imprivata®

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

Healthcare organizations are looking to mobile technology to streamline clinical workflows, improve care, and boost patient outcomes. But disjointed mobile device access control solutions and practices can frustrate users, introduce security vulnerabilities, and stall mobile healthcare initiatives.

Forward-looking organizations 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 let hospitals and healthcare systems take full advantage of all the benefits of mobile technology without impairing workflows, compromising IT systems, or exposing protected health information (PHI).

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

Mobile technology is transforming healthcare

Advances in mobile technology are fundamentally transforming the healthcare industry. Armed with specialized smartphones and tablets, today's on-the-go nurses and doctors can access all their critical healthcare applications and patient records from any location, at any time.

Mobile healthcare solutions help cut the cost of care by reducing IT expense and complexity. They help boost staff productivity and reduce clinical burnout by eliminating manually intensive and time-consuming tasks. They also improve patient satisfaction and outcomes by increasing clinical workflow efficiency, improving care team communications and collaboration, and enabling faster, more personalized care.

Around the world, hospitals, medical groups, and healthcare systems of every size and type are introducing mobile technology to improve patient experiences and boost results. Industry observers say 90% of healthcare organizations have already executed, or plan to execute, mobility initiatives. And according to a Zebra Technology survey, 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]

Mobility and security go hand in hand

The proliferation of mobile devices poses a variety of challenges for healthcare IT organizations and security teams. Healthcare organizations must implement new systems and practices to manage and track large numbers of smartphones and tablets scattered across the enterprise. They must institute strong security measures to control and monitor access to applications, and to safeguard the integrity and privacy of PHI. But they must also introduce reporting and auditing systems to support HIPAA, GDPR, and other data protection regulations across the globe.

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

To unleash the full potential of mobile technology, IT organizations must find ways to safeguard applications and data without burdening already overstretched medical staff. Innovative organizations 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.

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

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

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

Next-generation mobile access control solutions eliminate repetitive and risk-prone authentication schemes that rely on hand-entering device PINs 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.

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 Device Access eliminates adoption barriers

Imprivata Mobile Device Access 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 Device Access, healthcare professionals access clinical mobile endpoints with the simple tap of a proximity badge, and then single sign-on to all their applications.

The solution breaks down mobile healthcare adoption barriers, ensuring secure access to critical applications and PHI without impeding user productivity. Imprivata Mobile Device Access 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 and compliance auditing
- Drives adoption of mobile devices and applications

Specifically designed to safeguard shared mobile devices, Imprivata Mobile Device Access features a unique fast user-switching capability that automatically logs out an idle user, and logs in a new one, for ultimate efficiency and security. Imprivata Mobile Device Access 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, centralized platform. Better still, authorized healthcare workers gain secure access to all clinical devices and applications using a single proximity badge, making for unmatched convenience and simplicity.

KING'S DAUGHTERS MEDICAL CENTER
Taking Medicine Further℠

Imprivata Mobile Device Access in action

King's Daughters Medical Center, a 99-bed facility in Brookhaven, Mississippi, uses Imprivata Mobile Device Access to enable simple and secure access to Zebra mobile healthcare devices. The Zebra device delivers the capabilities of a hand-held scanner and a wall-mounted computer in a compact mobile end point, dramatically simplifying clinical workflows.

Used in conjunction with Imprivata OneSign, Imprivata Mobile Device Access eliminates tedious logon processes and password fatigue, allowing nurses and doctors to effortlessly access Zebra mobile devices as well as traditional clinical workstations with the simple tap of a proximity badge. The end-to-end Imprivata solution significantly improves user productivity, allowing care providers to focus on patients. It also spurs mobile adoption by making it easy for users to log on to Zebra devices and mobile applications. Thanks to Imprivata, the optional Zebra technology is widely used throughout the hospital.

Conclusion

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

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

- Rapid, secure device access and single sign-on to mobile applications
- Efficient user switching for shared mobile devices
- Unified access and SSO for all endpoints – mobile devices, workstations, virtual desktops
- End-to-end reporting and management tools for IT, security and compliance teams

Imprivata Mobile Device Access streamlines access to critical applications and PHI allowing healthcare professionals to focus on patient care. The solution improves workflow efficiency and clinician satisfaction, helping to drive the adoption of mobile devices and applications. Plus, it gives IT and security administrators greater visibility and control over users, improving management and compliance. Imprivata Mobile Device Access helps healthcare organizations unleash mobile productivity, mitigate risks, and make the most of their mobile technology investments.

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience.

For further information please contact us at

1 781 674 2700
or visit us online at
www.imprivata.com

Offices in

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands