Imprivata Customer Privileged Access Management

Secure and efficient remote access for medical device manufacturers

Increasing cybersecurity regulations and near-constant cyberattack threats demand that medical device manufacturers proactively manage and address cybersecurity risks and vulnerabilities to keep patients safe, ensure device performance, and protect their business. A key component of this is enabling secure, standardized, simplified access to the devices, equipment, and applications they implement and support.

Imprivata Customer Privileged Access Management (formerly SecureLink Customer Connect) provides medical device manufacturers with the streamlined and secure remote access to customer environments they need to maintain device cybersecurity and compliance.

With Imprivata Customer Privileged Access Management (CPAM), medical device vendors on average see a:

65% reduction in time spent managing and supporting remote access

75% reduction in time spent establishing remote connections with customers

70% reduction in security incident related expenses

How Customer Privileged Access Management streamlines and secures your remote access connections

Standardize remote access across all customers into a single platform

- Support native, anytime connectivity via any TCP or UDP-based protocol for any OS

- Connect faster with a single login for reps and improve time-to-resolution

Take advantage of the Imprivata network:
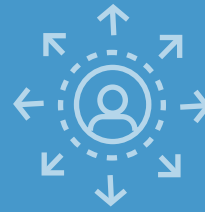
12,000+ healthcare providers, vendors, and device manufacturers using Imprivata for secure remote connectivity

Provide innovative support and meet healthcare customers' security requirements with control and visibility over access

- Contextual audit trails and video recordings provide visibility into user activity and proof of work completed in the case of an incident

- Provide customers with visibility and control over access with audit logs and fine-grained access controls

Meet and demonstrate compliance with HIPAA, PCI, the FD&C Act and others with audited, anytime access

- Access devices to deploy routine or critical patches or updates to address potential security issues and meet quality system regulations (QSRs)

- Limit access to only what's necessary and prevent inappropriate access to protected information, such as PHI

- Track all activity, tied to individual users, to meet documentation requirements

Limit liability and risk to your organization with access based on Zero Trust

- Limit exposure and ability for lateral movement with Zero Trust access and least privileged access policies

- Minimize the risk of compromised credentials, facilitating access without reps needing to know and manage user names and passwords

With cybersecurity regulatory requirements only increasing, customers are demanding higher levels of security, visibility, and control from their vendors' access. With CPAM, you can ensure the security of your medical devices and meet the requirements of your customers to achieve security, standardization, and efficiency – no compromises.

For more information on Imprivata Customer Privileged Access Management, **visit our website.**

![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:

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