WHITEPAPER

Shared mobile devices in healthcare: Opportunities, trends, and security challenges

imprivata®

CONNECTED HEALTH
Powered by Wavelink

Healthcare organisations are looking to mobile technology to streamline clinical workflows and improve care quality. However, disjointed mobile device access control solutions and practices can frustrate users, introduce security vulnerabilities, and stall mobile healthcare initiatives.

Forward-looking organisations are turning to a new generation of mobile security solutions to safeguard healthcare applications and data without impeding clinician productivity. This new class of user authentication solutions lets hospitals and healthcare systems fully leverage mobile technology without impairing clinical efficiency, compromising IT systems, or exposing sensitive patient information.

This paper reviews trends in healthcare mobility, explains some of the challenges mobile technology presents for IT and security teams, and describes the barriers and risks associated with traditional approaches to securing mobile devices. It summarises the capabilities and benefits of a next-generation mobile authentication solution, and outlines how Imprivata Mobile Device Access enables fast, secure access to clinical mobile devices and applications.

Mobile technology is transforming healthcare

Advances in mobile technology have lead to a paradigm shift in care delivery for the healthcare industry. Armed with specialised smartphones and tablets, today's on-the-go nurses and doctors can access all their critical healthcare applications and information from any location, at any time.

Mobile healthcare solutions can:

- Help cut the cost of care by reducing IT expense and complexity
- Increase staff productivity and reduce clinical burnout by eliminating manually intensive and time-consuming tasks
- Improve patient satisfaction and outcomes by increasing clinical workflow efficiency, improving care team communications and collaboration, and enabling faster, more personalised care

Around the world, hospitals, medical groups, and healthcare systems of every size and type are introducing mobile technology to provide better patient experiences and to improve provider satisfaction. Industry observers say 90% of healthcare organisations have already executed, or plan to execute, mobility initiatives.
And according to a Zebra Technology survey of several global healthcare markets, use of mobile devices by bedside nurses is expected to increase from 65% in 2017 to 97% in 2022, while use of mobile devices by physicians is projected to grow from 51% to 98% over the same period.[1]

1. The Future of Healthcare: 2022 Hospital Vision Study, Zebra Technologies

Mobility and security go hand in hand

Healthcare organisations must institute strong security measures to control and monitor access to applications, and to safeguard the integrity and privacy of PHI on mobile devices.

The proliferation of mobile devices poses a variety of challenges for healthcare IT organisations and security teams. Care delivery organisations must implement new systems and practices to manage and maintain mobile devices in use across the enterprise. They must institute strong security measures to control and monitor access to applications, and to safeguard the integrity and privacy of sensitive patient data. But they must also introduce reporting and auditing systems to support Privacy Act 1988, APEC Privacy Framework, GDPR, HIPAA and other data protection regulations across the globe.

Conventional approaches to protecting mobile applications and data are inherently inefficient and fraught with risk. Many organisations rely on tedious, manually intensive authentication methods to secure access to mobile technology. Healthcare professionals are forced to hand-enter PINs, user IDs, and passwords for each device and application which impairs productivity, frustrates users, and inhibits the adoption of mobile technology. To make matters worse, many organisations use a variety of authentication solutions and methods to secure different applications and endpoints, which complicates administration and can force clinicians to manage multiple security credentials, such as tokens.

Unable to remember dozens of different device passcodes and application credentials, clinicians often take shortcuts that can lead to data leakage, compliance violations, and cyberattacks. Common security workarounds include leaving shared devices unlocked, using one PIN for all users and devices, choosing the same password for all applications, and writing passwords on scraps of paper or sticky notes for the world to see.

Next-generation access management solutions streamline mobile usage

To leverage the full potential of mobile technology, IT organisations must find ways to safeguard applications and data without burdening already overstretched medical staff. Innovative organisations are turning to a new generation of mobile authentication solutions that give healthcare workers fast, easy, and secure access to all their applications and data, from any location, using any institution-owned device – smartphone, tablet, workstation, or virtual desktop.

Next-generation mobile access control solutions eliminate repetitive and risk-prone authentication schemes that rely on manual entry of device and application credentials. Instead, users securely access mobile devices and sign on to applications through a single, simple action, such as the tap of a proximity badge. This straightforward approach eliminates password fatigue and makes it easy for clinicians to share devices without compromising security.

Imprivata Mobile is the healthcare industry's first and only mobile authentication solution that enables fast, secure access to clinical mobile devices and applications.

Best-of-breed authentication and single sign-on (SSO) solutions support a wide array of endpoints, allowing users to securely access mobile devices, workstations, and virtual desktops, using the same simple method. Leading solutions also offer end-to-end management and reporting tools that let administrators set policies and monitor access activity in a uniform manner for all devices and applications across the enterprise.

Imprivata Mobile eliminates adoption barriers

Imprivata Mobile is the healthcare industry's first and only mobile authentication solution that enables fast, secure access to clinical mobile devices and applications. With Imprivata Mobile, users can access shared clinical mobile devices with the simple tap of a proximity badge, and can then single sign-on (SSO) to their applications.

The solution removes mobile adoption barriers, ensuring secure access to critical applications and patient data without impeding user productivity. Imprivata Mobile User Access Management eliminates password fatigue and user frustration and lets overburdened clinicians spend more time caring for patients.

IMPRIVATA MOBILE DEVICE ACCESS BENEFITS

- Improves clinical workflow efficiency
- Frees up clinicians to focus on patient care
- Improves security of devices and information
- Streamlines compliance auditing
- Drives adoption of mobility initiatives

Specifically designed to safeguard shared mobile devices, Imprivata Mobile features a unique functionality tailored to supporting security and efficiency in a shared-use environment. Imprivata Mobile provides comprehensive monitoring and reporting capabilities, making it easy for IT and security teams to track access activity and support compliance audits. And seamless integration with Imprivata OneSign® lets IT administrators institute uniform user authentication policies for all systems and workflows from a single, centralised platform. Better still, authorised healthcare workers gain secure access to all clinical devices and applications using a single proximity badge, making for unmatched convenience and simplicity.

Improving workflows across the enterprise

Mobile technology has the potential to streamline clinical workflows and improve patient care and satisfaction. But conventional access control solutions can impair user productivity, introduce risk, and hinder the adoption of mobility initiatives. Next-generation access management solutions can help care delivery organisations overcome common deployment obstacles and unlock the full potential of mobile technology, without sacrificing security.

Best-of-breed mobile authentication solutions like Imprivata Mobile provide:

- Rapid, secure device access and single sign-on to mobile applications
- Efficient user switching for shared mobile devices
- End-to-end reporting and management tools for IT, security and compliance teams

Imprivata Mobile is a comprehensive, end-to-end mobility solution that helps organisations optimise their mobile strategies. Imprivata delivers automated device provisioning, secure device checkout, and fast, secure access for users, helping customers unlock the full potential of shared mobile devices by ensuring a fast, efficient workflow while improving security and auditability.

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 03 8844 5533
or visit us online at intl.imprivata.com

Please contact our Australian partner, Connected Health at 1300 147 000
or sales@connected-health.com.au

Mob-WP-Shared-mobile-devices-INTL-0123