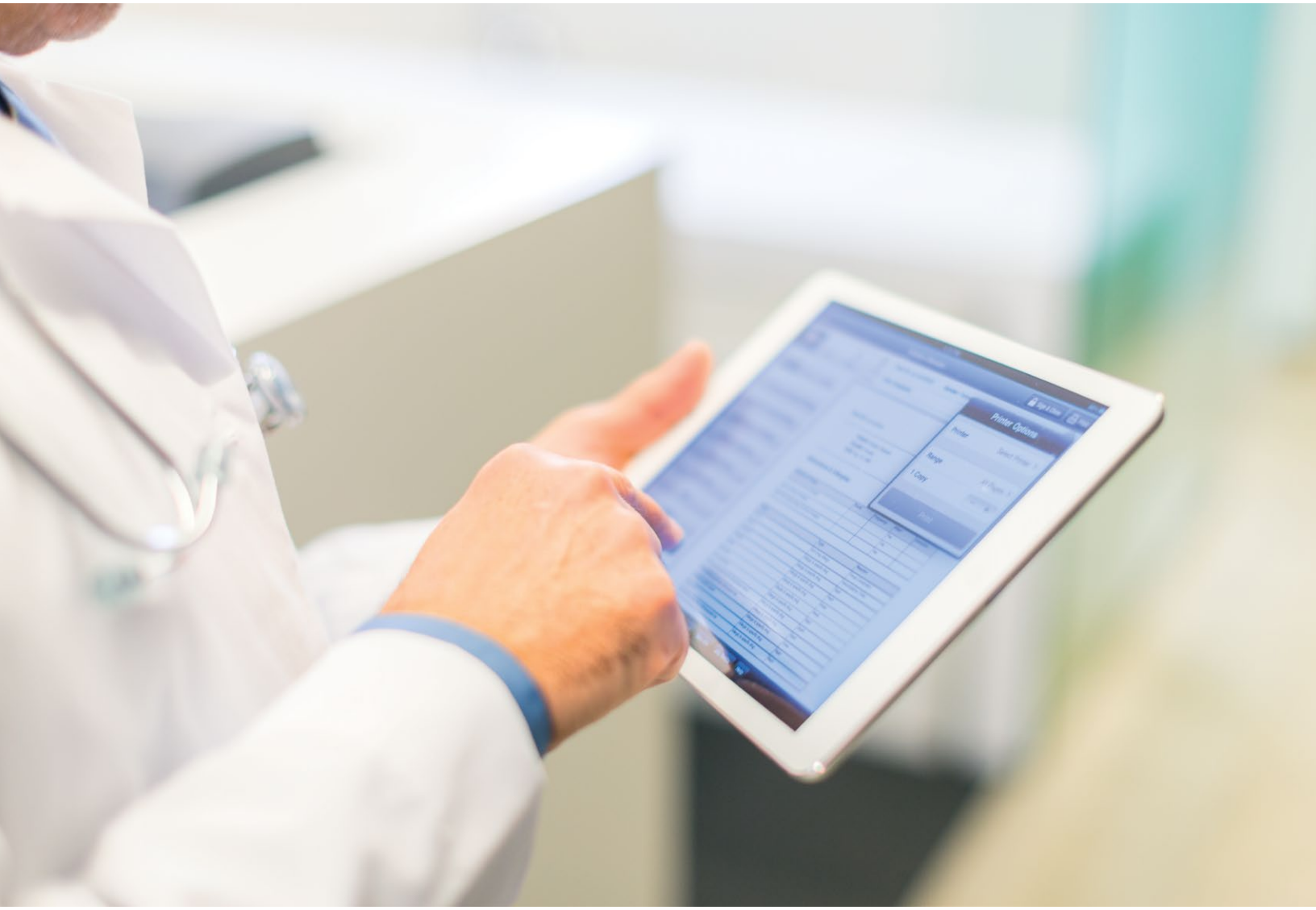


Protecting Medical Information: Two-Factor Authentication in a Healthcare Setting

CITRIX READY

imprivata | CITRIX

Healthcare organizations are under siege. Worldwide, the healthcare industry is facing unprecedented security challenges from phishing and ransomware. According to the U.S. Department of Health and Human Services, more than 110 million patient health records were compromised in 2015. During the brief two-year span of 2014-2015, more than 80 percent of healthcare organizations fell victim to a cyberattack that compromised patient health records.

Officials charged with protecting patient information face unique challenges. IT departments must strike balance between security and ease of use for providers. Implementing security protocols that delay or disrupt workflows in a healthcare environment are likely to result in unacceptable consequences.

Fortunately, security solutions do exist that serve to protect precious patient data while meeting healthcare's critical need for speed, interoperability and usability.

One of the most effective methods for securing login credentials is the deployment of a multifactor authentication system. This paper describes how a Citrix Ready-verified product, Imprivata Confirm ID™, enables a purpose-built authentication system perfectly suited to meet the demands of the healthcare industry. It shows how Imprivata Confirm ID provides healthcare organizations with the opportunity to:

- Make security invisible to end users by replacing passwords with innovative and convenient authentication methods such as hands-free authentication, push-token notification, fingerprint biometrics, and other methodologies designed to both strengthen security and make it easier for users to comply with security protocols
- Strengthen security and enhance compliance by creating a secure, auditable chain of trust wherever, whenever and however users interact with patient records and other sensitive data
- Centralize identity and two-factor authentication across all enterprise and clinical workflows, including remote access, electronic prescribing of controlled substances, medical device access, medication ordering, blood administration and other routine tasks

CITRIX® NetScaler

The paper also discusses the effectiveness of teaming Citrix NetScaler with Imprivata Confirm ID to meet healthcare's growing need for a secure remote access security solution.

Business Challenge Summary

News stories abound about identity theft and the hijacking of personal and corporate financial records from an array of industries. Healthcare organizations are no exception finding themselves in the unenviable position of providing an irresistible draw to hackers and cybercriminals.

Health records offer a wealth of data that enterprising criminals can turn into a bounty of potential income streams, including:

- Social Security numbers that may enable identity theft
- Financial information, including credit card and checking account numbers
- Sensitive personal data that may provide opportunities for insurance fraud

From the criminal's perspective, the theft of a healthcare record is a gift that keeps on giving.

In recent years, the healthcare industry has undergone a massive transformation from a mostly paper-based records paradigm to a computerized electronic records system. The result is an unprecedented onslaught of cybercriminal activity targeting healthcare organizations.

Healthcare organizations have attempted to counter the escalating threat. But as organizations have scaled their efforts at self-defense, criminals have responded by mounting ever more technologically sophisticated offensives such as ransomware and phishing. According to an HIMSS Cybersecurity Survey, phishing is widely considered the single greatest security threat facing the healthcare industry, but only a third of healthcare organizations feel capable of mounting an effective defense.

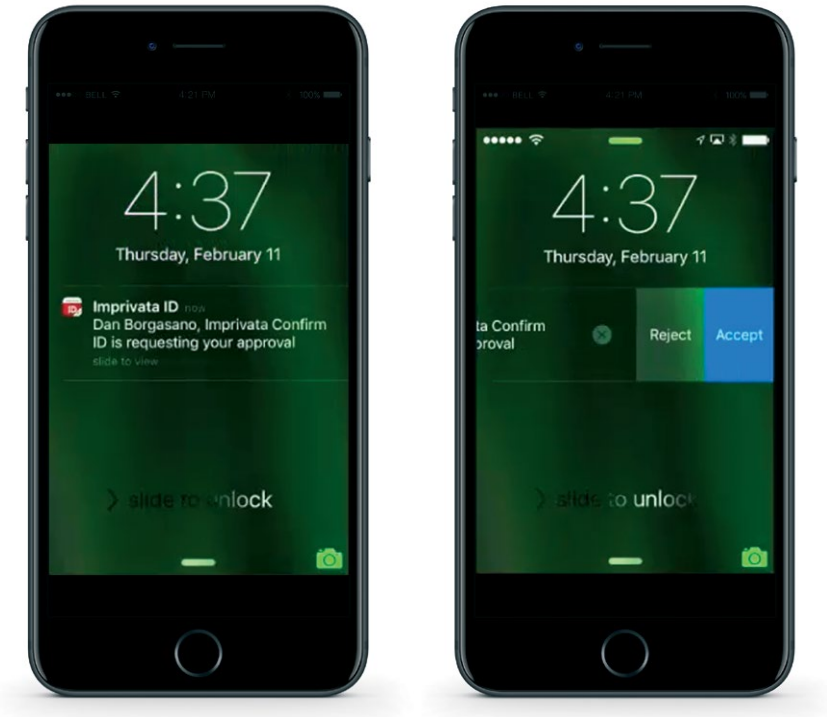
Unwittingly, the employees of healthcare organizations have become a lucrative resource for cybercriminals. Successful phishing attacks rely heavily upon obtaining login credentials from unsuspecting employees as they go about their jobs. Though no employees willingly give away login credentials, cybercriminals have become highly adept at disguising illegitimate requests for sensitive information. The methodologies employed by cybercriminals have become so sophisticated that even the most cautious of employees are unlikely to become suspicious of an attempt to hijack login credentials. And entire systems can become compromised through a single employee's failure to recognize and refuse an illegitimate request for login credentials.

Top Features to Consider in a Multifactor Authentication Solution for Health Care

The need for effective two-factor authentication among healthcare organizations has never been more urgent. But maximizing the potential of a two-factor authentication methodology requires the installation of a system that delivers a full range of key capability and usability features.

The following, in particular, should be considered must-have features for two-factor solutions undergoing evaluation for deployment in a healthcare setting:

1. **Flexible Authentication Options:** Capable of augmenting or replacing passwords with a range of innovative, convenient authentication methods, including fingerprint biometrics, Hands Free Authentication (exclusive to Imprivata) and push token notification. Flexible authentication options help make security protocols transparent to end users, and offer the flexibility necessary for customizing security to methodologies that best mesh with users' preferences and established workflow processes.



2. **Single-Platform Authentication:** Provides a single platform to manage authentication credentials, and through a single server. Deployment from a single, centralized authentication management platform enables greater, more precise control over users' interactions with patient records and other sensitive information. Improves security, usability and compliance auditing.

3. **Extensibility to All Workflows:** Adding a layer of security during the authentication process holds the potential of negatively impacting the user experience. The best two-factor solutions, however, are extensible to all workflows. For example, single push-notification through a cellular phone can result in a user experience that is equal or even superior to simple password-protected systems.

4. **Easy Administration:** The potential benefits of a two-factor solution can be largely negated if the solution is not easy to manage and administer. Solutions that offer easy administration lessen the demands upon IT department resources, helping to reduce the likelihood of security breaches that may result from errors committed by an overburdened IT staff.

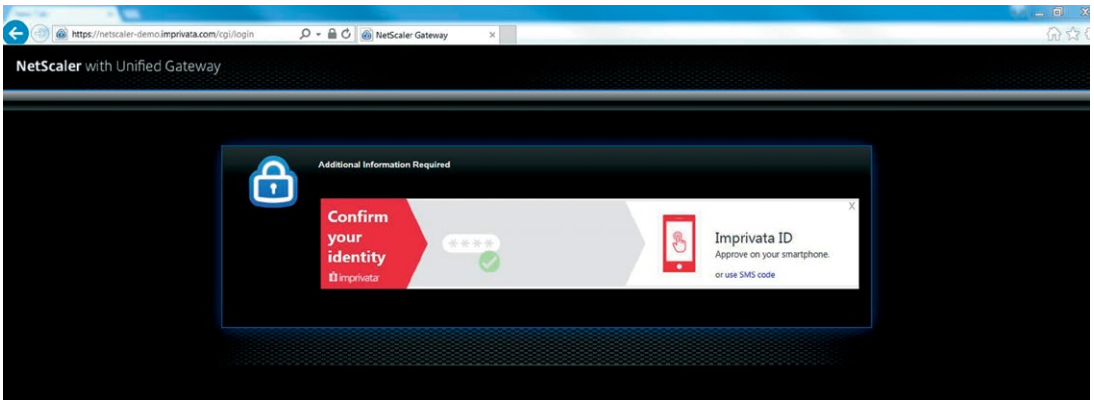
5. **Compatibility with Popular Security Systems:** A two-factor solution should be easily integrated with the leading security systems commonly deployed by healthcare organizations.

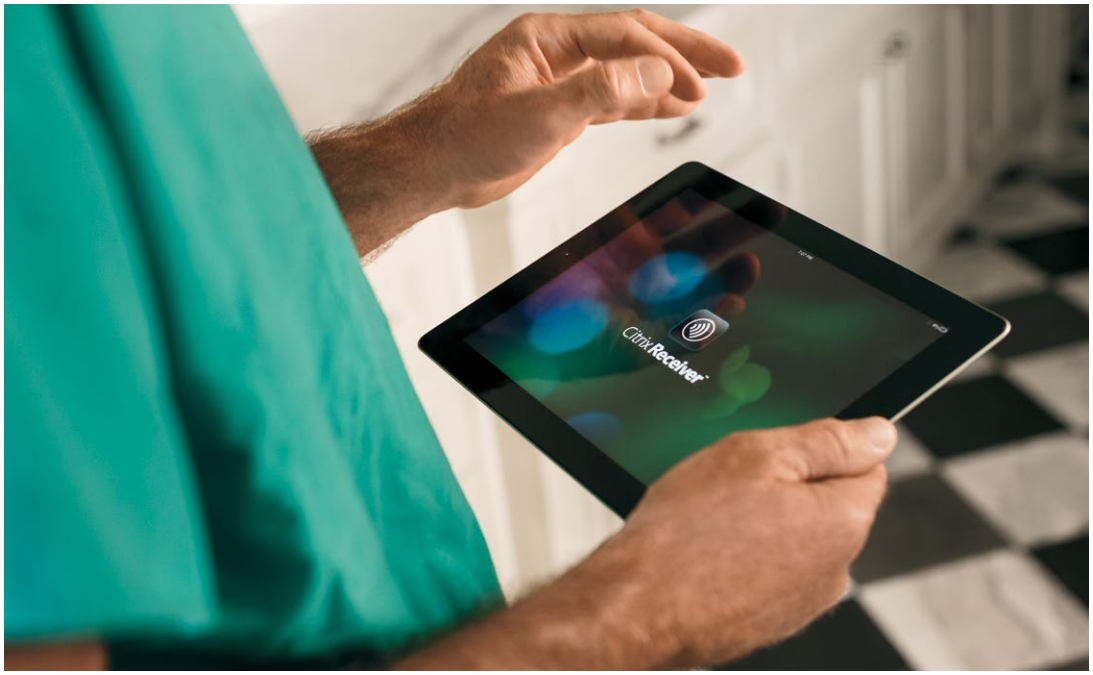
6. **Compliance with the Highest Standards:** The healthcare industry has unique compliance needs. For example, the DEA has special standards that providers must follow when prescribing controlled substances electronically. A two-factor authentication solution must be able to meet or exceed these complex requirements.

CITRIX® XenDesktop

Citrix Ready Secure Remote Access Program Overview

Citrix's solutions deliver across five security pillars with a complete portfolio of products supporting Secure Access of Apps and data anytime, at any place, on any device and on any network. This includes XenApp and XenDesktop to manage apps and desktops centrally inside the data center, XenMobile to secure mobile applications and devices while providing a great user experience, ShareFile to provide controlled and audited data access, storage and sharing, both on-premise and in the cloud, and NetScaler to contextualize and control connectivity with end-to-end system and user visibility.





Citrix solutions integrate with third-party security products to provide advanced levels of system management and identity, endpoint and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to smoothly integrate with Citrix products, and that work to enhance Secure Remote Access by adding extra layers of Security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, distributed denials of service (DDoS) and other security attacks that may be perpetuated via Remote Access.

Citrix advises that healthcare organizations can best defend against security attacks that might occur through Remote Access by following five best practices — pillars of focus that support enterprise security:

1. **Identity and Access:** Properly identify users requesting access to a system, and limit the degree of access granted. In comparison to simple password-based systems, two-factor authentication offers a vast improvement in the ability to properly identify requests for access. And the degree of access granted to each individual user should be context based. Enacting the principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs.

2. **Network Security:** The growing demand for remote access complicates the process of securing a network. And yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multi-layer approach helps to boost network security while ensuring availability.

3. **Application Security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created an additional point of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams to protect web-based apps can also help to reduce app-related security vulnerabilities.

4. **Data Security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data, by enforcing secure file sharing (to reduce data loss), and by the containerization of data (both in-transit and at rest). Data security might be considered more important for the healthcare industry than for any other business discipline. The typical patient record contains a rich resource of criminally actionable data: Social Security numbers, bank account and credit card numbers, home addresses, driver's license numbers, and much more are likely to be contained in most patient records.

5. **Monitoring and Response:** Vigilance and fast action are required to successfully counter the attacks that most healthcare enterprises face on a daily basis. A rapid response to breaches is also critically important, given that even the most secure systems are not completely invulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and help to limit susceptibility to imminent additional attacks. End-to-end visibility into application traffic supports faster identification of security breaches and system anomalies.

The Benefits and Burdens of Remote Access

Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word "workplace" must be redefined to be less location-specific and more worker-specific. The adoption of mobility enhancing tools such as tablets, smartphones and other mobile devices has transformed many enterprise roles into an anyplace, anytime proposition. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps of productivity that remote access enables.

But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of Virtual Public Networks (VPN) over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justifies the need for an increased focus upon security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above, while meeting the skyrocketing demand for more remote access capabilities.

Imprivata has been selected to participate in the Citrix Ready Secure Remote Access program. Imprivata's products have demonstrated the ability to consistently conform with, and support, the five security pillars of the Remote Access program. Key features of Imprivata's security products include:

- **Ease of Use:** Imprivata's security solutions provide the rare benefit of augmenting security with a fast, consistent authentication workflow for end users. This unique benefit enhances the flexibility that is so crucial in assuring that security methodologies are adaptable to user workflows and personal preferences. Many security solutions focus solely on security, sacrificing the flexibility that enhances the user experience and that promotes productivity. Imprivata provides security solutions that provide the ultimate in security while also enhancing usability and flexibility. Its different authentication options enable ease of use depending on a user's preferences.

- **Two-Factor Authorization:** The ability to identify and authorize users based upon multiple factors (rather than just a single password) supports the 'Identify and Access' security pillar. Imprivata's two-factor authentication methodology is designed specifically to enhance security for both on-premise and remote logins, bolstering the ability of healthcare organizations to protect patient data without stifling staff productivity.

- **Secure VPN Access:** The use of Virtual Public Networks is rapidly growing. The benefits of VPN, such as privacy protection and enhanced connectivity options, assure that the use of VPNs will continue to grow. But VPNs are often accessed over insecure or even public networks. Imprivata's security solutions ensure that security is maintained even when network connections to VPNs fall short of providing optimum security protocols.

Overview of Imprivata

Imprivata is truly a market leader in providing IT security solutions for healthcare enterprises. Imprivata currently serves over 1,000 healthcare organizations in 20 countries worldwide, with licensed users in excess of 2 million. Recognized as an industry leader by organizations such as Gartner, KLAS Research, and the American Hospital Association, Imprivata has earned an impressive array of honors, recently including:

- The Healthcare Informatics Leading Edge Award for clinical workflow improvement
- The FierceMarkets 2015 Fierce Innovation Awards: Healthcare Edition in the Revenue Cycle Management category
- Selection as the Best Healthcare IT Company – UK in CV Magazine's Technology Innovator Awards for Cybersecurity – UK
- Best of VMWorld Europe User Awards 2015
- Summit 2015 Customer Experience Program of the Year

Imprivata provides healthcare organizations with an industry-leading platform that addresses critical compliance and security challenges while improving provider productivity and the patient experience. Imprivata's focus is upon balancing the security needs of healthcare enterprises with provider productivity, with the ultimate goal of consistently improving patient care and the security of patient data.

Simply stated, Imprivata enables healthcare providers to ACT: Access, Communicate and Transact patient health information securely and conveniently.

Imprivata's unique offerings include:

- **Multifactor Authentication (Imprivata Confirm ID™):** Imprivata Confirm ID is a single, centralized solution that enables remote and on-premise users to transact with patient health information securely and conveniently. Imprivata Confirm ID is a multifactor authentication platform that combines security with user convenience by offering a broad range of multifactor authentication methods, including Hands Free Authentication, push-token notification and fingerprint biometrics.

  Available on and off-premise, Imprivata Confirm ID meets HIPAA and EPCS regulations. Imprivata Confirm ID enables healthcare providers to meet DEA requirements for prescribing controlled substances electronically, and supports healthcare providers' efforts to meet all government-mandated and ethical industry requirements.

- **Single Sign-On (Imprivata OneSign®):** Imprivata OneSign allows fast, secure access to clinical and administrative systems by eliminating the need to memorize and repeatedly type multiple user IDs and passwords. Imprivata OneSign provides desktop access into workstations, connects to Virtual Desktop Infrastructure, and enables virtual desktop roaming.

  In use in healthcare environments around the world, Imprivata OneSign has been shown to save care providers up to 45 minutes per shift. User satisfaction levels are improved, clinical workflows are optimized, and patient care delivery is enhanced. Imprivata OneSign also helps to simplify HIPAA and HITECH compliance without diminishing the productivity of care providers or IT staff.

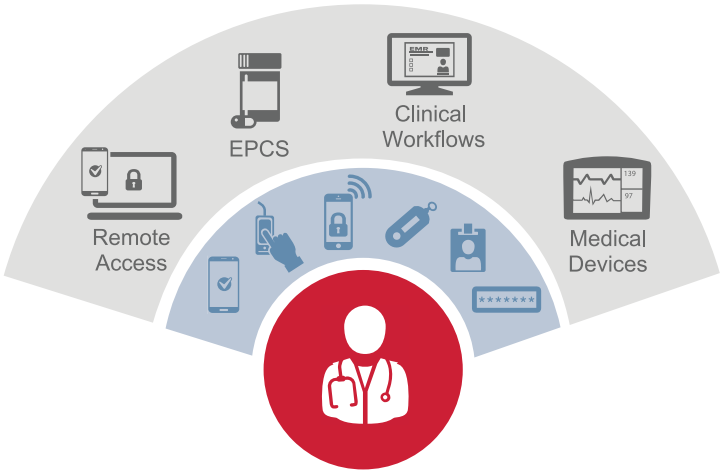
  Imprivata OneSign is easily integrated with Citrix environments, and securely simplifies the authentication and login process for accessing Citrix products such as XenDesktop and XenApp.

Partner Solution Detail

Imprivata Confirm ID offers a broad array of authentication options designed to provide comprehensive security support for a range of healthcare workflow requirements, including:

- Remote access
- EPCS support
- Medical device integration
- Clinical workflow support

Imprivata Confirm ID for Remote Access improves security by enabling two-factor authentication for remote access via a VPN. Remote two-factor authentication protects against the successful use of stolen credentials — often pilfered through phishing and other cyberattacks — to breach the network and gain access to sensitive patient and administrative information.



Imprivata Confirm ID fills a need for the many healthcare organizations that seek to implement two-factor authentication for staff, affiliates, contractors, and any personnel that are granted access to the system. Imprivata Confirm ID is an agile solution that can be administered quickly through features such as self-enrollment. Usability is enhanced through innovative features such as push-token notification. Users simply download the app to their phone, and during login can swipe the notification to confirm second-step authentication without even unlocking their phone.

Imprivata Confirm ID eliminates the need for multiple authentication solutions, giving healthcare organizations a single, robust platform for enterprise-wide identity and authentication management. The single platform system is appealing to users and efficient for administrators. Ultimately, Imprivata Confirm ID improves efficiency and satisfaction for users, while streamlining authentication management and security policy enforcement for IT.

A Proven Partnership for Healthcare Enterprises

Ninety percent of the largest healthcare providers — including 100 percent of the U.S. News and World Report top hospitals — rely upon Citrix products to help maximize IT efficiencies and security. Citrix NetScaler is a prime example; many organizations deploy NetScaler as part of a broad, enterprise multifactor authentication platform.

Imprivata Confirm ID integrates seamlessly and easily with Citrix NetScaler, an industry-leading Application Delivery Controller, providing a multifactor authentication platform purpose-built for healthcare. The certification of Imprivata Confirm ID a by the Citrix Ready Secure Remote Access program provides healthcare enterprises with a proven, reliable, remote access security solution for facing the ever-escalating security needs of the modern healthcare environment.

For more information about Imprivata Confirm ID, please visit:
https://www.imprivata.com/two-factor-authentication

For more information about Imprivata OneSign, please visit:
https://www.imprivata.com/enterprise-sso

For more information about Citrix NetScaler, please visit:
https://www.citrix.com/products/netscaler-adc/

Appendix

Learn more about choosing the right two-factor authentication solution for your healthcare organization by downloading this white paper:
https://www.imprivata.com/resources/whitepapers/choosing-right-two-factor-authentication-solution-healthcare

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at:
https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

Get tips for avoiding phishing attacks by downloading this white paper:
https://www.imprivata.com/resources/whitepapers/avoid-becoming-catch-day-four-steps-combat-phishing-attacks

To learn more about security solutions for the healthcare industry, contact Citrix and Imprivata.

About Citrix Ready
Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About Imprivata
Imprivata, the healthcare IT security company, enables healthcare globally to access, communicate, and transact patient information, securely and conveniently. The Imprivata platform addresses critical compliance and security challenges while improving productivity and the patient experience. For more information, visit www.imprivata.com.