imprivata

DATASHEET

Imprivata Enterprise Access Management with secure walkaway technology

Leverage the power of Bluetooth and mobile devices to secure PHI on unattended workstations without disrupting clinical workflow

Securing PHI on shared clinical workstations continues to challenge healthcare. Shared workstations represent a potential point of exposure of PHI and other sensitive data, so they must be properly secured when unattended. But clinicians need fast, easy access to patient information to deliver efficient and effective care.

To mitigate the risk, organizations ask their clinicians to log out of the workstation before they move on, but this is not always a viable solution given the fast-paced nature of care. As a contingency, IT will implement timeouts that automatically lock workstations after a certain period of inactivity. But these timeouts can create challenges themselves.

Key benefits

- Improve security by reducing the risk of unauthorized access to PHI
- Increase clinical workflow efficiency
- Improve patient safety by preventing clinicians charting under the incorrect ID
- Unlock the power of proximity-based authentication for additional workflows, including EPCS

If the inactivity timeouts are too short, they can create inconvenience and frustration for clinicians – for example, if they are reviewing patient charts but not using the keyboard. This then requires clinicians to enter their password yet another time. And, if the timeouts are too long, the risk of exposing PHI or of a clinician charting under the wrong ID increases.

Striking the right balance of security and convenience on shared workstations is critical, but a viable solution has remained elusive.

Secure walkaway, powered by Bluetooth

Imprivata Enterprise Access Management with secure walkaway technology (EAM) leverages the power of Bluetooth Low Energy (BLE) and the ubiquity of mobile devices to secure PHI on shared workstations without disrupting clinical workflow or patient care. Locking and unlocking of workstations is based on the presence of the user's mobile device, which removes the burden of passwords and disruptive inactivity timeouts.

Using secure BLE connectivity, EAM enables continuous authentication and monitors for the Imprivata ID mobile app running on the user's mobile device. If EAM detects the presence of the user's mobile device, the workstation will remain unlocked. This enables organizations to set much longer inactivity timers to avoid exposing PHI without disrupting workflow.

When the user steps away from the workstation, EAM will no longer detect their mobile device and it will initiate the pre-defined logout sequence. And, when the user returns, their mobile device will be detected again, which will unlock the workstation without any interaction from the user.

This fast, seamless authentication secures PHI on shared workstations without impeding clinical access. Organizations can employ shorter timeouts to ensure security, knowing they will only be invoked when a workstation is unattended (and not when a provider is simply reading something on the screen).

With EAM, organizations can:

- Increase security by reducing the risk of unauthorized access to PHI on unattended workstations
- Improve clinical workflow efficiency by limiting the need to manually interrupt inactivity timers
- Improve patient safety by minimizing the risk of providers charting under the wrong ID

Unlock the power of proximity-based authentication for additional workflows

In addition, with EAM in place, complete with proximity-aware secure walkaway technology, organizations can leverage the infrastructure to enhance workflows across their Imprivata environment, including:

- **Multifactor authentication for remote network access –** The secure walkaway capabilities of EAM leverage Imprivata ID, Imprivata's mobile one-time-password (OTP) token application, which can also be used as second-factor authentication for remote network access, cloud applications, and other workflows, which improves security.
- **Hands Free Authentication for EPCS –** In the same manner that EAM detects a user's mobile device to secure shared workstations with proximity-based awareness, Hands Free Authentication leverages Bluetooth to detect and wirelessly authenticate a user for electronic prescribing for controlled substances (EPCS). EPCS requires two-factor authentication at the time of prescribing, which organizations can greatly simplify by enabling Hands Free Authentication. After the user enters the first factor (either a password or biometric), Hands Free Authentication will automatically complete the second factor without any user interaction, enabling an exceptionally fast, convenient, and DEA-complaint EPCS workflow.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

4018-2026_EAM-DS-secure-walkaway-technology