Deploying iPad to Patients

Setup Guide

Contents

Overview

Healthcare institutions are increasingly focused on engaging patients to be actively involved in their health and delivering a great experience throughout their stay in the hospital. Deploying iPad with patient-centered apps enables hospitals to enhance each step of the patient journey, from check-in through discharge. With third-party iPadOS apps, hospitals can empower patients to access their daily schedule, connect with their care team, track their progress, get educated on their treatment plan, order food, and personalize their entertainment — putting patients in the center of their care. And with Apple TV in each room, institutions can enrich patients' experience by allowing them to stream movies from iPad to a larger screen using AirPlay.

This setup guide offers guidance to the hospital IT staff who are configuring and deploying iPad for patients to use. iPad can be preconfigured with minimal setup so that patients have access to iPadOS apps. And IT can use mobile device management (MDM) to protect patient data while also preserving a great user experience. Once a patient has been discharged, iPad can be securely wiped to remove all patient-generated data and reset to factory settings so it's ready for the next patient.

A key decision for organizations deploying iPad to patients is choosing between in-room and centralized storage of the device (described in the In-Room Storage and Centralized Storage sections). In-room storage is enabled by the over-the-air (OTA) wiping and resetting of iPad, which allows the device to stay in the patient's room at all times. Many hospitals prefer this deployment because it minimizes work for nurses or other staff members. Or hospitals may have compelling reasons for choosing centralized storage deployment, such as having fewer iPad devices than rooms or having staff or volunteers who are readily available to help keep track of devices as patients are admitted and discharged.

Regardless of which deployment scenario you choose, the preparation steps described in this paper are important for any successful deployment.

Choose app solutions

Many great app solutions are available for patients, including MyChart Bedside, Lana Health, and Fusion Bedside. These solutions include robust services that integrate seamlessly into existing hospital systems, like nurse call, entertainment systems, room controls, electronic medical records (EMR), and more.

When evaluating whether a potential app solution is right for your institution, it's important to consider the following:

- What specific tasks does the app solution support?
- Is the app onboarding process efficient and easy?
- Does the app solution integrate with your systems?
- Is the app intuitive and easy for new users to learn?
- What's the recommended deployment model?

Getting Prepared

This section outlines three steps to follow when you're preparing to deploy devices and apps in the hospital.

Evaluate your infrastructure

The first step is to assess your network infrastructure. The hospital's layout and how people interact within the physical space is critical to how you design your network and plan for Wi-Fi coverage and capacity.

Wi-Fi and networking

Consistent and dependable access to a wireless network is key to setting up and configuring iPad devices. Confirm that your hospital's Wi-Fi network can support multiple devices with simultaneous connections from all your users. You might also need to configure your web proxy or firewall ports if devices are unable to access Apple's activation servers. Apple and Cisco are optimizing the network experience for devices using iOS 10 or later or iPadOS. Talk to your Apple or Cisco representative to get the latest information about these networking features.

Content caching

An integrated feature of macOS, content caching stores a local copy of frequently requested content from Apple servers, helping minimize the bandwidth needed to download content on your network. Content caching speeds up the download and delivery of software from the App Store. It can also cache software updates for faster downloading to multiple iPadOS devices. Content caching includes the tethered caching service, which allows a Mac to share its internet connection with many iPad devices connected by USB.

Investing in an MDM solution

MDM gives organizations the ability to securely enroll iPadOS devices in the hospital environment, wirelessly configure and update settings, establish policies, deploy and manage apps, and remotely wipe or lock managed devices. These features are built into iPadOS and enabled by third-party MDM solutions. MDM solutions are available from a wide range of vendors and can be cloud hosted or installed on premise. They come with different features and pricing, so you have flexibility in deciding which solution best fits your needs. Some MDM solution providers also offer predefined settings that make it even easier to configure devices for patient use.

Create a configuration

Once you've selected an MDM solution, you'll need to create a configuration that's specifically optimized for the patient use case and that your MDM solution can install over the air. A configuration typically contains settings and restrictions that set up the device in a way that's appropriate for patient use. These settings will help streamline the initial patient experience and disable features or services that might store personal data or be unnecessary.

Restrictions

The following settings are examples of restrictions you'll likely enable so that no personal information is left on the device. **Note:** Descriptions may vary by MDM solution.

Device management: Disallow manual profile installation, disallow restrictions configuration, disallow device name changing, disallow account modification, force Limit Ad Tracking, and disallow pairing with non–Apple Configurator hosts.

Data management: Disallow documents from managed sources to unmanaged destinations, disallow documents from unmanaged sources to managed destinations, and enforce AirDrop as an unmanaged destination.

Apps: Disallow the App Store icon on the Home Screen, disallow app removal, disallow in-app purchase, disallow user to trust unmanaged enterprise apps, and hide specific apps on the Home Screen.

Media: Disallow the use of Game Center, skip Apple ID password for media purchases, and restrict media content as needed.

Home Screen layout, Lost Mode, and other settings

You can manage how apps, folders, and web clips are arranged on a supervised device's Home Screen. You can also enable use of the device's camera so that hospital staff can scan a patient's QR code using a secure patient app or add the patient's photo to an EMR app.

To track a missing iPad, make sure your MDM solution supports the features related to Lost Mode, such as a lost message text, tracking the device's location, and reenabling Lost Mode after a reset or restore.

Note: Lost Mode allows an administrator to query the location of an organization-owned lost device even if the user has disabled location services.

Automate device setup

Apple Business Manager (ABM) and Apple School Manager (ASM) provide a fast, streamlined way to deploy hospital-owned iPadOS devices that were purchased directly from Apple or from participating Apple Authorized Resellers or carriers. These programs enable automatic MDM enrollment of devices on activation. With ABM or ASM, devices are always supervised and MDM enrollment is mandatory.

You can manually enroll iPad in ABM or ASM using Apple Configurator, regardless of how you purchased the device. But the user has a 30-day provisional period to remove the device from enrollment, supervision, and MDM.

Assigning apps to devices

For in-room and centralized storage deployments, you'll need to assign apps directly to devices using your MDM solution or Apple Configurator. Once assigned to a device, an app is pushed to that device by MDM — no Apple ID account is required. Anyone who uses that device has access to the app.

Setting up an app catalog

It's highly recommended that you work with your MDM solution provider to create a catalog of apps that you'd like your patients to use. Typically, only a few essential apps might need to be preinstalled for the patient during initial setup. An app catalog presents suggested apps for patients to download themselves as needed. This reduces the load on your Wi-Fi network and significantly reduces deployment time.

In-Room Storage

Once your network and MDM infrastructure are set up, you'll need to choose your preferred deployment scenario. With an in-room storage deployment, you can leverage OTA device setup and software updates and then automatically reset iPad when the patient is discharged. This deployment scenario enables you to keep devices in each room, so patients can customize their iPad the moment they arrive.

Perform initial setup

When a patient is first handed an iPad, the built-in Setup Assistant will guide them through personalizing the device. From the Hello screen, the patient should choose a language, tap a region, tap Set Up Manually, and choose a public Wi-Fi network. No other steps are required, and all other Setup Assistant screens can be skipped through MDM.

To establish initial connectivity and enrollment, you should provide a public Wi-Fi network without using a captive portal. Once an iPad is enrolled, MDM can automatically transition the device to a private Wi-Fi network for the rest of the setup. Using a private Wi-Fi network will also provide better security for the duration of the patient's hospital stay.

When this setup is complete, MDM will configure the device settings and install apps over the air. The amount of time this takes will depend on your Wi-Fi network, whether you're using Caching Server, and the number of apps you're installing on each iPad.

Reset your device

After the patient is discharged, you'll need to reset the device for the next patient by erasing all content and settings. You can either wipe the iPad remotely using MDM or manually reset it.

Remote wipe with MDM

To wipe iPad remotely, MDM can perform a full device wipe over the air. Typically an IT administrator performs this task, but it's better to automate the remote wipe command with your MDM solution. For example, in a hospital setting, the EMR system can send a notification to the MDM solution when a patient is discharged. This signal can then trigger the MDM server to remotely wipe the device. There are two potential approaches to enabling this process:

- MDM vendors can integrate their solutions with EMR providers to monitor when a patient gets admitted, discharged, or transferred (ADT) to initiate the remote wiping of iPad to factory settings. Return to Service, introduced in iPadOS 17, allows an MDM solution to provide the device with all the information needed as part of the erase command to reset and reenroll. This includes the ability to define what Wi-Fi to connect to and what MDM to enroll in. As part of the process, the previously selected language and region settings are applied. Once the device receives the erase command from MDM with the additional information, it resets, securely erases all data, connects back to Wi-Fi, activates, enrolls into management, and returns back to the Home Screen — ready to be used.
- EMR systems can automate the process so that iPad is wiped the moment a patient has been admitted, discharged, or transferred.

Manual reset

For a manual reset, a staff member can go to General settings, tap Transfer or Reset iPad, then choose Erase All Content and Settings. Some MDM vendors also offer a reset app that allows patients to securely reset all user data on iPad with one tap.

Note: When using a centralized storage deployment, it's not necessary to enable remote wipe. Learn more in the following "Centralized Storage" section.

Centralized Storage

The alternative to in-room storage is storing multiple iPad devices in a secure cart attached to a portable workstation. Each iPad is connected by USB, and an automated enrollment process is used to erase it, apply configurations, and automatically bring the device to the Home Screen before it's assigned to the next patient.

This workflow uses Apple Configurator — or one of several other turnkey solutions — to enable a hands-free setup, so users don't need to be involved in the activation process. This also makes it easy for staff to check iPad devices in and out.

Store

The workflow can be achieved with a workstation and an appropriate USB hub. But the following considerations can improve the efficiency of the deployment, as well as the user experience for patients and staff:

- Sufficient power and throughput to support multiple devices
- Indicator lights or a display that provides device status
- Dimensions that support iPad and any accessories, like a case
- Security of the devices that balances easy access for staff

Connect

Wired connectivity provides an opportunity to reduce the burden on your Wi-Fi network and your location's WAN connection.

- Use the content caching service in macOS.
- Allow the workstation to share its network connectivity with the iPad devices by USB.

Automate

To eliminate the need to repeat various steps on every device refresh, consider the following when choosing and configuring an automation tool:

- Physically connecting the device should trigger the refresh.
- Use a consistent supervision identity across all workstations and your MDM.
- Fully erase and restore the device after each use.
- Provide a Wi-Fi configuration profile for ongoing connectivity.
- It's recommended that the device be enrolled in ABM or ASM.
- Enroll the device in your MDM solution.
- Use MDM to set the time zone (for iPadOS 14).
- Skip all setup screens.

Administration

Depending on your automation solution, ongoing workstation management can be performed through either a web interface or a client management solution like Apple Remote Desktop.

Install Apple Remote Desktop

Apple Remote Desktop is a macOS remote desktop management app. It can be used for software distribution, asset management, and remote assistance. With a centralized storage deployment, Apple Remote Desktop allows you to remotely manage multiple Apple Configurator workstations from a single Mac. This enables you to quickly make any required updates to your configuration profiles without having to interrupt your staff from checking iPad devices in and out.

Take a package, from either Apple or a third party, and simply use the install package to copy and install it on multiple workstations in your hospital environment. The screen-sharing features of Apple Remote Desktop allow you to provide immediate help to your remote stations, saving time for both you and the hospital staff.

To learn more about setting up Apple Remote Desktop, visit support.apple.com/guide/remote-desktop/welcome/mac.

Summary

You have options for deploying and managing iPad for your patients to use, whether your hospital deploys devices to a group of users or across the entire organization. And by choosing the right deployment strategies for your organization, you can help your staff focus on what's most important — providing care to your patients.