

How to secure and manage mobile devices in healthcare during the COVID 19 pandemic



hexnode

The COVID-19 pandemic has become an overwhelming reality for most industries but among the worst affected is Healthcare. In the US, several Frontline hospital workers provide us vastly differing pictures of preparedness on all fronts. This level of saturation can also be found in the technological spectrum of healthcare. Companies like [Giesinger Health](#) are dealing with up to a 500% increase in teleconsulting and with over 13000 employees working remotely.

This is the case with most healthcare institutions worldwide. With social distancing becoming the norm, more and more patients are opting for an impersonal approach. Telemedicine service providers are trying to match this level of demand surge.



Just having a telemedicine solution at your disposal is simply not going to be enough. Preparing the devices that run the software—both at the patient end and the healthcare provider end, setting up devices with the supporting applications, troubleshooting systems, ensuring health data is transmitted and stored securely are all going to be critical in times like these. A multi-platform device management solution like [Hexnode](#) can take care of all the security and provisioning challenges, so you can focus on what matters most in providing timely and effective care.

How Can Hexnode Help?

Facilitating a Telemedicine Portal for patients

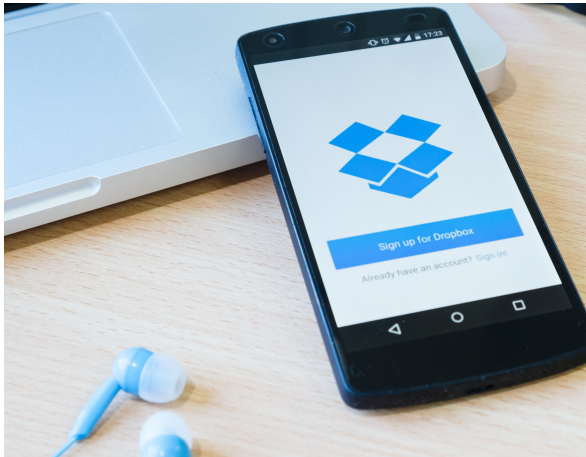
The [World Health Organization \(WHO\)](#) defined Telemedicine as “healing from a distance”. A doctor’s visit without any person-to-person interaction. It is ideal for the COVID-19 pandemic because you can essentially create a virtual appointment with your physician to guide you through any early symptoms. This saves time for hospital staff, as they can attend to patients in this manner. It also alleviates the risk of the virus spreading to the hospital staff or physician.

Now even though this method diminishes the risk of the virus spreading, it opens a Pandora’s box of device management issues. Providing a smooth experience for users at both ends of the spectrum i.e., doctors and patients is also important.

Securing mobile devices in healthcare institutions is a top priority. These devices house Patient Health Information (PHI). This is extremely confidential information and any form

of data leaks should be avoided at any cost. Setting up a remote access VPN client would be a step in the right direction as it protects data in transit i.e. when there is communication between the doctor and the patient or any other external source. With the help of Hexnode MDM you can facilitate a Telemedicine portal for your patients through these features:

App and content management



Hexnode has the capability to facilitate User or Device groups. These groups may contain users or devices with homogenous functionalities. App or Content can be pushed to these groups in bulk, messages can also be broadcasted in the desired groups.

Using the file management capabilities of Hexnode UEM, documents like PHI reports can be pushed to doctors or healthcare works working remotely.

Remote access

For Android Devices that have been issued to patients, the 'Remote View and Control' feature of Hexnode MDM allow admins to monitor and manage an enrolled device's screen remotely, easily and effortlessly, directly from the Hexnode MDM Console. This feature allows to track devices, take control of devices as if the unit were in hand and use a mouse and virtual keyboard to operate them.

Since remote access and control is a critical feature, only the admin may have access to it. But the admin can add multiple technicians to decide which healthcare staff member can take control of the devices. For example, App and reports manager role can be assigned to the staff member responsible for pushing medical apps to the devices. For iOS devices, the admin can remotely, view, monitor and manage devices in real-time. Through these remote access functionalities, doctors can check the vital signs of patients, which would be displayed on the devices issued to the patients with the help of telemedicine software. Signs such as heart rate, oxygen intake levels, and other vitals is made easily accessible to doctors through this feature.

Medical kiosk mode

With the kiosk lockdown feature available on both Android and iOS platforms for Hexnode MDM, the admin can lock down the patient's device with a single app or multiple app kiosk modes.

With such lock-down capabilities, these devices can be converted into dedicated-purpose-driven tools. It may only run pre-approved medical apps or telehealth software used to track the patient's state of health. Essentially this creates a carepoint with on-demand consultations provided by a physician in a physical point of care.

Inappropriate system functionalities such as camera, call, and texting, social networks, screenshots etc. can be disabled for a hospital environment. Hexnode's messenger can be used to pass critical messages, notifications or instructions at ease from the admin to the Kiosk devices.

The admin can also use the silent app installation feature to install apps directly to the Medical Kiosk device, remotely, without any user intervention. Through app grouping, the admin can also compile the critical medical apps which need to be deployed to all medical kiosk devices.

Wearables troubleshooting



Telemedicine software providers may use wearable technology to collect vital information about the patient. Information like heart rate can be easily monitored with the help of wearables. With Hexnode MDM you can determine how the device will behave with the managed device issued to the patient. You can configure and troubleshoot these wearables remotely too.

Managing devices used by the hospital staff

Hospital staff including doctors and nurses are in the frontline for this fight against COVID-19. They are putting themselves in personal danger to curb this pandemic. So, in this time of crisis hospital staff require secure access to patient information, in an efficient manner.

Securing patient's Protected Health Information (PHI)

Hexnode can help your healthcare institution in developing data protection policies that aim to minimize inadvertent data loss. The IT administrator can ensure that sensitive data is bound to the safety of corporate devices.

With the help of managed open-ins, you can prevent staff members from opening PHI documents on unmanaged devices. This ensures that sensitive content doesn't get opened in unmanaged devices and then gets leaked. Restrictions can also be placed on transfer via Bluetooth, USB, tethering or any other means.

You can place a network restriction that would only allow documents such as the PHI to be opened in managed corporate WiFi or an approved VPN. This can mitigate online data breaches to a great extent along with that data during transit would also be protected with this restriction.

Restriction can also be placed on Copy / Paste functionality. This can prevent data leakage through any unmanaged applications. This is particularly relevant in a BYOD scenario.

If the device issued to any staff member containing PHI gets lost or stolen, you can initiate certain actions through Hexnode's console.:

The admin can activate a **lost mode protocol**. This locks down the entire device and displays a short text which has been entered by the admin. All the functions of the device would be suspended. If there is no way of retrieving the stolen or lost device, the admin can initiate a remote wipe. This would perform a factory reset on the device and all the data within it would be wiped clean.

Manage Point of Care devices



Point of Care or POC is the stage at which physicians provide patients with healthcare products and services at the time of care. Mobile devices like Tablets are used nowadays to document the happening at the POC. The aim of this process is to collect medical information relating to the health care needs of patients. The document prepared is legal in nature and has confidential information in it. So, the devices used to collect the said information should be secure in every way possible. The Electronic Medical Record (EMR) should not be vulnerable to data breaches or leakages. The admin has to utilize all the data loss prevention actions which are available to them through Hexnode to keep this device safe.

Network restrictions have to be placed on these devices so that they are never opened in an unmanaged WIFI network or without a VPN. A strong password policy must be pushed to these devices so as to avoid unnecessary logins.

BYOD management

Issuing work-ready devices to all the hospital staff members in your healthcare institution on short notice is a herculean task, to say the least. A possible workaround for this dilemma is adopting a BYOD policy. Hexnode MDM has adept BYOD management capabilities in-built.

For Android devices, the admin may deploy Android for Work profiles to isolate patient information and personal data. For the purpose of BYOD, you can enroll the device as a profile owner. This can be easily done by downloading the Hexnode for Work app available in the Play Store and enrolling the device via open enrollment methods like QR codes or just entering the portal name. The apps within the work container would be given a work badge.

Specific restrictions like Network restrictions, copy/paste restrictions, etc can be placed on these apps. Along with that, the admin can perform a remote wipe to remove all the data from the work profile if the user decides to stop using the device or it gets lost or stolen.

For iOS devices, the admin can create a policy for a Business Container in the Hexnode portal and associate the targeted devices to the said policy. Restrictions like not being able to open managed documents, like PHI documents, in unmanaged apps and vice versa, blocking the sharing of managed documents via AirDrop, etc. can be applied.