



How Hexnode helps meet HIPAA compliance standards?

The Health Insurance Portability and Accountability Act (HIPAA) safeguards patient health information amidst the challenges doctors face in protecting digital medical records, ensuring privacy, security, and integrity.



Why HIPAA compliance for organizations?

- 1 By adhering to HIPAA regulations, organizations demonstrate their commitment to maintaining patient privacy, security and confidentiality.
- 2 Compliance helps establish trust with patients, enhances the organization's reputation and mitigates the risk of data breaches and legal consequences.
- 3 By implementing appropriate administrative, physical, and technical methods, organizations can safeguard sensitive patient data and uphold the principles of HIPAA.

Who is HIPAA applicable to?



HIPAA applies to healthcare providers and health plans (such as insurance companies) that process electronic health information.



HIPAA also covers business partners who manage protected health information on behalf of covered entities, such as billing firms and IT service providers.



To secure patient health information, both covered companies and business partners must adhere to HIPAA standards.

The 4 Must-Know Rules of HIPAA

Privacy rule

Sets standards for protecting patients' personally identifiable health information and establishes patients' rights regarding their health information.

Security rule

Specifies safeguards for Electronic Protected Health Information (ePHI) and outlines administrative, physical, and technical measures to ensure its confidentiality, integrity, and availability.

Breach notification rule

Requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services (HHS) and, in some cases, the media in the event of a breach of unsecured PHI.

Enforcement rule

Establishes procedures and penalties for non-compliance with HIPAA, including investigations, audits, and civil monetary penalties imposed by the Office for Civil Rights (OCR).

HIPAA compliance with Hexnode UEM

- Device security and management**
Hexnode UEM allows admins to enforce strong device security policies, including passcodes, biometric authentication, and device lock-down.
- User access control**
Admins can create and sync user groups and assign specific permissions and configurations. This feature helps ensure that only authorized individuals have access to patient data.
- Content management**
allows secure access and sharing of patient files and will provide the ability to enforce document-level encryption and restrictions on data sharing.
- Geofencing and location tracking**
helps administrators to define virtual boundaries and monitor device location.
- Secure containerization**
allows to create a separate, encrypted workspace to isolate and protect sensitive patient data.
- App whitelisting and blacklisting**
ensures that only authorized and secure applications are installed on devices.
- Secure web browsing**
provides built-in web filters and URL whitelisting/blacklisting options. It serves to safeguard against potentially harmful websites and ensures secure access to online healthcare resources.
- Policy enforcement and monitoring**
ensures the adherence to data security guidelines. Real-time monitoring and alerts enable proactive identification and resolution of potential compliance violations.

Hexnode also helps you with...

- Data encryption
- Secure communication
- Remote wipe
- Data loss prevention
- Strong authentication
- Auditing and reporting
- Reduced risk of data breaches

Hexnode offers a comprehensive solution that not only helps healthcare organizations meet HIPAA compliance standards but also simplifies device management and enhances data security. So, take advantage of the **14-day free trial** to experience the ease of device management and the peace of mind that comes with Hexnode's secure data protection. Start your trial today and unlock the benefits of hassle-free device management with Hexnode.