gov/ocr/privacy/

For additional information on Risk Assessments and Risk Management solutions visit www.halock.com/risk

THE GUIDE

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Administrative Safeguards. A covered entity or business associate must, in accordance with § 164.306: Implement policies and procedures to prevent, detect, contain, and correct security violations.				
Security Management Process	164.308 (a) (1)	Risk Analysis (R)	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 covered entity or business associate.	Risk analysis asks the following questions; What could go wrong? What is the likelihood and impact of it happening? Is that likelihood and impact acceptable? If not, what safeguard should we put in place? Does that safeguard pose an unacceptable risk to the organization or others? Following risk assessment standards, such as NIST SP 800-30 in conjunction with NIST SP 800-37, or ISO 27005, organizations should develop an honest picture of their "duty of care" in their current state, and a plan for attaining that duty of care if they are off the mark. "Acceptable risk" can be clearly defined by including business objectives and security objectives in the risk assessment calculus. This ensures that the business' responsibility is in balance with its capability, as the regulation requires. HALOCK provides guidance for developing a risk assessment that achieves these goals.
		Risk Management (R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)	Implement the security safeguards that were designed in the risk assessment, but also test and monitor those safeguards regularly. Remember that controls must be effective in order to maintain compliance.
		Sanction Policy (R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Ensure that policies describe sanctions against personnel that do not follow them.
Assigned Security Responsibility	164.308 (a) (2)	Information System Activity Review (R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	You will need to put in place methods for checking systems that access, store, transmit or otherwise service ePHI. Done incorrectly, this can be an overwhelming undertaking. To get this right-sized, be sure in your risk assessment to consider which systems to log, what activities to log, what alerts should be raised based on what activities, and how frequently you should review those records. This sounds daunting, but if your assessment systematically asks questions about what could go wrong and where, the requirements for log review almost write themselves.
		Assigned Security Responsibility (R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Do not choose the person for this role casually. This must be a management-level person with the authority to make policies that are enforced throughout all parts of the organization that can access or otherwise process ePHI.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.				
Workforce Security	164.308 (a) (3)	Authorization and/or Supervision (A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Your risk assessment should consider accidents or intentional threats that can occur in locations where ePHI is accessed. Where the impact and likelihood of those threats is unreasonably high, consider the safeguards you would put in place to authorize or supervise personnel that would bring those risks down to a reasonable and appropriate level.
		Workforce Clearance Procedure (A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	The principle of least access applies here. The fewest people accessing the least data necessary. Also, the fewest people with the least ability to change configurations is a great idea. Your risk assessment can help you determine whether a role that personnel serve is "in" or "out" when requesting access. It is appropriate to consider the background and conflicting interests of personnel to determine if they pose a risk to ePHI that they would access.
		Termination Procedures (A)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Your termination procedures should also leave records of when the personnel change was made and of when the access rights were removed.
Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.				
Information Access Management	164.308 (a) (4)	Isolating Health Care Clearinghouse Function (R)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	For a business associate that provides information processing (conversion of information from standard-format to non-standard-format, or vice-versa) on behalf of a covered entity, ensure that these functions are separated from other parts of the business to keep the scope of the HIPAA Security Rule outside of non-ePHI-related activities.
		Access Authorization (A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Ensure that individuals are granted access to ePHI through a procedure that verifies their identity, the appropriateness of their access, and the principles of least privilege. Your risk register will help you determine how rigorous the procedures should be for each asset. For instance, a simple email from a manager may be sufficient for a request for access to a low-risk asset, but in-person access requests with photo ID may be necessary for granting access to high risk assets.
		Access Establishment and Modification (A)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Establish policies and procedures that control how access rights are added or changed. This includes writing and following procedures for administrators who create and alter user accounts.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).				
Security Awareness and Training	164.308 (a) (5)	Security Reminders (A)	Implement a security awareness and training program for all members of its workforce (including management). Periodic security updates.	Develop training materials for personnel who may come into contact with ePHI, or the environment that supports ePHI. The training should be provided to all personnel who enter roles that give them access to ePHI. Also, keep in mind that annual security training is a common requirement in organizations. Your risk analysis should consider at least annual security training for all personnel as reminders of their obligations to secure information. Make their training as meaningful to their role as possible. For instance, special instructions meant for systems administrators should be provided for that audience. Special training for care givers and pharmacists, or for administrative staff should be considered. This ensures that training will be meaningful to audience members. As well, be sure to capture evidence that training occurred for each applicable staff member. Consider security reminders in the form of signs in areas where high-risk ePHI activity occur, and in emails to personnel.
		Protection from Malicious Software (A)	Procedures for guarding against, detecting, and reporting malicious software.	This is an area of risk assessments that may cause you to do more than what you originally planned to do. While anti-virus applications are common now, it is also important to understand the growing and common risk of advanced malware that cannot be detected by most anti-virus applications that are available as the Omnibus Rule was published. Some type of advanced malware threat protection may be necessary for your environment. Again, this is why we do risk assessments, to be sure we're addressing the actual risks, rather than checking off "compliant" boxes.
		Log-in Monitoring (A)	Procedures for monitoring log-in attempts and reporting discrepancies.	Monitoring log-ons as a security practice yields interesting results. Are super-users (root, SA, administrator, etc.) logging into systems and applications? That should cause alarm. Are there several failed attempts at logging into systems and applications? You should know that in case it indicates an attempted breach. During your risk assessment, ask what threats would be indicated by unusual log-in attempts. Then plan to monitor that type of log-in attempt. Again with a good risk assessment, these safeguards almost write themselves.
		Password Management (A)	Procedures for creating, changing, and safeguarding passwords.	Because passwords are the keys to access, we need to carefully manage them; either through providing, changing or storing them. But it is also the case that some password policies can create new risks, If you ask many users to create complex passwords that change every 30 days, they will start to write them down and leave them at their desks (unless you provide them with easy-to-use password managers). In your risk analysis, think through the level of risk that you are addressing by creating password use policies, and compare them to the risks of having too-demanding policies. If you are relying on passwords for access (rather than two-factor authentication or other means), then consider designing the strictest password rules you can design that are still simple for end-users to adhere to. Consider using "password safes" or other tools to assist your end-users.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Security awareness and training. Continued:				
Security Incident Procedures	164.308 (a) (6)	Response and Reporting (R)	Implement policies and procedures to address security incidents. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Develop and test a plan that contains explicit procedures (as well as forms and other supporting documents) that guide management through responding to security breaches. The plan should be designed to support management's adherence to requirements for protecting individuals and for complying with regulations and statutes as an incident occurs.
Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.				
Contingency Plan	164.308 (a) (7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Establish (and implement as needed) procedures to restore any loss of data. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. Implement procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components.	Your risk assessment should help you determine how quickly you need to recover ePHI if it becomes unavailable at certain systems or facilities. Then design methods for backing up and restoring that information to the degree that is appropriate to the risk of having it not available. Ensure that an emergency operations mode is prepared for the time span required to restore access to information. This plan should be tested on a regular basis to ensure that it can be relied upon.
Evaluation	164.308 (a) (8)	Evaluation (R)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	An internal audit function should regularly check to see that safeguards are operating as they are designed. Safeguards that are in place to protect high risks should be tested more frequently and more diligently than those that protect a low risk.
Business Associate Contracts and Other Arrangement	164.308 (b) (1)	Written Contract or Other Arrangement (R)	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. (2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information. (3) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a)	As part of your requirements of each business associate, require that they have conducted a risk assessment that conforms to the guidance provided by the Office for Civil Rights, NIST SP 800-30 or ISO 27005. Also require that they have put in place controls that keep identified risks down to a reasonable and appropriate level, and that they inform you of when those controls are not effective, and that they provide a plan for remediating any identified weaknesses.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Physical Safeguards. A covered entity or business associate must, in accordance with § 164.306: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.				
Facility Access Controls	164.310 (a) (1)	Contingency Operations (A)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	When in your risk assessment you address the emergency plan (to determine how much of an emergency operating plan you will need in order to address availability risks) ensure that you address the physical spaces required to operate, and to restore access to systems and ePHI.
		Facility Security Plan (A)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Consider the physical security risks that your organization faces as well as the technical and procedural. Ensure that physical risks to ePHI are reduced to a reasonable and appropriate level.
		Access Control and Validation Procedures (A)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Ensure that access rights to facilities and physical perimeters that prevent unapproved access to ePHI are designed, implemented and tested so that they reduce risks to a reasonable and appropriate level.
		Maintenance Records (A)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	For barriers and physical security controls that protect against risks to ePHI, ensure that changes to those physical safeguards are approved, and when modified, ensure that they function as designed, and that they effectively reduce risks to ePHI to a reasonable and appropriate level.
Workstation Use	164.310 (b)	Workstation Use (R)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Provide policies and procedures that state the appropriate use of technical systems, such as workstations, and the physical security requirements for the spaces in which this use of systems occurs.
Workstation Security	164.310 (c)	Workstation Security (R)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Physical security requirements should be reviewed in the risk assessment to ensure that the safeguards are appropriate for the risk that they are mitigating. Common physical security controls, such as video cameras and screen protectors should only be put in place if they demonstrably reduce risks to a reasonable and appropriate level.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.				
Device and Media Controls	164.310 (d) (1)	Disposal (R)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Policies and procedures should be in place to destroy ePHI either in its digital format or in its physical formats. It is critical to include in these procedures the recording of disposal events as evidence in case there is a later concern of a breach due to improper disposal. Again, consider what assets require high scrutiny during disposal and which do not by considering the likelihood and impact of a breach for each asset type. In other words, improperly disposed information about configurations of systems that carry ePHI have a lower risk than improperly disposed ePHI, but it also has a higher risk than an employee contact list. Disposal procedures should be aligned with the risk that information poses.
		Media Re-use (R)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	Similar to the above concern, re-purposing electronic media should ensure that ePHI, or configurations that permit access to ePHI, should not allow personnel or systems to access ePHI if they are not authorized to do so. If a team is permitted access to ePHI, then repurposing those assets within the team may pose a lower risk than repurposing the assets outside of the team. It may be reasonable for repurposing procedures to take into consideration the risk posed by each repurposing event.
		Accountability (A)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Tracking the movement of hardware and media, including the change of assignment of those assets, can help determine whether or not a breach has occurred. However, it may not be reasonable for an organization to track all such assets. Ensure that the movement and changed ownership of assets is considered in the risk assessment to determine the degree of record keeping that the organization needs to keep.
		Data Backup and Storage (A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	This should be as simple as ensuring that the data backup processes have functioned correctly prior to moving systems that have ePHI on them. As for accountability, yes, this would be one of those movements you would track.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Technical Safeguards. A covered entity or business associate must, in accordance with § 164.306: (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).				
Access Control	164.312 (a) (1)	Unique User Identification (R)	Assign a unique name and/or number for identifying and tracking user identity.	While this seems easily done and trivial to most organizations, consider two common scenarios: the use of "Power User" accounts, such as dba, sa, root and administrator accounts, and the use of shared work stations. This specification can create real challenges in this scenario. When devising a plan for addressing this specification, ensure that the specification is followed, but consider whether the user account scenarios you put in place can reduce the likelihood and impact of a breach when they are used.
		Emergency Access Procedure (R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Similar to the "Emergency Mode Operation Plan" this specification requires that technical access procedures are in place and operational.
		Automatic Logoff (A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Your risk assessment should address the question of risks to ePHI and to systems if they are left unattended for periods of time. In quasi-public locations, very short automatic log-off periods should be implemented. In highly secured spaces in which ePHI-approved personnel are permitted exclusive access, log-off periods may be appropriately longer. This determination should be recorded in the risk register.
		Encryption and Decryption (A)	Implement a mechanism to encrypt and decrypt electronic protected health information.	The essential goal that the specification is trying to achieve is to ensure that ePHI is only accessible to those who have approved access to it. Encryption is a common and easily accessible means for providing that assurance, but it may not be practical in many cases, especially when information needs to move from one organization to another.
Audit Controls	164.312 (b)	Audit Controls (R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	This is another required specification that must be implemented, but that will be implemented so that it addresses the risks that were called out in the risk register. For instance, if a database application has identified vulnerabilities, your audit controls could be configured to detect the presence of a threat against that application. More critical threats, or threats that require a speedy response, could be aligned to alerting functions in the log management software. When the risk assessment is conducted well, these audit control requirements almost write themselves.

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	Specification Text	What This Means
Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.				
Integrity	164.312 (c) (1)	Mechanism to Authenticate Electronic Protected Health Information (A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Your risk assessment should consider the threats against ePHI that could compromise the integrity of the information. If the impact and likelihood of those threats is higher than your acceptable level of risk, then develop appropriate safeguards to bring those risks down.
Person or Entity Authentication	164.312 (d)	Person or Entity Authentication (R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Your procedures for providing personnel with access to ePHI must be designed so that the identity of the person who is receiving access has been verified, as well as their authority to access that information. Be sure to consider how this verification works when altering account access, such as requests for password resets.
Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network				
Transmission Security	164.312 (e) (1)	Integrity Controls (A)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Your risk assessment should consider the threats against ePHI that could compromise the integrity of the information while it is in transit. If the impact and likelihood of those threats is higher than your acceptable level of risk, then develop appropriate safeguards to bring those risks down.
		Encryption (A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	As with the “Encryption and Decryption” specification above, the goal of this specification is to ensure that ePHI is only accessible to those who have approved access to it. Encryption is a common and easily accessible means for providing that assurance, but it may not be practical in many cases, especially when information needs to move from one organization to another. Alternatives may be de-identification, or in some lower-risk environments, dedicated communication channels.