INFOBRIEF

Unlock the power of mobile workflows

Organizations are looking to mobile tools to improve freedom and flexibility of workflows, especially in the face of constrained budgets and personnel resources. However, it isn't easy to achieve an efficient workflow experience on mobile devices without compromising security, privacy, and compliance. Additional security requirements can create barriers that hinder usability and threaten adoption, leaving organizations unable to optimize their investment in mobile technology.

Imprivata delivers mobile device security and privacy without compromising on workflow efficiency, solving challenges for both BYOD and enterprise-owned device environments. By leveraging digital identity to support security and compliance directly within mobile workflows, Imprivata eliminates friction that can impact usability while also reducing points of exposure. Imprivata removes barriers to use and supports care delivery with secure, real-time access to critical tools and information, from anywhere at any time.

Improve access security on personal devices

When organizations allow employees to expand their workflows beyond the walls of the organization, it's critical that privacy and security measures expand in kind, offering protection regardless of where or how employees access sensitive information. To maximize the benefits of mobile technology, organizations must enforce strong authentication in convenient, familiar ways that usability and adoption. Imprivata Digital Identity plays a key role in supporting this dynamic.

Enforce stronger, practical security on mobile devices

- Enforce strong authentication methods and complex passwords without disrupting users
- Require multifactor authentication to access sensitive information
- Establish trust to leverage mobile-based authentication modalities

Create a seamless user experience

- Leverage familiar authentication workflows on your mobile device, such as facial recognition, soft tokens, and biometric identification
- Turn mobile devices into a trusted, second factor of authentication for a hands-free authentication experience
- Support secure access to critical tools from anywhere, at any time, including EPCS-compliant devices that meet FDA requirements for prescribing controlled substances

Enable privacy in shared-use environments

Organizations are leveraging shared-device models to help reduce the investment needed to support untethered workflows. As with any workplace technology, usability and efficiency are equally important, and staff need to access all critical tools and information regardless of which device they use. But when resources are shared between users, this balance is more difficult to achieve. Imprivata is the only solution that supports both privacy and personalization in enterprise-owned, shared device environments.

Ensure only trusted access to devices and applications

- Leverage trusted digital identity with badge-tap assignment of mobile devices
- Lock down shared devices between users to prevent unauthorized access
- Enforce authentication after device lock to control access to sensitive information

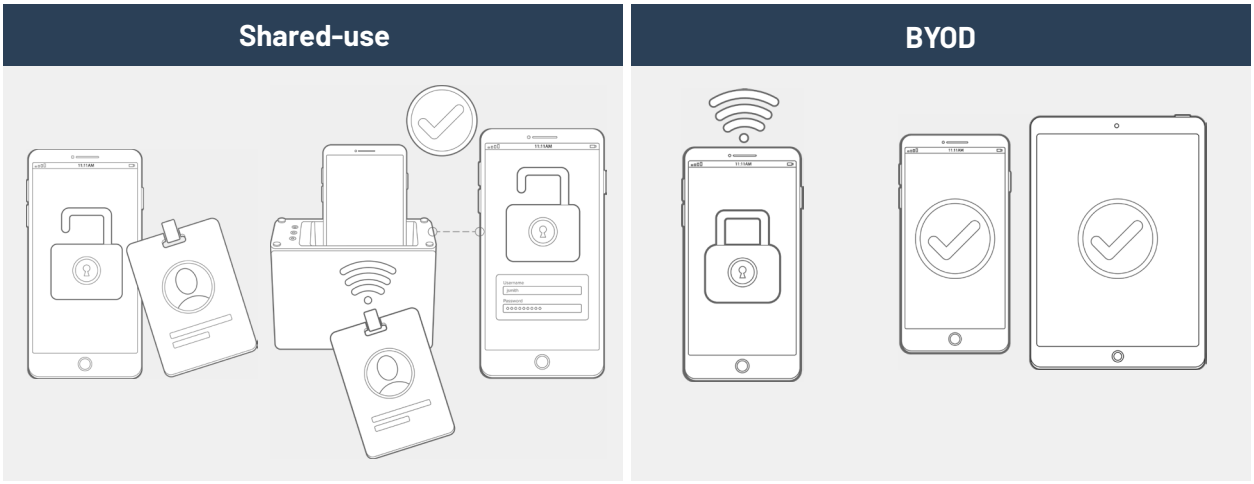
Streamline access and device management

- Leverage familiar authentication workflows on your mobile device, such as facial recognition, soft tokens, and biometric identification
- Turn mobile devices into a trusted, second factor of authentication for a hands-free authentication experience
- Create audit trails for who used which device when, where, and for how long, to reduce device loss
- Depersonalize devices between users by removing user credentials and controlling access to information as devices are exchanged between users

.

Enabling secure access without barriers

By leveraging digital identity to enforce authentication at the device and application level, Imprivata delivers frictionless security for both shared-use and BYOD environments. We support adoption by extending familiar digital identity driven access and authentication to mobile workflows.



Imprivata Mobile Device Access:

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

Imprivata Mobile Access and Control (formerly GroundControl):

Enable a hands-on device management experience from the cloud – maintaining and updating from anywhere at any time. Employees and IT teams benefit from simple, personalized device checkout, effortless application access, and cloud-based management of assets and workflows.

Imprivata Enterprise Access Management (formerly OneSign and Confirm ID) for remote access:

Improve security by enabling enterprise-wide two-factor authentication for remote network access, cloud applications, and Windows servers and desktops.

Imprivata Enterprise Access Management for EPCS:

Providing the broadest range of DEA-compliant two-factor authentication modalities, including Hands Free Authentication, push token notification, and fingerprint biometrics, to make EPCS fast and convenient for providers.

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**

MAC-infobrief-unlock-power-mobile-workflows-0124