Health Insurance Portability and Accountability Act

The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of Protected Health Information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, electronic, etc. Furthermore, only the minimum health information necessary to conduct business is to be used or shared. As an On-Premise solution, Endpoint Central has taken steps towards HIPAA compliance to ensure confidentiality and security of health information. Endpoint Central On-Premise is a HIPAA compliant solution. Check this page for more information.

What is HITECH and how is it related to HIPAA?

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was passed by the US government in 2009. After 13 years of HIPAA's operation, the HITECH Act was birthed as an extension of HIPAA. As HITECH is a superset of HIPAA, becoming HIPAA compliant automatically gives you certain degree of HITECH compliance. The two acts work together to improve healthcare and protect patient information. HITECH encourages the meaningful use of EHRs (Electronic Health Records) while promoting the security and privacy rules required by the HIPAA Act. In order to be HITECH compliant, organizations need to be HIPAA compliant first. This document will guide you on how Endpoint Central helps you achieve a level of HIPAA compliance.

How does Endpoint Central help?

Requirement	Requirement Description	How Endpoint Central fulfills it?
§ 164.308(a)(1)(ii)(A)	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.	Endpoint Central's patch management feature helps in deploying patches across every major operating system (Windows, Mac & Linux) and helps in patching third party applications. The periodic scans initated in the network gives details of the IT assets in the network and identifies vulnerable systems and applications. Endpoint Central also provides exhaustive reports on system vulnerabilities, patches, OS, firewall, filevault, bitlocker, antivirus, etc. which elaborates the threats present in the network devices..
§ 164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	Endpoint Central's Automate Patch Deployment (APD) feature provides administrators the ability to deploy patches missing in their network computers automatically, without any manual intervention. Periodic patching of vulnerable devices ensures the security of the ePHI available in the network devices. Endpoint Central's Secure USB feature allows network administrators to limit the scope of USB device usage by restricting selectively, blocking or allowing full use, thereby prohibiting any data leak. Geo-tracking, data wipe, putting the device in Kiosk Mode and remote lock of mobile devices enhances device security. Endpoint Central helps to deploy customised firewall settings and prohibit software to implement additional security measure. The Browser Security module helps in preventing browser based threats and protect enterprise data from credential thefts, phishing attacks and accidental data leakage.
§ 164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Endpoint Central provides various reports based on User log on/log off, USB device, alerts based on Software added/removed, periodic anitivirus updates, firewall, bitlocker and filevault status.
§ 164.308(a)(3)(ii)(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.	With the help of Endpoint Central, an IT admin can authorize permission to access file/folder/registry to users and groups who work with ePHI. Using User logon reports, log on information can be periodically reviewed and inapproriate/failed log on can be detected.
§ 164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Using Endpoint Central, an IT admin can manage permissions granted to access file/folder/registry to users and groups who work with ePHI. With user logon reports, logon information can be periodically reviewed and failed logon can be detected.
§ 164.308(a)(4)(ii)(B)	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.	An IT admin can manage access provided to the users using Endpoint Central. Using Group Management, the administrator can add, remove or modify user policies and user groups thereby securing access to ePHI. Also, permission to add/remove drives, can be provided to specific resources in the network.
§ 164.308(a)(5)(ii)(A)	Periodic security updates	Endpoint Central provides Automate Patch Deployment (APD) feature, Antivirus definition updates and driver updates to secure the network.
§ 164.308(a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.	Endpoint Central's ability to prohibit software and block executable files helps in guarding against malicious software. The firewall configuration in Endpoint Central additionally helps in protecting all network devices.
§ 164.308(a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.	Endpoint Central provides numerous reports on User log on/logoff, Last Logon Failed User Accounts, Currently Logged on Users, Currently Logged on Computers, etc. to monitor log-in attempts.
§ 164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.	With the help of Endpoint Central, an IT admin has the provision to change user's password.
§ 164.310(a)(2)(i)	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.	Using Endpoint Central, the administrator can take folder/file backup of important data which can be used to restore lost data under emergency conditions.
§ 164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Endpoint Central provides remote lock, signoff and shutdown features to terminate a session.
§ 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.	Endpoint Central provides centralised inventory of hardware/software details of mobiles, desktops and laptops. With User Logon reports, one can record the log on activities in Information Systems.
§ 164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Using Endpoint Central, permissions to access restricted files/folders can be allowed for specific users.