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?



maintaining patient privacy, security and confidentiality.

By adhering to HIPAA regulations, organizations demonstrate their commitment to

Compliance helps establish trust with patients, enhances the organization's reputation and mitigates the risk of data breaches and legal consequences.



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?



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

HIPAA applies to

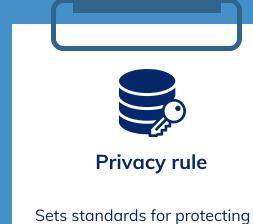


business partners who manage protected health information on behalf of covered entities, such as billing firms and IT service providers.



information, both covered companies and business partners must adhere to HIPAA standards.

The 4 Must-Know Rules of HIPAA



### patients' personally identifiable

health information and establishes patients' rights regarding their health information.



#### **Electronic Protected Health** Information (ePHI) and outlines

administrative, physical, and technical measures to ensure its confidentiality, integrity, and availability.



### Human Services (HHS) and, in some cases, the media in the

event of a breach of unsecured

PHI.



### investigations, audits, and civil monetary penalties imposed

by the Office for Civil Rights (OCR).

#### Hexnode UEM allows admins to enforce strong device security policies, including passcodes, biometric

HIPAA compliance with Hexnode UEM

#### patient files and will provide the ability to enforce document-level encryption and restrictions on data sharing.

allows secure access and sharing of

**Content management** 

Device security and management

authentication, and device lock-down.

Secure containerization allows to create a separate, encrypted workspace on devices to isolate and protect sensitive patient data.

provides built-in web filters and URL whitelisting/blacklisting options. It

serves to safeguard against potentially

harmful websites and ensures secure

# B

### helps administrators to define virtual boundaries and monitor device location.

User access control

access to patient data.

Admins can create and sync user groups

configurations. This feature helps ensure

and assign specific permissions and

that only authorized individuals have

Geofencing and location tracking

Policy enforcement and monitoring

ensures the adherence to data security guidelines. Real-time monitoring and alerts enable proactive identification and

App whitelisting and blacklisting

ensures that only authorized and secure applications are installed on devices.

## access to online healthcare resources.

Secure web browsing



## violations.

resolution of potential compliance

**Data encryption** 

Hexnode also helps you with...

**Secure communication** Remote wipe **Data loss prevention Strong authentication** 

Reduced risk of data breaches

**Auditing and reporting** 

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.

For more information, visit www.hexnode.com