# Imprivata OneSign with secure walkaway technology

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

### Key benefits

- Improve security by reducing the risk of unauthorised 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

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, organisations 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.

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.

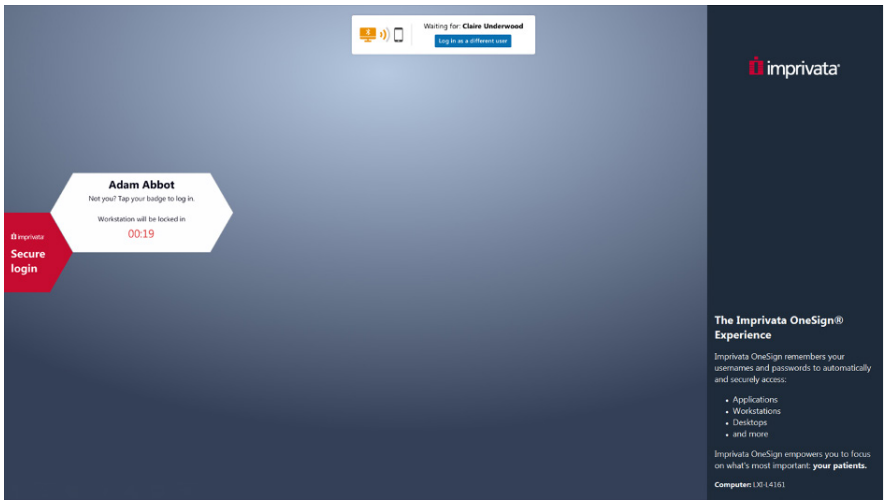
Striking the right balance of security and convenience on shared workstations is critical, but a viable solution has remained elusive.

### Secure walkaway, powered by Bluetooth

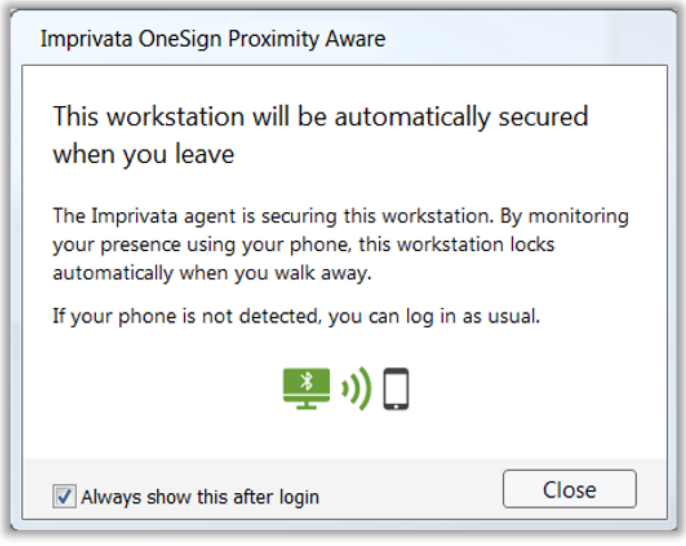
Imprivata OneSign® with secure walkaway technology leverages the power of Bluetooth Low Energy (BLE) and the ubiquity of mobile devices to secure PHI on shared workstations without disrupting clinical workflow or patient care. Locking and unlocking of workstations is based on the presence of the user's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

Imprivata OneSign with secure walkaway technology 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.

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




When the user steps away from the workstation, Imprivata OneSign 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. Organisations can employ shorter timeouts to ensure security, knowing they will only be invoked when a workstation is unattended (and not when a clinician is simply reading something on the screen).

With Imprivata OneSign and secure walkaway technology, organisations can:

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

If Imprivata OneSign detects the presence of the user's mobile device, the workstation will remain unlocked.

## Supported technology

Imprivata OneSign with secure walkaway technology requires a suitable Bluetooth device, currently supported readers include:

| | |
|---|---|
|  | **IMP-80-BLE**<br><br>The HDW-IMP-80 is a dual-frequency proximity card reader with additional Bluetooth Low Energy (BLE) support. The card reader is capable of working with a wide variety of card types. This is a 13.56 MHz contactless, or 125 kHz proximity, card reader. It will read: low and high frequency card types, typical card types including basic HID iClass, ISO 14443A, ISO 15693, Indala, CASI-RUSCO, and HID PROX. The device can support up to four card configurations.* The BLE component supports all Imprivata workflows enhanced by BLE connectivity. |
|  | **IMP-82-BLE**<br><br>The HDW-IMP-82 is a dual-frequency proximity card reader that is capable of working with the widest variety of card types. This is a 13.56 MHz contactless, and 125 kHz proximity card reader with additional Bluetooth Low Energy (BLE) support. It will read: low and high frequency card types, typical card types including HID iClass ID, HID iClass SETM, ISO 14443A, ISO 15693, Indala, CASI-RUSCO, HID PROX and premium HID card types including HID SEOS, HID iClass ID. The device can support up to four card configurations.* The BLE component supports all Imprivata workflows enhanced by BLE connectivity. |

Organisations can employ shorter timeouts to ensure security, knowing they will only be invoked when a workstation is unattended (and not when a clinician is simply reading something on the screen).

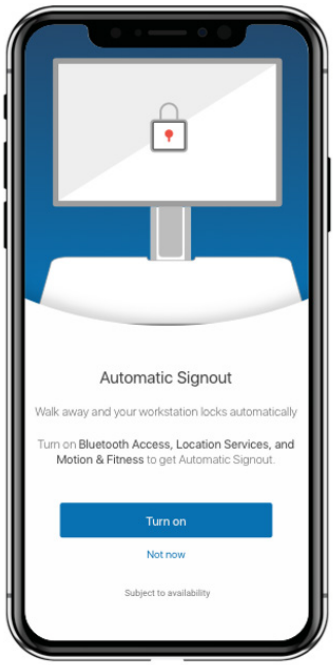
| | |
|---|---|
|  | **HDW-KSI-1700 SX HCB-16**<br>**HDW-KSI-1802R SX HCB-16**<br>These models are all in one keyboard and proximity card readers with additional Bluetooth Low Energy (BLE) support. They have built in 13.56 MHz contactless, or 125 kHz IMP-80 dual-frequency proximity card reader that is capable of working with Mifare card types. The BLE component supports all Imprivata workflows enhanced by BLE connectivity. |
|  | **HDW-IMP-IIUR**<br>The HDW-IMP-IIUR is a Bluetooth Low Energy (BLE) receiver, which supports all Imprivata workflows enhanced by BLE connectivity. |

*Imprivata proximity card readers are supported on all Windows desktops.

## Hardware availability

Hardware is available for sale in the EU, Switzerland, United Kingdom, Australia, New Zealand, and the United States.

Users will need a compatible iOS or Android phone and the Imprivata ID app, available from the Apple AppStore and Google Play store.



## Unlock the power of proximity-based authentication for additional workflows

In addition, with Imprivata OneSign with secure walkaway in place, organisations can leverage the infrastructure to enhance workflows across their Imprivata environment, including:

- Multifactor authentication for remote network access – Imprivata OneSign with secure walkaway technology leverages 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.

### About Imprivata

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 further information please contact us at

+44 (0)208 744 6500
or visit us online at
www.imprivata.co.uk

### Offices in

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