How is mobility helping the healthcare industry

WHITE PAPER

hexnode

TABLE OF CONTENTS

Introduction

Modern healthcare and technology are mutually inclusive. We can see a rapid adoption of mobile devices and mobile health (mHealth) apps in healthcare. The ease that mobile technology brings to the industry is definitely a factor. However, the increased quality of health resulting from the adoption of mobile technology is also a main thing that led to this development.

The advent of technology in healthcare has helped caregivers, clinicians and patients alike. Mobility has its set of challenges in IT. When it comes to healthcare, we cannot afford to leave the devices unmanaged. The devices should be compliant with privacy standards like HIPAA and be secure to prevent leakage of Protected Health Information (PHI). In this white paper, we would be discussing the different ways that healthcare has gone mobile, how to manage all these mobile endpoints along with some case studies where mobility management helped healthcare organizations find their footing.

1

Technology in Healthcare

Simply put, mHealth is the use of mobile technologies for improving the quality of healthcare.

Crucial factors like the delivery of health services, patient experience and the overall cost of healthcare are all influenced by mHealth.

From bleeding the patients with leeches to advanced technologies for inspecting every part of human body in detail, healthcare has come a long way.

What is mHealth?

World Health Organization’s Global Observatory for eHealth defines mobile health (mHealth) as a “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices”.

The mHealth initiatives are not anything new in the world today. Let’s have a look at some of the ways that mobile technology is changing healthcare for the better around the world.

Where does mHealth stand today?

Remote monitoring tools for chronic diseases

There are many chronic diseases that require constant monitoring. For example, let us take the example of diabetes. According to a report from CDC, around 34.2 million people in US suffer from diabetes. This makes up almost 10.5 percent of the total population. The statistics are no joke. People who suffer from diabetes need to monitor their blood glucose levels and regulate their insulin intake accordingly.

There are more options today. The patients can use remote monitoring tools that record their blood glucose levels in real-time and send the data to the doctor or the caregiver if the levels cross a threshold limit. This is just one example of how mobility in healthcare is helping people lead healthier lives. The remote monitoring tools can also help patients with cardiovascular diseases, memory issues, monitor outbreaks of diseases like Dengue and much more. Managing these devices in a compliant manner is important to keep them secure.

> “Now, before mHealth, the only way to do that was to book an appointment with the doctor, get tested and then wait for the test results. It was a time-consuming process and often, an expensive one.

Purpose-oriented devices for healthcare workers

We cannot appreciate the caregivers enough and these devices exist to make their jobs just a little easier. The point-of-care devices enable healthcare workers to access patient records easily. It helps in reducing manual errors which would happen if they enter the patient information themselves. Speed and quality are two indispensable elements when it comes to healthcare.

Other uses

Mobile technologies have many other uses like:

- Communication capabilities including voice or video calling, email, and messaging.
- Hospital information systems – Health records, medical records and other information systems.
- Applications like disease diagnosis aids and medical calculators.

Challenges faced

If there are devices with sensitive information out there, if there are devices that are supposed to serve a specific purpose but are being misused, then these devices need to be managed.

The challenges faced by admins in healthcare is the same as admins everywhere.

- Preventing data leakage.
- Increasing user productivity.
- Deploying system updates.
- Managing network connection issues.
- Installing, uninstalling and updating apps.
- Configuring and enforcing restrictions and policies.

Common mobile threats

Phishing

If you aren't a complete beginner in IT, you would be knowing what phishing is. Phishing is one of the most common mobile threats faced worldwide without exception. The attackers pose as legitimate and reputed sources while they trick the unsuspecting users into giving up important information. There are many kinds of phishing. Fraudulent websites, apps and even networks could be the reason that sensitive health data is compromised.

Ransomware

Ransomware attacks are very common. The attackers encrypt your data and demand a hefty ransom to decrypt it. More often than not, the victims of ransomware attacks feel like they have no option but to pay the ransom. Ransomware attacks are prevalent in healthcare. In fact, the the healthcare industry is one of the most attractive targets for the attackers.

Even now, healthcare organizations are a lucrative target. In the past one year, around 81 percentage of healthcare organizations in UK were the victim of a ransomware attack.

> The first known ransomware attack that happened in 1989 was also targeted at the healthcare industry.

Network threats (Unsecured Wi-Fi)

It doesn't matter if you have followed all the security procedures in the world if the devices are connected to an unsecured network. Make sure that the users always connect to a secured network by setting up needed restrictions and policies.

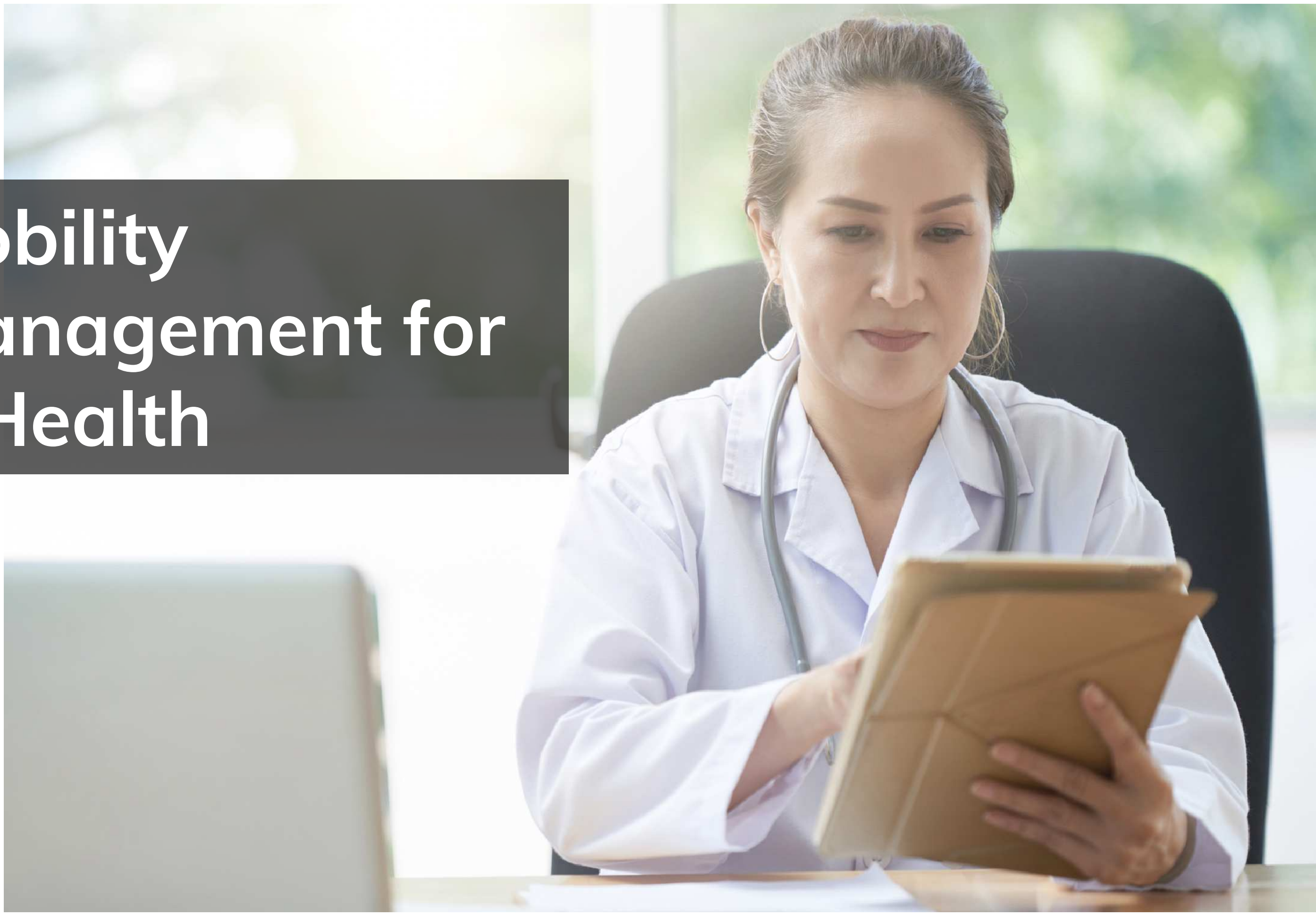
Data leakage

Data in healthcare is a sensitive matter. The repercussions of data leakage are huge. The average cost of a data breach in a non-healthcare related sector is around $158 per stolen record. In contrast, the cost is an average of $355 for healthcare organizations. Even information like credit card credentials or Personally Identifiable Information are valued less than PHI in the black market. The reason? Unlike data like credit cards, a patient's health history cannot be altered.

Larger attack surface with IoT

Internet of Things – IoT – is an intricate network of devices that are all connected. It is an excellent technology with a lot of scope.

According to a Technavio report, IoT platform market is projected to grow by around USD 12.5 billion by 2025. IoT devices are playing an important role in increasing the quality of healthcare too. For instance, IoT devices can be used for remote patient monitoring, glucose monitoring, heart-rate monitoring or even for predicting the “mood” of the patients. The drawback of IoT is that the attack surface is much bigger. If there is one weak link in the array of connected devices, it is going to be cyber nightmare. Most of the data collected by the Internet of Medical Things (IoMT) devices qualifies as PHI under HIPAA regulations.



2

Mobility management for mHealth

The scope of all the different attacks can be minimized or even stopped with mobility management. Just as we cannot take our health lightly, we cannot take the security health of the mHealth devices lightly either.

MDM solutions can be used to manage mobile devices. EMMs are a perfect solution for BYOD since they provide containerization capabilities.

There are different solutions in the market to help you manage devices. However, it is critical to choose the right one for your organization. A good rule of the thumb is to use a mobility management solution that can manage all the devices deployed.

Mobility Management Solutions - MDM vs EMM vs UEM

Mobile Device Management (MDM)

MDM solutions can be used to manage mobile devices. They also support remote device management features across different platforms.

Enterprise Mobility Management (EMM)

EMM is the combination of Mobile Device Management (MDM), Mobile Application Management (MAM), Identity and Access Management (IAM), Mobile Content Management (MCM) and Mobile Expense Management (MEM). EMMs are a perfect solution for BYOD since they provide containerization capabilities.

Unified Endpoint Management (UEM)

UEMs are comprehensive endpoint management solutions that allows you to manage desktops, laptops, smartphones, tablets, IoT devices, smart TVs and wearables from a single console. In addition to the features provided by EMM solutions, UEMs also support functionalities like no-touch deployment, advanced kiosk management, CYOD (Choose Your Own Device) and COBO (Corporate Owned Business Only).

About Hexnode

Hexnode is a Unified Endpoint Management (UEM) solution that has helped numerous healthcare organizations manage, secure and monitor their devices. There is a single console for the complete IT inventory of the healthcare facility. Hexnode also enables the healthcare organizations achieve HIPAA compliance.

3

Getting started with healthcare mobility management

The good news about endpoint management is: if you know the basics and have a solution like Hexnode, you can manage devices in any industry.

Hexnode admins have a wide array of enrollment methods for their endpoints.The no-touch enrollment methods and the bulk deployment options form an essential part of an IT admin's set of requirements.

Let's have a look at a few core functions to help you get started with mobility management in healthcare.

No-touch and bulk deployments

Hexnode admins have a wide array of enrollment methods for their endpoints. The no-touch enrollment methods and the bulk deployment options form an essential part of an IT admin's set of requirements. Let's have a look at what Hexnode offers:

Android

While there are many enrollment options like QR code enrollment, email or SMS enrollment, self-enrollment and so on for Android, we would be focusing on the no-touch enrollment methods in this whitepaper.

Android Zero-Touch Enrollment: Android ZTE is an out-of-the box enrollment method that allows secure deployment of devices without manually configuring each one of them. Once the devices are powered on and connected to a network, they would be automatically enrolled in Hexnode.

Samsung Knox Enrollment: This enrollment method is for Samsung devices running Knox version 2.4 and higher. Knox Mobile Enrollment lets you bulk enroll the devices in one go, automatically install the MDM profile when they are powered on for the first time and re-enroll the devices even if they are factory reset.

Apple devices

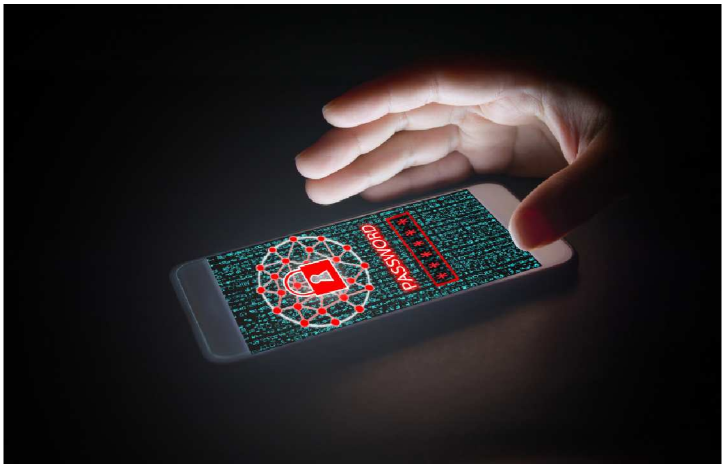
For macOS, iOS, iPadOS and tvOS devices, use Automated Device Enrollment for bulk no-touch enrollment. You would need either an Apple Business Manager (ABM) or Apple School Manager (ASM) account. If you do not have an ABM or ASM account, you could go for other enrollment methods like self-enrollment or enrollment with Apple Configurator.

Windows

Enroll Windows devices using self-enrollment or Email/SMS enrollment methods. For bulk deployments, use the provisioning package (.ppkg) enrollment.

Help the user configure strong passwords

Passwords are the first line of defense against any kind of cyber-attacks. Configure strong password policies so that the users are forced to configure strong passwords in compliance with the policy.



Some tips:

- Complexity requirements: Configure parameters like minimum password length, mandatory use of alphanumeric and special characters and so on.
- Password age: Set an expiry date for passwords. The users must change the passwords at regular intervals to reduce risks. Restrict reuse of the old passwords.
- Provision for too many wrong attempts: To prevent brute-force attack, configure a policy to wipe the device if there are too many wrong attempts.

Secure networks and connections

> “ Network security is one of the most important responsibilities of the IT admins in healthcare.

Use Hexnode to:

- Push Wi-Fi configurations remotely. The devices would be automatically connected the Wi-Fi without needing the user to manually input the password.
- Configure and deploy VPN. Virtual Private Networks (VPNs) remain the best method for perimeter security. If your organization is not operating on Zero Trust principles, use VPN for securing the flow of data in networks.
- Enforce certificate authentication with SCEP. This ensures that you are protected against security threats caused by accessing work emails, Wi-Fi, VPN and more.
- Set up Global HTTP Proxy settings to ensure that all HTTP network traffic pass through it.
- Disable pairing with Bluetooth devices.
- Configure data expense management policies to control Wi-Fi and data usage.

Manage all the applications involved

Apps form an integral part of mobile healthcare. Use Hexnode to install, uninstall or update the apps remotely in the managed devices. You can also blacklist or whitelist the apps as needed to prevent the use of unauthorized applications. That’s not all. Hexnode’s kiosk features let you lock down your generic Android, Windows, iOS, iPadOS or tvOS into single app or multi app mode. Manage all these features remotely from Hexnode’s web portal.

Deploy OS updates

Schedule important OS updates for managed devices. The devices would be automatically updated as scheduled. This reduces reliance on the end user.

BYOD Management

Bring Your Own Device (BYOD) policies are becoming increasingly common in the IT world. Healthcare organizations have traditionally struggled with BYOD as it is hard to ensure proper security.

Hexnode's BYOD policies helps healthcare organizations to achieve compliance and security while giving the employees freedom to use their personal devices for work. The isolation of work apps and data in a separate container (containerization) makes sure that the personal and work data do not mix. It is also an excellent security feature to prevent the flow of data between work and personal apps.

A good BYOD policy should have:

- Clear segregation between personal and work data.
- Security and adherence to compliance principles.
- App management policies.
- Wipe feature for work container, i.e., corporate wipe.

Inventory and reports

The importance of regular reports can never be downplayed. Hexnode admins have access to a wide range of reports that include device and user information, location reports, compliance reports, data management reports, application reports and so on. These reports can be downloaded manually or be scheduled to arrive in your inbox at regular intervals. You can also get a rough overall idea about your endpoints by checking the dashboard regularly.

Remote monitoring and management

The responsibility of healthcare workers is not something that we can take lightly. The healthcare industry deals with human lives and when you are placing your trust on mobile technology to help, you need to be sure that it is working properly at all times.

Hexnode's remote features help you do that and more. Let's have a look at the remote options that Hexnode admins have at their disposal:

Remote view and remote control: These two features are a real help when the devices are scattered in different locations. All devices running on Android version 5 and above supports the remote view feature. Remote view is also supported in iOS, Windows and macOS devices. The remote control feature lets you take over the device in real-time to do the necessary troubleshooting. It is supported in Samsung Knox devices.

Location tracking: What if devices containing sensitive patient data is lost or stolen? Or, what if the devices are in transit and you need regular location updates? If they are still connected to the network and managed by Hexnode, you can use the location tracking feature.

Lost mode: This feature disables all device features and locks down the device with a custom message and phone number. If the device is lost or stolen, the finder would not be able to use the phone. The person can call the number provided on the lock screen to return the device.

Remote lock/wipe: Lock or factory reset the remote devices with just a click on your Hexnode web console.

Compliance Management

There are strict guidelines and federal regulations for technology in healthcare and with good reason. Hexnode helps your organization be compliant with standards like HIPAA.

“ WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act is a federal law passed in 1996 with the purpose of protecting sensitive patient health information from being disclosed without the consent of the patient.

4

Some healthcare success stories

Case study 1: Kiosk for higher productivity

The background

The Greek Orthodox Community of NSW in Australia is one of the oldest organizations that provides a wide range of social services. Amongst those services, the organization also runs an old age nursing home. The staff members in the nursing homes were equipped with mobile devices that were meant to make their work easier.

However, these devices were soon being used for all sorts of non-word activities such as making telephone calls over VoIP, browsing the internet during work hours, frequent use of camera and so on. Sam Dasakis, the IT manager at Greek Orthodox Community of NSW, was at a loss on how to manage all these unmanaged devices. He tried to configure the device settings manually, but it was just not productive to configure a large number of devices one by one. It was a complex process – trying to figure out the settings and configurations.

The solution

> “I just need to install the required application, and everything is done automatically

While looking up solutions, Sam came across Hexnode in Google search. It was easy to get started with device management as Hexnode provided a 30-day trial version completely free of cost. Sam signed up for the free trial and found it very easy to deploy the software by himself. Sam used Hexnode’s Android kiosk solution to lock down all the devices into a single application or a set of apps as required. Now, all this was done from a single console. There was no longer the need to manually configure each device. All Sam needed to do was configure a policy with the required configurations and push it to the devices in one go.

In addition to the lockdown feature, there were other attractive features as well. The admins could remotely track the device location, lock or wipe the device if it was lost or stolen.

> “Earlier it took me a lot of time to set up devices... Now it’s much easier, and the software is user-friendly and works well

Hexnode admins could also remotely view the Android devices for easy troubleshooting. If the devices were rooted Android or Samsung Knox, the admin could take the device control one notch higher with the Remote Control feature.

The result

The secure lockdown solution offered by Hexnode resulted in greater workforce productivity. The bulk deployment features, automatic configurations of Wi-Fi and VPN, easy management of apps and tons of other features helped them secure and manage their devices seamlessly.

Case study 2 - One man team for IT

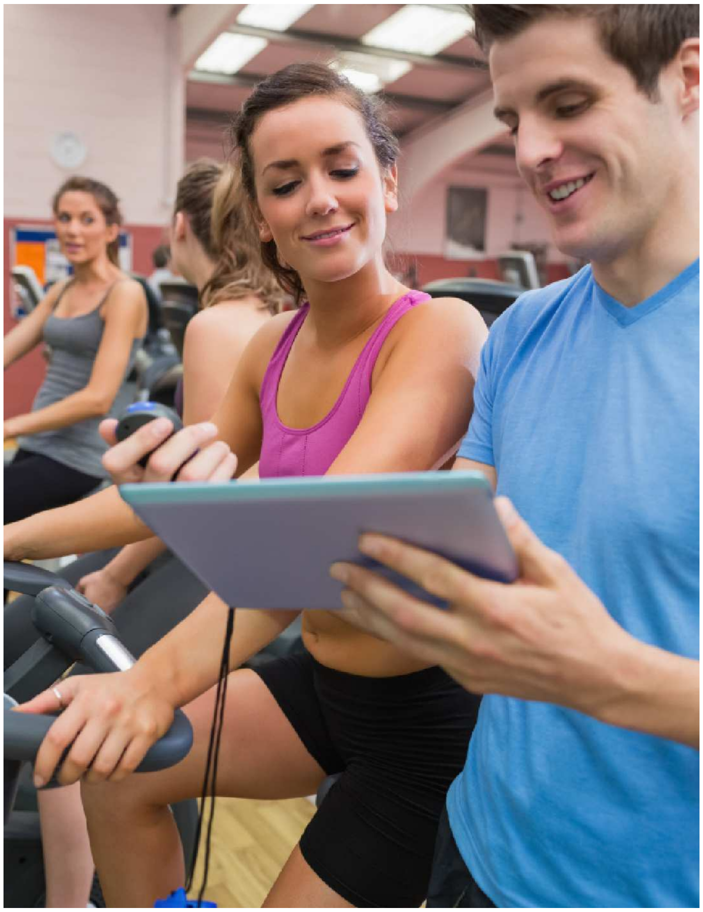
The background

Weight Watchers is a known name in the fitness industry. The largest Weight Watchers’ franchise group, operating in Michigan, has been playing an excellent role in promoting healthy habits in people. The company purchased tablets for its traveling salespeople.

The challenge

The devices that were provided to the salespeople were scattered over different locations. Keith Lubeck, the Senior Network Analystat Weight Watchers Group, needed a solution that would help him manage and monitor the devices at scale.

He tried out a few solutions and found them all unsatisfactory. Keith was assigned the super admin role in the company and he was the only one responsible for IT management.



The solution

Through a thorough Google Search, he found out about Hexnode UEM. The combination of a simple UI and excellent technical support convinced Keith to go with Hexnode.

He used Hexnode to restrict the employees from accessing unwanted applications, deploy different Wi-Fi configurations to the devices, configure web content filtering to restrict access to malicious/undesirable websites, schedule OS updates and monitor the status of each device remotely from the web console.

> “ It was easy to set up the software, and your tech support is brilliant... That's the main reason I went with you guys.

The result

With Hexnode, Keith found managing devices easy even if he was a one-man IT team. He could save a lot of time that he had previously used for manual management. Keith rated Hexnode a solid 9/10 for satisfying all his requirements topped with friendly support.

> “ I was able to manage every iPad and Android tablet quickly and easily. Hexnode helped me save hours and hours for device management.

Conclusion

According to the latest IMARC Group's report, the global mHealth market is growing at a remarkable pace. The market value is expected to reach as high as USD 1.95 billion by 2026. However, there is no need to be scared about the penetration of IT into healthcare. The number of devices does not really matter if you have a proper endpoint management solution to rely on. Hexnode has been helping healthcare companies find the balance between security, compliance and user convenience as we can see from the case studies. Figure out your requirements and start solving it for a cybersecure future in mobile heath management.