Nightfall™

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Section I: Administrative Safeguards				
Risk Analysis	Required	Security Management Process 45 CFR § 164.308(a)(1)	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.	Risks assessments require you to survey and inventory risks specific to your org. Some questions to consider include: -**How does ePHI move throughout your systems? You should identify the lifecyle (creation, use, storage, deletion, etc.) of ePHI within your org.** **-Who are your high risk users? This can either be as a result of their position (they have the most access/privileges and are likely to be targeted by threat actors) or as a result of their behavior (they consistently engage in risky behavior)** **-What does your third party risk look like? What ePHI will third-parties have access to and what policies do you have in place to moderate their behavior?** **-What are potential sources of external access to ePHI from outside your org?** **-What are some environmental threats to your ePHI? What kinds of disruptions would such threats result in?**
Risk Management	Required		Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.	Based on your Risk Assessment, you'll most likely want to identify and adopt an appropriate security framework to address risks (i.e.NIST CSF, HITRUST, etc.) Regardless of how you go about this you should: **-Make sure your risk assessment has effectively categorized the different types of risks specific to your org as well as how severe or urgent they are.** **-Invest in the tools/controls necessary to maintain visibility into risks.** **-Set objectives for your security program based on the urgency and nature of the risks unique to your org.** **-Create metrics that measure and demonstrate how your security program is minimizing risks and mitigating the ones that emerge.**
Sanction Policy	Required		Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Being able to apply sanctions to workforce members who violate policy entails: **-That you have detailed security policies in place.** **-That these policies as well as any sanctions for violations of policies are clearly communicated to employees.** **-For good measure employees should be required to demonstrate competency around policies regularly through training and testing (See the section of our Remote-First Security Playbook on building a high-quality security training program for more on this).**
Information System Activity Review	Required		Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	To monitor and regularly audit logs, you'll want to make sure you: **-Have a way to monitor and digest logs for systems across your organization.** Many security teams invest in tools like a **Security Information and Event Manager (SIEM)** which allows their security tool alerts and system logs to feed into one place.
	Required	Assigned Security Responsibility 45 CFR § 164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule.	As part of guidance for this rule the HHS notes that: **-This standard is comparable to the Privacy Rule standard that requires a privacy officer or official to be designated [45 CFR §164.530(a)(1)].** **-The security official and privacy official can be the same person, but are not required to be.**

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Authorization/Supervision	Addressable	Workforce Security 45 CFR § 164.308(a)(3)	Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Implementing authorization and/or supervision could entail: **-Enforcing role-based access or using the identity lifecycle to manage the permissions and authorizations of users based on their function.** **-Additionally remediating violations that expose data to unauthorized users.** **-To accomplish this invest in controls that monitor for policy violations and/or restrict access based on attributes of the user.** For example, Nightfall's healthcare customers integrate our platform within SaaS environments like Slack and Gmail to monitor employee communications for potential PHI violations. When Nightfall detects a violation it can prohibit ePHI from appearing within channels, files, and other content accessible by unauthorized users. You'll need to think carefully about where ePHI is within your org and the persons who have access to it in order to determine what types of controls and policies make sense to satisfy this requirement.
Workforce Clearance Procedure	Addressable		Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Procedures to manage an employee's access to ePHI to ensure it's appropriate: **-Can involve onboarding processes that ensure each individual employee is only given access to the systems and data they use in their regular work, based on role or function.** **-Can involve regularly reviewing employees' permissions to ensure that permissions are revoked for systems and data employees no longer used in the course of their work.** **-Finally, when an employee is terminated, make sure there is an immediate process to deprovision access to all systems.** For an overview of what this might entail, see the section titled "What is Identity and Access Management" in our Remote-First Security Playbook.
Termination Procedures	Addressable		Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in the Workforce Clearance Procedure.	See above
Isolating Helathcare Clearinghouse Function	Required	Information Access Management 45 CFR § 164.308(a)(4)	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.	This implementation specification only applies in the situation where a health care clearinghouse is part of a larger organization. In these situations, the health care clearinghouse is responsible for protecting the ePHI that it is processing. Evaluating how to approach this requires understanding how ePHI flows between the clearinghouse and other entities within the org.
Access Authorization	Addressable		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.	Policies and procedures to authorize access to ePHI should: **-Determine who needs access to ePHI, when, and for what purpose.** **-Ensure there's a reliable way to verify employee identities to ensure the correct person is being granted access to systems and data.**
Access Establishment and Modification	Addressable		Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Policies and procedures to manage access to ePHI should: **-Involve regular review of access logs and permissions to ensure that users are accessing only the resources they need.** **-Can involve tracking user permissions via the identity lifecycle, depending on the relationship of the user to the org.** **-Involve editing access to resources as the nature of a user's role changes or as the purpose of the ePHI evolves.**

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Security Reminders	Addressable	Security Awareness Training 45 CFR § 164.308(a)(5)	Implement periodic security updates.	As part of guidance for this rule the HHS notes that: **-There are many types of security reminders that covered entities may choose to implement.** **-Examples might include notices in printed or electronic form, agenda items and specific discussion topics at monthly meetings, focused reminders posted in affected areas, as well as formal retraining on security policies and procedures.** **-Covered entities should look at how they currently remind the workforce of current policies and procedures, and then decide whether these practices are reasonable and appropriate or if other forms of security reminders are needed.** To provide a concrete example, we want to note that Nightfall's healthcare customers integrate our platform within their SaaS environments to monitor employee communications for potential PHI violations. When Nightfall detects a violation it can send a custom message to the employee who violated policy to remind them of how to appropriately share or disclose ePHI, before remediating the incident.
Protection from Malicious Software	Addressable		Procedures for guarding against, detecting, and reporting malicious software.	Under the Security Awareness and Training standard, the workforce must also be trained regarding its role in protecting against malicious software, and system protection capabilities. See Section A of our Remote-First Security Playbook to learn how to build a culture of security within your workforce.
login Monitoring	Addressable		Procedures for monitoring login attempts and reporting discrepancies	As part of risk management and audit logging you should monitor access to resources, including systems requiring authentication. Doing so can tell you if a malicious actor is trying to use credentials as opposed to a genuine user. As part of your work in satisfying this requirement you can also evaluate tools like **User and Entity Behavior Analytics (UEBA)** to apply heuristics that may proactively blog illegitimate and unauthorized users from misusing credentials.
Password Management	Addressable		Procedures for creating, changing, and safeguarding passwords.	You should create policies that: **-Determine password complexity for user accounts.** **-Determine how frequently passwords should be changed.** **-Encourage practices that employees must observe in managing their credentials (i.e. not storing passwords on sticky notes)**. Tools like Single Sign On or password managers can simplify this process and allow you to use a security solution to make it easier for you to monitor user behavior and enforce proper policies. For an overview of what this might entail, see the section titled "What is Identity and Access Management" in our Remote-First Security Playbook.
Response and Reporting	Required	Security Incident Procedures 45 CFR § 164.308(a)(6)	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; and document security incidents and their outcomes.	Incident response can involve: **-Determining how employees should respond to security incidents and disruptions based on their role and responsibilities.** **-Determining how the incident will be documented and remediated.** **-Determining how to evaluate the extent of the disruption caused by the incident and when the organization's function has returned to normal.** We discuss some of this in Section C of our Remote-First Security Playbook.
Data Backup Plan	Required		Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	You should adopt policies and tools that help you: **-Identify critical ePHI that requires redundancies.** **-Store backups securely.** **-Develop a process for retrieving backups under the appropriate circumstances.**
Disaster Recovery Plan	Required		Establish (and implement as needed) procedures to restore any loss of data.	Guidance for this section notes that while you might have a general disaster recovery plan for your broader business, you need policies and practices in place to securely recover ePHI. For a broad overview of Disaster recovery see Section C of our Remote-First Security Playbook.

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Emergency Mode Operation Plan	Required	Contingency Plan 45 CFR § 164.308(a)(7)	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.	When a covered entity is operating in emergency mode due to a technical failure or power outage, security processes to protect ePHI must be maintained. This might include: **-Evaluating alternative security measures that should be already in place in the instance of a failure.** **-Identifying if there need to be manual procedures in place to secure ePHI during the emergency or enable normal operations once the emergency has passed.**
Testing and Revision Procedure	Addressable		Implement procedures for periodic testing and revision of contingency plans.	As part of guidance for this rule the HHS notes that: **-This implementation specification applies to all implementation specifications under the Contingency Plan standard, including the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operations Plan.**
Applications and Data Criticality Analysis	Addressable		Assess the relative criticality of specific applications and data in support of other contingency plan components	As part of guidance for this rule the HHS notes that: **-This implementation specification requires covered entities to identify their software applications (data applications that store, maintain or transmit ePHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operations plans. A prioritized list of specific applications and data will help determine which applications or information systems get restored first and/or which must be available at all times.**
	Required	Evaluation 45 CFR § 164.308(a)(7)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.	As part of guidance for this rule the HHS notes that: **-Initially the evaluation must be based on the security standards implemented to comply with the Security Rule. Subsequent periodic evaluations must be performed in response to environmental or operational changes that affect the security of ePHI. The on-going evaluation should also be performed on a scheduled basis, such as annually or every two years. The evaluation must include reviews of the technical and non-technical aspects of the security program.**
Written Contract or Other Arrangement	Required	Business Associate Contracts and Other Arrangement 45 CFR § 164.308(b)(4)	Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate that meets the applicable requirements of the organizational requirements [§164.314(a)] in the Security Rule.	As part of guidance for this rule the HHS notes that: **-To minimize additional work efforts, can existing business associate contracts, which involve ePHI, could potentially be modified to include Security Rule requirements**
Section II: Physical Safeguards				
Contingency Operations	Addressable	Facility access Controls 45 CFR § 164.310 (a)(1)	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.	As part of guidance for this rule the HHS notes that: **-Facility access controls during contingency operations will vary significantly from entity to entity.** **-For example, a large covered entity may need to post guards at entrances to the facility or have escorts for individuals authorized to access the facility for data restoration purposes. For smaller operations it may be sufficient to have all staff involved in the recovery process.** **-In the instance that some of the content of this procedure is also addressed within the organization's contingency plan, it could be valuable to combine it.**
Facility Security Plan	Addressable		Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	As part of guidance for this rule the HHS notes that: **-Facility security plans must document the use physical access controls. These controls must ensure that only authorized individuals have access to facilities and equipment that contain ePHI.** **-Plans must be reviewed periodically, especially when there are any significant changes in the environment or information systems.**

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Access Control and Validation Procedures	Addressable		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.	As part of guidance for this rule the HHS notes that: **-The purpose of this implementation specification is to specifically align a person's access to information with his or her role or function in the organization. These functional or role-based access control and validation procedures should be closely aligned with the facility security plan.** **-The controls implemented will depend on the covered entity's environmental characteristics.**
Maintenance Records	Addressable		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).	As part of guidance for this rule the HHS notes that: **-In a small office, documentation may simply be a logbook that notes the date, reason for repair or modification and who authorized it. In a large organization, various repairs and modifications of physical security components may need to be documented in more detail and maintained in a database.**
	Required	Workstation Use 45 CFR § 164.310(b)	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.	As part of guidance for this rule the HHS notes that: **-The Workstation Use standard requires covered entities to specify the proper functions to be performed by computing devices as well as the proper environment for workstations (where to use, how to store).** **-Organizations might want to specifically identify devices that contain/have access to ePHI versus those that don't.** Organizations can address this with acceptable use policies that account for the locations where employees work, as well as the obligations employees have for ensuring the safety of devices
	Required	Workstation Security 45 CFR § 164.310(b)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	As part of guidance for this rule the HHS notes that: **-While the Workstation Use standard addresses the policies and procedures for how workstations should be used and protected, the Workstation Security standard addresses how workstations are to be physically protected from unauthorized users.** **-As with all standards and implementation specifications, what is reasonable and appropriate for one covered entity may not apply. Your risk analysis should be used to help with the decision-making process.**
Disposal	Required	Device and Media Controls 45 CFR § 164.310(d)(1)	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.	As part of guidance for this rule the HHS notes that: **-When covered entities dispose of any electronic media that contains ePHI they should make sure it is unusable and/or inaccessible.**
Media Re-use	Required		Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	As part of guidance for this rule the HHS notes that: **-In addition to appropriate disposal, covered entities must appropriately reuse electronic media, whether for internal or external use. Internal re-use may include re-deployment of PCs External re-use may include donation of electronic media to charity organizations or local schools.**
Accountability	Addressable		Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	As part of guidance for this rule the HHS notes that: **-Many applications have configuration settings for automatic logoff. After a predetermined period of inactivity the application will automatically logoff the user.**
Data Backup and Storage	Addressable		Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	As part of guidance for this rule the HHS notes that: **-This specification protects the availability of ePHI and is similar to the Data Backup Plan implementation specification for the contingency plan standard of the Administrative Safeguards, which requires covered entities to implement procedures to create and maintain retrievable exact copies of ePHI. Therefore both implementation specifications may be included in the same policies and procedures.**
Section III: Technical Safeguards				
Unique User Identification	Required		Assign a unique name and/or number for identifying and tracking user identity.	As part of guidance for this rule the HHS notes that: **-The Rule does not describe or provide a single format for user identification. Covered entities must determine the best user identification strategy based on their workforce and operations.**

HIPAA Security Rule Implementation Specification Matrix

Implementation Specifications	Status	Safeguard	Description	Guidelines to Consider
Emergency Access Procedure	Required	Access Control 45 CFR §164. 312(a)(1)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	As part of guidance for this rule the HHS notes that: **-Access controls are necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. Covered entities must determine the types of situations that would require emergency access to an information system or application that contains ePHI.**
Automatic Logoff	Addressable		Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	As part of guidance for this rule the HHS notes that: **-Many applications have configuration settings for automatic logoff. After a predetermined period of inactivity the application will automatically logoff the user.**
Encryption and Decryption	Addressable		Implement a mechanism to encrypt and decrypt electronic protected health information.	As part of guidance for this rule the HHS notes that: **-There are many different encryption methods and technologies to protect data from being accessed and viewed by unauthorized users. Evaluate your organizational structure to determine where encryption is appropriate (i.e. at rest, in-transit) and by what means to employ it.**
	Required	Audit Controls 45 CFR § 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	As part of guidance for this rule the HHS notes that: **-It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.**
Mechanism to Authenticate ePHI	Addressable	Integrity 45 CFR § 164.312(c)(1)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	As part of guidance for this rule the HHS notes that: **-In order to determine which electronic mechanisms to implement to ensure that ePHI is not altered or destroyed in an unauthorized manner, a covered entity must consider the various risks to the integrity of ePHI identified during the risk analysis. Once covered entities have identified risks to the integrity of their data, they must identify security measures that will reduce the risks.**
	Required	Person or Entity Authentication 45 CFR § 164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	As part of guidance for this rule the HHS notes that: **-Although the password is the most common way to obtain authentication to an information system and the easiest to establish, covered entities may want to explore other authentication methods**.
Integrity Controls	Addressable	Transmission Security 45 CFR § 164.312(e)(1)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	As part of guidance for this rule the HHS notes that: **-Protecting the integrity of ePHI maintained in information systems was discussed previously in the Integrity standard. Integrity in this context is focused on making sure the ePHI is not improperly modified during transmission. A primary method for protecting the integrity of ePHI being transmitted is through the use of network communications protocols. In general, these protocols, among other things, ensure that the data sent is the same as the data received. There are other security measures that can provide integrity controls for ePHI being transmitted over an electronic communications network, such as data or message authentication codes, that a covered entity may want to consider.**
Encryption	Addressable		Implement a mechanism to encrypt electronic protected health information.	As part of guidance for this rule the HHS notes that: **-As previously described in the Access Control standard, encryption is a method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensible text. The Encryption implementation specification is addressable, similar to the addressable implementation specification at §164. 312(a)(2)(iv), which addresses Encryption and Decryption.** It's important to note that this implementation specification explicitly refers to data in-transit, like for an employee sharing PHI over a network or the internet. As an illustration, Nightfall works with Virtru to enable encryption of PHI over Gmail, so that email communications containing specific PHI identified by your security program will automatically be sent encrypted.