NIST and HIPAA compliance:

Remediate risks, address compliance gaps, and ensure PHI integrity

ManageEngine
AD360

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Companies that deal with protected health information (PHI) must have a physical, network, and process security measures in place to ensure HIPAA compliance.

The HIPAA Security Rule provides the standards that must be applied to safeguard electronic protected health information (ePHI) against threats, hazards, and unauthorized usage. The HIPAA security rule requires the implementation of administrative, physical, and technical controls to ensure the confidentiality and integrity of ePHI. The failure to comply with HIPAA regulations can result in substantial fines being issued – even if no breach of PHI occurs.

Drawbacks with HIPPA regulations

Having said that, there is one major caveat to HIPAA regulations. The HIPAA Security Rule is designed to be flexible, scalable, and technology-neutral – and accommodates integration with various information security frameworks. Due to this, IT teams in the healthcare industry find HIPAA clauses to often have vague language and leave a lot for interpretation.

However, the NIST Cybersecurity Framework, despite being a non-regulatory regulation, has been voluntarily adopted by many. This can be attributed to the granularity of the NIST Cybersecurity Framework's subcategories due to which some HIPAA Security Rule requirements may map to more than one of the Cybersecurity Framework's subcategories.

Taking this into consideration, the HHS Office for Civil Rights (OCR) released a crosswalk between the requirements of the HIPAA Security Rule and the NIST Cybersecurity Framework. The crosswalk – which was developed in conjunction with the National Institute of Standards and Technology (NIST) and the HHS Office of the National Coordinator for Health IT – maps each administrative, physical, and technical safeguard standard and implementation specification of the HIPAA Security Rule to the relevant subcategory in the cybersecurity framework.

Who is this crosswalk for?

This crosswalk is aimed at organizations that have aligned their information security programs to either the Cybersecurity Framework or the Security Rule to identify potential gaps in their programs and in managing the risks in their information security environments.

Addressing security gaps to bolster critical PHI

In this e-book, we'll be going through certain crucial requirements of HIPAA that can be mapped to relevant sections of the NIST Cybersecurity Framework and how ManageEngine AD360 can help you adhere with the crosswalk's regulations.

AD360 is our integrated identity and access management solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps healthcare organizations protect patient privacy, prove compliance, fend off attackers, improve operational efficiencies, and confront healthcare IT challenges from a simple, easy-to-use interface.

Function	Category	Subcategory	Relevant Control Mappings	How AD360 can tackle
Protect (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identitie and credentials are managed for authorized devices and users	NIST SP 800-53 Rev. 4 AC-2, IA Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)	Leverage AD360's real-time change monitoring function, and take proactive measures to keep patient information private.
		PR.AC-3: Remote access is managed	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 • HIPAA Security Rule 45 C.F.R. §§ 64.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)	Remote and terminal services management

		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)	Enable a fully secure and reliable remote work experience in just a few clicks. Allow or deny remote access permissions to employees who work from home in bulk.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	NIST SP 800-53 Rev. 4 SC-28 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 64.310(d), 164.312(a)(1), 164.312(a)(2)(iii) 164.312(a)(2)(iv) 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)	With continuous file access monitoring and automated incident response, AD360 is your organization's best defense against internal and external threats to data security and integrity. Track every access to the operating system (OS), database, and application software files; archived logs and reports; and other critical files, and verify whether the action was warranted.
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i),1 64.310(d)(2)(iv)	With AD360, back up AD objects, Exchange mailboxes, and SharePoint sites, all from a single console. Schedule backups to happen automatically during non-business hours to reduce the strain on your network. Always stay in the know by getting real-time alerts via email on the status of backup and recovery actions.

	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality	NIST SP 800-53 Rev. 4 AU Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b),	AD360 allows you to identify compromising file changes in the event of a data breach, and share findings by exporting event details and generating custom reports tailored to your needs. AD360 helps you make sure each user has the right amount of privileges and access. Maintain an audit trail of every user's access to resources while managing permissions and rights granted to users.
		PR.PT-2: Removable media is protected and its use restricted according to policy	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)	Detect USB devices plugged in to domain controllers, servers, or workstations, and receive alerts when files are copied to them.
Category: Detect (DL)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)	Detect, investigate, and mitigate threats like malicious logins, lateral movement, privilege abuse, data breaches, and malware. With AD360, receive notification if there's been an attempt to exfiltrate or delete data.

	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events **DE.CM-4:** Malicious code is detected	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)	See who did what, when, and where, along with other details surrounding each anomaly and receive notification when there is an unusual process running on a machine.
Category: Respond (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-3:** Forensics are performed	NIST SP 800-53 Rev. 4 AU-7, IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)	Identify compromising file changes in the event of a data breach, and share findings by exporting event details and generating custom reports tailored to your needs.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained **RS.MI-2:** Incidents are mitigated **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)	Receive alerts about sudden spikes in file activity, a tell-tale sign of ransomware intrusion, and execute scripts to shut down the infected machines and halt the spread of malware. The user behavior analytics (UBA engine) identifies an acceptable baseline of user activity and detects deviations to spot any unusual volume of file changes, potential data breaches, and more.

Summary

While the use of the framework does not guarantee HIPAA compliance, and the HIPAA Security Rule does not require use of the NIST Cybersecurity Framework, the crosswalk was developed as a tool to help healthcare tech and healthcare organizations manage risks in a comprehensive manner.

This crosswalk provides a helpful road map for HIPAA-covered entities and their business associates to understand the overlap between the NIST Cybersecurity Framework, the HIPAA Security Rule, and other security frameworks that can help entities safeguard health data in a time of increasing risks.

AD360 brings you 24x7 monitoring, email alerts, and easy-to-view, pre-configured reports. With over 200 reports to view changes, compliance doesn't get simpler than this. Audit access to files containing PHI, monitor privileged user activity, enable user behavior analytics, meet healthcare regulations, and fortify patient data from unauthorized access, all from a single console. AD360 helps improve your cybersecurity posture and lets you concentrate on what's important.