ManageEngine
AD360

Implementing NIST 800-66: The actionable guide for HIPAA compliance

www.manageengine.com/ad360

Table of **Contents**

Introduction

The global healthcare industry, a sector that holds sensitive protected health information (PHI), has constantly been the target of high-volume cyberattacks.

Healthcare organizations in India suffered 1.9 million cyberattacks in 2022 alone, according to a report published by cybersecurity think tank CyberPeace Foundation and Autobot Infosec Private Ltd.

To further highlight the highly alarming expansion of the healthcare sector's attack surface, the US Department of Health & Human Services - Office for Civil Rights (HHS-OCR) reported that the nation's healthcare sector has witnessed 295 cyberattacks in the first half of 2023, impacting 39 million individuals.

The OCR presented a report to the US Congress, stating that between 2017 to 2021, the number of HIPAA violations had increased by 39%. This was followed by a press release in which OCR Director Melanie Fontes Rainer assured that they will "continue to provide guidance and technical assistance on compliance with the HIPAA Rules, as well as vigorous enforcement program to address potential HIPAA violations."

Common IT security and compliance challenges of the healthcare sector

As illustrated previously, the intensity of cyberattacks faced by the healthcare sector has witnessed an unprecedented spike. A report published by Checkpoint Research revealed that the global healthcare industry suffered 1,463 breaches per week in 2022, a 74% rise in attacks from 2021. Some of the pertinent IT challenges encountered by the healthcare sector include:

Lack of IT visibility

Healthcare delivery organizations (HDOs) operate in IT environments that comprise of multiple directories, medical devices, electronic health records (EHR) systems, identity providers, administrative software and so on. Therefore it is highly essential for HDOs to have centralized view of their IT environment. Without a bird's eye view of the ecosystem, IT teams will be running the risk of data and identity silos, where they can't single out perceived and active threats.

Siloed identity management

HDOs are built upon a complex organizational structure, which apart from permanent employees, also comprises temporary staff such as contractual employees and interns. Many of these temporary employees might have access to sensitive information.

With poor IT visibility and manually-driven processes, administrative teams will find it overwhelming to onboard and offboard users. This results in the accumulation of inactive accounts that can potentially act as attack vectors for bad actors to exploit protected networks and the sensitive assets housed within them. Moreover, HDOs operating without a unified IAM framework can end up duplicating essential security procedures such as authentication, authorization, auditing, backup, and recovery.

Unmanaged access permissions

Access privileges make or break an organization, and this holds more relevance in the healthcare sector. Healthcare organizations run the risk of exposing their PHIs to malicious actors, especially insiders, by not regulating access to their electronic private health information (ePHI). Without gaining visibility on who has access to what resource, and at which time period, IT environments of HDOs can be prone to unauthorized access and data breaches.

What is NIST 800-66?

Established in 2008, the NIST 800-66 is officially titled "(the) Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," and it provides a set of guidelines and mandates that aim at standardizing HIPAA compliance management. NIST 800-66 elaborates upon the necessary physical and technical safeguards that complement with HIPAA's requirements.

What does the second revision of NIST 800-66 offer?

The second revision of NIST 800-66, currently open for public opinion, has expanded on various security requirements which include:

Access Authorization

Decide and document how access to ePHI will be granted for privileged functions.

Consider whether multiple access control methods are needed to protect ePHI according to results of the risk assessment.

Access establishment and modification

Regularly review personnel access to ePHI to ensure that access is still authorized and needed.

Modify personnel access to ePHI, as needed, based on review activities.

Termination of access

Healthcare organizations must consider implementing user recertification processes to ensure that least privilege is enforced.

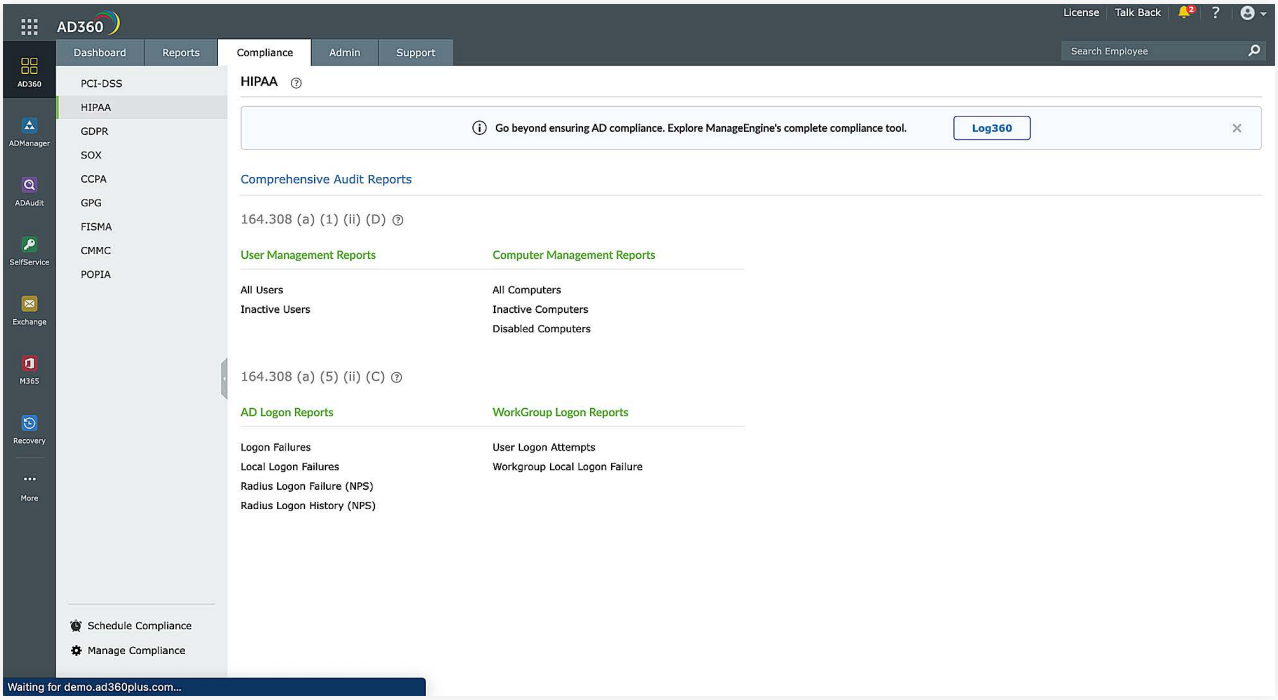
How does NIST 800-66 and AD360 steer organizations toward HIPAA compliance?

NIST 800-66 recommends the essential capabilities required by HIPAA's privacy and security rule. AD360, ManageEngine's IAM solution, helps healthcare organizations ace HIPAA compliance by intrinsically delivering the features put forth by NIST 800-66 as illustrated by the matrix below:

NIST 800-66 Recommendations	Corresponding HIPAA Security Rule Requirement	AD360 capabilities that align with the requisite
Implement user authentication and authorization controls	HIPAA 164.312(a)(1) - Access control	AD360's authentication module offers: • Unified **multi-factor authentication** (online and offline), **single sign-on**, and **passwordless authentication** across on-prem AD, Azure AD, and non-AD applications. • **Risk-based authentication** by leveraging contextual factors such as geolocation, device type, and logon failures. • **Self-service credential resets**, where users can reset passwords on their own, without help desk intervention. This saves time, resources, and efforts.
Implement strong authentication methods	HIPAA 164.312(d)(2)(iii) - Person or Entity Authentication	
Develop and implement policies for user access	HIPAA 164.312(d) - Person or Entity Authentication and HIPAA 164.308(a)(4)(i) - Information Access Management	
Ensure user identity verification	HIPAA 164.312(d)(2)(iv) - Person or entity authentication	
Enforce role-based access control	HIPAA 164.312(a)(2)(iii) - Access control	• HDOs can leverage AD360's adaptive MFA feature to enforce conditional access across users, thereby regulating their access to sensitive PHI and applications. • Using AD360's AD Management module, organizations can streamline the delegation of **access permissions** for bulk users according to their roles, groups, and designation across their hybrid AD and G-Workspace environments. applications. • AD360 can also automate several identity governance and administration (IGA) processes such as user creation, modification, and deletion by leveraging pre-built automation template and CSV-based creation, and integration with Human Resource Management Solutions (HRMS)

Conduct regular access reviews and audits	HIPAA 164.312(b) - Audit controls	• Audit file access in real-time using AD360's AD auditing module. With AD360, organizations can: • Enable real-time access monitoring of file access across Windows servers, failover clusters, and NAS devices (NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx for Windows, and QNAP). • Review access attempts made by users on unauthorized files. • Audit access attempts across shared folders and sensitive files. • AD360's access certification workflows periodically identify and review users' access to their organization's critical resources. This helps organizations ensure that users only have access to appropriate resources throughout their digital life cycles. • AD360's AD auditing module leverages user behavior analytics to monitor user activity and provide visibility towards anomalous events that veer away from the user's behavior profile. • AD360 helps establish a clear audit trail of passwords, user activity, and critical user management actions such as create, modify, rename, move along with the details of what, when, and where.
Establish access control procedures for electronic PHI	HIPAA 164.308(a)(4)(ii)(C) - Information Access Management	
Maintain user activity logs and audit trails	HIPAA 164.312(b)(1) - Audit controls and HIPAA 164.312(b)(2) - Audit controls	
Monitor user activities and implement audit controls	HIPAA 164.312(b) - Audit controls	
Develop an incident response plan	HIPAA 164.308(a)(6)(i) - Security incident irocedures	• AD360's audit-ready user reports and insights help IT and SOC teams gain a bird's eye view of their IT environment and perceived threats.In turn help organizations define granular incident response plans.

AD360 also enhances the compliance-readiness of HDOs by featuring a consolidation of reports and audits that augur well for HIPAA compliance. These pre-defined reports are also available for several data privacy standards such as GDPR, PCI-DSS, SOX, CCPA and so on. This library of reports expedites compliance by eliminating the need to parse information manually.


AD360
License
Talk Back
Dashboard
Reports
Compliance
Admin
Support
Search Employee
AD360
ADManager
ADAudit
SelfService
Exchange
M365
Recovery
More
PCI-DSS
HIPAA
GDPR
SOX
CCPA
GPG
FISMA
CMMC
POPIA
Schedule Compliance
Manage Compliance
HIPAA
Go beyond ensuring AD compliance. Explore ManageEngine's complete compliance tool.
Log360
Comprehensive Audit Reports
164.308 (a) (1) (ii) (D)
User Management Reports
All Users
Inactive Users
Computer Management Reports
All Computers
Inactive Computers
Disabled Computers
164.308 (a) (5) (ii) (C)
AD Logon Reports
Logon Failures
Local Logon Failures
Radius Logon Failure (NPS)
Radius Logon History (NPS)
WorkGroup Logon Reports
User Logon Attempts
Workgroup Local Logon Failure
Waiting for demo.ad360plus.com...

Conclusion

As emphasized by HIPAA, NIST 800-66, and the HHS' Health Industry Cybersecurity Practices guide, identity and access management has come to be a necessary component to secure healthcare organizations from an expanding threat surface and ensure compliance. AD360's automated IAM capabilities provides the necessary safeguards that HDOs can use to:

- Closely monitor sensitive assets that hold ePHI.
- Implement authentication and access control across their IT environment.
- Review user privileges.
- Automate user life cycle management.
- Generate audit-ready reports that expedite compliance management.
- Gain end-to-end visibility of IT environments.