CASE STUDY

Leading healthcare provider in major metropolitan area manages mobile access to Epic patient records and healthcare systems via shared devices using Imprivata

No matter the scale, Imprivata GroundControl can automate, secure, and optimize the use of shared iOS and Android devices across an enterprise

Challenge

- Providing mobile access across hospital sites using multiple legacy systems
- Deploying and managing over 8,000 shared mobile devices across a staff of 25,000+
- Improving workflow efficiency for nurses, doctors, and patient transporters

Solution

- Imprivata GroundControl provides security and efficiency with automated device management, secure device checkout, and fast, secure access with Enterprise Password AutoFill
- Imprivata OneSign® Single Sign-On enables more efficient logins to save time, effort, and resources

Results

- Simplified management of over 8,000 shared mobile devices with automated workflows and cloud-based visibility into fleet status
- Easy shared-device check-out/check-in for clinicians and simple asset management of hospital-owned devices
- Secure, frictionless access for mobile applications improving healthcare workflows

Organization snapshot

Expansive, influential healthcare provider in a major metropolitan area delivers specialized services to over 700,000 people across multiple municipalities.

A leading healthcare provider in a major metropolitan area delivers specialized services to over 700,000 people across multiple municipalities. With over 25,000 staff delivering high-quality care and support, the facility estimated it would need over 8,000 mobile devices to provide access to Epic Rover for frontline teams. With a need for so many devices, the provider required a comprehensive and robust solution to manage them efficiently. The provider selected Imprivata GroundControl to do the job.

Challenge: Promoting flexible workflows with mobile tools

For years, the provider sought to improve efficiency, data security, and patient outcomes. As part of a system-wide Epic implementation, it was decided that mobile devices would be deployed to support flexible access to patient records.

With an average of over 8,000 staff working during each shift, the provider needed to adopt a shared-device strategy to provide a cost-effective approach to supporting mobile workflows. The provisioning and management for such a large number of devices needed to be automated as much as possible, all while patient data security, efficiency, and auditability were maintained.

From an information governance perspective, the provider's number one priority was to "protect the data of the general public, patients, and staff," according to one senior engineer.

Solution: An end-to-end mobility solution for shared devices, rooted in digital identity

Deploying devices at scale

After deciding to take a shared-device approach, the provider evaluated solutions to support the mammoth task of provisioning over 8,000 mobile devices. The shared mobile devices needed to support use of Epic Rover, mainly used by nursing workflows. The provider also needed to maintain a spare pool of physician devices for access to Epic Haiku.
Due to the success of their single sign-on implementation, the evaluation team tested Imprivata GroundControl for automated provisioning and deprovisioning of shared mobile devices, and quickly chose this as the system-wide solution.

> **"All the configuration for devices was preloaded so on the ward 99.9% of the device setup was automated."**
>
> – Senior End User Computer Engineer & Epic Client Systems Administrator

With a well-executed implementation strategy for device configuration in place, the provider was able to commission over 6,000 phones in hundreds of locations over a period of only two-and-a-half weeks.

Supporting end user efficiency

The provider is a long-time user of Imprivata OneSign, a solution that enables single sign-on (SSO), across its multiple hospital locations. Without the need for clinicians to remember multiple user IDs and passwords or to repeatedly, manually log in and out of multiple systems, end users save valuable time over each shift and remove frustrating workflows. Extending these same workflows to mobile devices and applications was a logical evolution of the provider's digital identity strategy.

The provider's system and IT administrative team found Imprivata OneSign Single Sign-On integrated into Imprivata GroundControl well, leading to a smooth, efficient workflow for staff. One senior engineer reported that the provider was able to take this capability to senior leadership, who "fell in love with the product" the second they saw it.

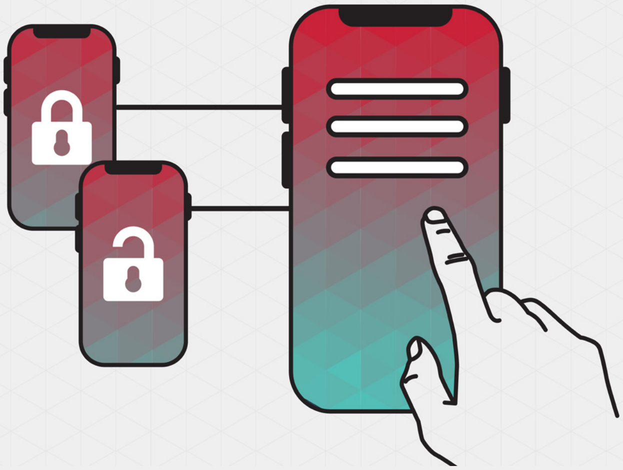
Results: Delivering the secure power of mobility to clinicians, labs, patient transporters, and more for improved workflow efficiency

The advantages of a mobile access and control solution have been clearly demonstrated by the provider, going from having only a very small number of iPads in use, and no means to manage the introduction and provisioning of shared devices, to having a customized, ready-for-use large scaled solution which could be rapidly introduced into each location. This enabled the successful rollout of more than 8,000 shared devices to support the 25,000+ workforce, together with tight controls to minimize loss of devices and a system to easily manage provider-owned mobile device assets.

> **"We found that Imprivata OneSign Single Sign-On integrated into Imprivata GroundControl quite nicely where it allowed us to then pass the user's Active Directory credentials into the Rover application and pretty much just work seamlessly."**
>
> – Senior End User Computer Engineer & Epic Client Systems Administrator

Minimizing device loss and protecting investments

Supported by Imprivata GroundControl, rules have been put in place so that devices are tracked as they are moved so that they can be returned to their registered location and depersonalized between each user. Users are also allowed to take a phone home or out of the hospital to work, but if the phone has not been returned within one hour of shift end, then the manager will be emailed to request the phone's return.



If doctors do not have their own Bring Your Own Device (BYOD) with them, they can check out a device with Haiku access for a shift and still have secure and fully auditable access to their notes and patient data as they work around the hospital.

The provider built out additional automation rules as well. A senior engineer noted that when a doctor takes a phone from one place and leaves it in another, the manager of the department where the device was taken then "gets an email that says a specific user has taken a phone with this serial number and where they have left it, so that it can be collected and returned to its rightful location."

Looking to the future: Commitment to providing secure, mobile workflows

Beyond the clinical staff, the solution has been deployed to hundreds of patient transporters who use Rover to access the patient transporting system. Imprivata GroundControl was also used in the management of the devices for this group. They tap in and out and use Rover devices when, for example, collecting samples from different locations and delivering these to specific labs for testing. They also use them when moving patients around the hospital, with simplified management and access to mobile applications improving healthcare workflows.

The provider successfully leveraged Imprivata to gain the full benefit of their mobile assets, bringing secure and efficient mobile workflows to end users across the provider's network of hospitals and clinics, and supporting IT and mobile teams in effectively managing an extensive fleet of shared devices across dispersed locations.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com