How to maintain HIPAA compliance with Mobile Device Management

Nowadays, mobile devices are omnipresent, and sooner rather than later it was inevitable that it would come trickling down to the healthcare sector. And with it came the risks that are carried by mobile devices everywhere, data breaches. There are many ways in which confidential information stored in a mobile device can be stolen or be lost. These could include malware attacks, unsecured Wi-Fi networks, accidental data disclosure, outdated operating systems, and loss or theft.
When it comes to healthcare, no matter what type of device is used by the institution, they are liable to protect the patient's confidential data.

What is the Health Insurance Portability and Accountability Act (HIPAA)?

HIPAA compliance in its bare bones is a regulatory compliance policy aimed at keeping the average consumer's personal data safe, in this case, its patients. Here the data is ePHI or Electronic Protected Health Information. It includes personal information such as the name of the patient, address, social security no. Etc. Along with that, it also includes confidential medical data like e-prescription, X-Ray or MRI results, Blood Test results, etc.

HIPAA is now more important than ever. The US Department of Health and Human Services has specifically mentioned that all healthcare entities who deal with confidential patient information i. e, PHI uses completely computerized methods. This includes Electronic Health Records(EHR) computerized physician order entry and other systems. While all these electronically dependent methods can increase mobility and efficiency, it can also increase the security risks regarding healthcare data.

Hexnode and HIPAA compliance

Hexnode's device management platform comes with a slew of restrictions that would help your organization in the journey to attain regulatory compliance. Hexnode can help with regulations such as HIPAA, GDPR, SOC-2, ISO, etc.

Applying Encryptions

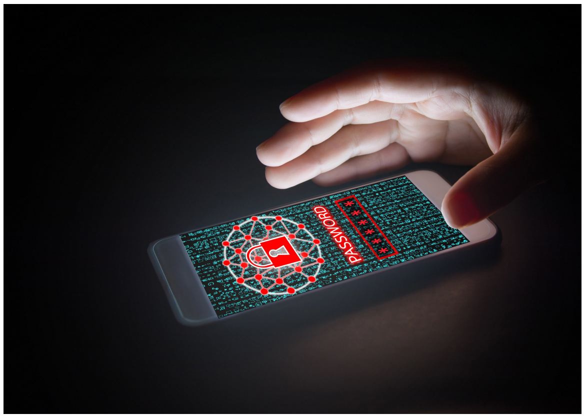
It's stated in HIPAA compliance security rule requirement 164.312(a)(2)(iv) as "Implement a mechanism to encrypt and decrypt electronically protected health information."

Encrypting the data in a device makes sure that the confidential information present can only be read using a specific key.

Hexnode enables you to make encryption mandatory for all devices. Hexnode also has various tools at its disposal like BitLocker for Windows and FileVault for Macs to encrypt storage disks as a whole. Advanced algorithms are also used to identify and monitor non-compliant devices that are encrypted. Furthermore, separate work containers can be created on devices, which are encrypted, to store sensitive data like ePHI.

By enabling screen locks on mobile devices, (iPad, iOS, and Android) you can ensure that all the data within the device is encrypted.

Deploying Passwords



Coming to passwords, it is stated in HIPAA compliance security rule requirement 164.308(a)(5)(ii)(D), “Procedures for creating, changing, and safeguarding passwords”. Demanding users to identify themselves with unique credentials is the first line of defense when it comes to device security. A simple password can go a long way in securing the device and the data present within.

Hexnode lets you clearly define enterprise-grade password standards for the devices. These standards can include, length, history, characters, etc. Password age can also be set so that the user may change the password at regular intervals. And yes, these password standards also apply to the encrypted work container mentioned earlier.

Mitigating Network Risks

Protecting data in movement is also as important as protecting data at rest. Even if a potential attacker can’t access the data while it is still in the device, they can try to intercept it while it is being transferred. So, the network avenues used to transfer ePHI data should be as strong as they can be.

It is stated in HIPAA compliance security rule requirement 164.312(e)(1), “Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.” With Hexnode, admins can provide Transport Layer Security (TLS) by limiting user access to corporate content only via corporate Wi-Fi and preconfigured Virtual Private Networks (VPNs).

If there arises an issue regarding network security, Hexnode also gives the admin the authority to disable all network connectivity or restrict to either Wi-Fi/mobile data for targeted devices. Admin can also view per-app data usage for analysis.

Breach of Data

Making a device completely safe from human error is close to impossible, but with Hexnode you do get pretty close. One of the potential risks that might be associated with a device concerning human error might be breaching of ePHI by accident or by purpose. Hexnode addresses these issues with various restrictions.

To avoid the breach of content by accident or by purpose, devices can be incorporated with a work profile that can contain the ePHI. Work profiles provide a virtual separation of sensitive content and confines interaction of this content to apps and functionalities that are defined within the work profile and thereby denying access of ePHI to apps and functionalities defined anywhere else on the device. Cut, copy, and paste capabilities of the device can be restricted. Geofencing can further secure the content by letting the admin remove the content once the device leaves a defined area. Compliance for devices can be continuously verified and access can be revoked for non-compliant devices.

Avoid Sharing of ePHI

The sharing of ePHI can be avoided by restricting the applications that are installed in the device. Apps are essential to reap the benefits of using a mobile device so, each app in the device should be studied thoroughly and their permissions should be scrutinized diligently. File sharing applications can be blacklisted. Access to blacklisted applications is denied. Applications can also be whitelisted, in effect blacklisting all other applications in the device. Admins can also restrict file sharing by disabling Bluetooth, USB file transfer, NFC, Android Beam, or even through text.

Handling lost devices

Lost devices are a huge liability for healthcare institutions. The data present in the device is of utmost confidentiality and a leak could lead to some serious trouble.
With Hexnode you can ensure devices are remotely locked or wiped to ensure maximum security of sensitive content when the device is lost. Enabling lost mode on a device will

lock down the device and display the message, number, and footnote which was entered from the Hexnode portal. The lost mode can be enabled and disabled directly from the portal. If the device is lost, a remote ring can be activated from within the portal to play a sound on the device even if the device is muted. Device locations can be monitored from the Hexnode portal. Restrictions can be enforced on devices that leave designated areas.

Staying up to date

Managing software updates is quite frankly a very tedious task but nonetheless, it is very important. Keeping the operating system up to date means that you will always have the best security updates at your disposal. App updates are also very important, as app developers change the way the app behaves as time goes by.
These tasks can be performed by the admin Remotely with the help of Hexnode.

A secure messaging channel

A secure messaging avenue is a requirement for any healthcare institution. Sending messages on an unsecured messaging service can lead to data leakage. Hexnode has an in-house Messenger called Hexnode Messenger which helps the admin and staff to essentially communicate with each other in a secure manner. It can also be used by the admin to broadcast messages to the medical staff in bulk.

Conclusion

Many healthcare institutions around the world lose confidential data every day just because they don’t protect their devices properly. Take the steps now to protect the devices in your organization and the data it holds.
The right device management solution goes a long way in fulfilling some key HIPAA compliance guidelines. By taking care of all the nitty-gritty device management aspects, clinicians and healthcare professionals can provide an elevated quality of service to their patients.

Disclaimer: This article and the information in it do not constitute legal advice and is intended to support customers in their compliance efforts.