

Choosing the right two-factor authentication solution for healthcare

The healthcare industry's transition from paper to electronic records has introduced significant security risk from hackers around the globe, and care providers find themselves in the midst of a cybersecurity war to protect patient health information.

In 2015, more than 80 percent of healthcare organizations reported they had been compromised by a cyberattack in the previous two years, and only half believe they are adequately prepared for future attacks¹. The U.S. Department of Health and Human Services documented that hackers accessed more than 110 million patient health records in 56 major cybersecurity attacks in 2015 alone².

Many of these successful breaches use social engineering techniques to obtain access to networks, applications, and information. Phishing and similar attacks, for example, leverage cleverly disguised requests for login credentials to dupe unsuspecting employees into entering their usernames and passwords, and have emerged as the top security threat facing healthcare organizations³.

To address these threats, organizations continue to adopt two-factor authentication as a best practice for secure access, requiring users to submit a combination of two of the following to authenticate:



Two-factor authentication can significantly improve security, and according to the Annual Report to Congress on the Federal Information Security Management Act, up to 65 percent of cybersecurity incidents could have been prevented with strong, two-factor authentication⁴.

1. 2015 KPMG Healthcare Cybersecurity Survey, August 26, 2015, <http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf>

2. 2015 KPMG Healthcare Cybersecurity Survey, August 26, 2015, <http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf>

3. 2015 HIMSS Cybersecurity Survey, June 30, 2015, <http://www.himss.org/2015-cybersecurity-survey>

4. Annual Report to Congress: Federal Information Security Management Act, February 27, 2015, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf

Healthcare needs a two-factor authentication platform that extends to all workflows

Since 2010, the number of U.S. hospitals using two-factor authentication has increased by 53⁵ percent to address threats from outside the firewall as well as to secure high-value clinical workflows inside the hospital. Healthcare delivery organizations across the country are faced with meeting DEA requirements for two-factor authentication for electronic prescribing of controlled substances (EPCS), and there are a number of other clinical workflows where additional authentication is critical to ensuring quality of care. For example, within EpicCare alone, there are more than 40 clinical workflows that may require users to authenticate. These include witnessing medication wasting, blood administration, anesthesia attestation, and others.

Adding these layers of security has the potential to create inefficiencies, so there are a number of factors healthcare organizations must consider when selecting an authentication platform to ensure they do not frustrate users, impede workflow, or create barriers to patient care. These considerations include:

- Extensibility to meet all present and future authentication needs, inside and outside the hospital
- Security balanced with convenience to enable—not impede—patient care through:
 - Embedded authentication workflows that tightly integrate with your EHR and other applications, medical devices, remote access gateways, virtual desktop platforms, and other systems.
 - Flexible, comprehensive portfolio of authentication methods
- Compliance with the highest standards regulating care, such as the DEA requirements for EPCS
- A platform built specifically for healthcare and its unique workflow needs

Imprivata is proud to be the healthcare IT security leader, with more than 1,500 customers and 4 million clinicians using our technology to provide the security that healthcare requires with the convenience that providers need to deliver high-quality care. We have built our solutions from the ground up to meet the unique security and efficiency requirements for healthcare workflows.

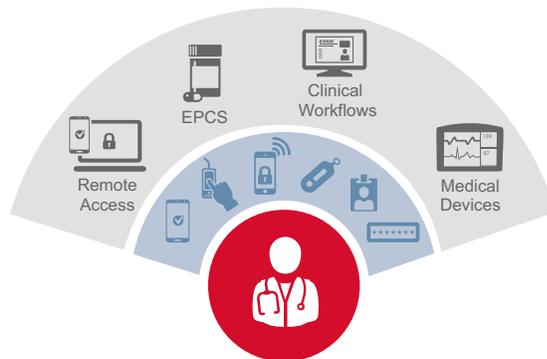
65 percent of cybersecurity incidents could have been prevented with strong authentication

5. ONC Data Brief: State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals, November 2015, https://www.healthit.gov/sites/default/files/briefs/oncdatabrief32_two-factor_authent_trends.pdf.

Imprivata Confirm ID offers the widest range of authentication modalities and workflows for healthcare

Imprivata Confirm ID™ - The comprehensive, enterprise-wide two factor authentication platform

Imprivata Confirm ID is purpose-built to meet healthcare’s unique requirements for solutions that balance security with convenience. Through an unrivaled ecosystem of EHR integrations and the broadest range of innovative, convenient, and DEA-compliant authentication options, Imprivata Confirm ID gives healthcare organizations a complete solution for improving enterprise-wide security without impacting workflow efficiency—both on premise and outside the hospital. This eliminates the need for multiple authentication methods from different vendors, increases efficiency for users, improves security and compliance, and reduces total cost of IT ownership.



Seamless workflow integration

Imprivata Confirm ID offers the most comprehensive ecosystem of direct, productized API-level integrations with leading VPNs and remote access gateways, EHRs and other clinical applications, desktop virtualization platforms, and medical devices. This makes it easy and convenient for users to authenticate within existing workflows and eliminates the need for different authentication solutions for different applications. Instead, users have an easy, fast, and consistent authentication experience across all workflows.

Fastest, convenient authentication methods

Imprivata Confirm ID offers the broadest range of innovative and convenient authentication options to meet the requirements of all healthcare workflows and individual user preferences. The fast-paced and increasingly mobile nature of care delivery necessitates convenient and flexible two-factor authentication options that can be used inside and outside of the hospital. Imprivata Confirm ID gives users the ability to leverage the methods that best meet their workflow needs. Users are only prompted for the authentication methods that are available and allowed, which further streamlines authentication and improves efficiency.

DEA-compliant two-factor authentication methods

Imprivata Confirm ID offers a wide array of DEA-compliant authentication options to help organizations meet the two-factor authentication requirements for EPCS. While most security vendors offer standard one-time password (OTP) tokens to satisfy DEA compliance, Imprivata understands the need to make physician workflows fast, seamless, and convenient. Imprivata Confirm ID offers Hands Free Authentication, push token notification, and fingerprint biometrics to overcome the challenges of manual OTP tokens, improve EPCS efficiency, and drive adoption.

The following table provides an overview of the unmatched breadth of innovative, convenient, and DEA-compliant authentication options offered by Imprivata Confirm ID:

Something you are	Something you have						Something you know		
Fingerprint Biometrics	Hands Free Auth	Push Notification	SMS	Soft Token	Hard Token	Proximity Badge	Password	PIN	Q&A
 DEA Compliant	 DEA Compliant	 DEA Compliant		 DEA Compliant	 DEA Compliant		 DEA Compliant		

As a trusted, strategic IT security partner, Imprivata can help you evaluate your requirements for two-factor authentication

Selecting the best two-factor authentication platform for your organization

As a trusted, strategic IT security partner, Imprivata can help you evaluate your requirements for two-factor authentication, including which authentication methods are best-suited to meet your various workflow requirements. Below is a summary checklist to help you evaluate the best solution for your healthcare enterprise needs.

		Traditional token vendors
Seamless workflow integration		
VPN integrations	✓	✓
Embedded EMR integrations	✓	
Virtual desktop infrastructure integration	✓	
Medical Device integrations	✓	
Fast, Convenient Authentication methods		
Fingerprint biometrics	✓	
Hands Free Authentication	✓	
DEA-compliant push notification	✓	
Extensible platform for healthcare		
Centralized authentication management	✓	
Holistic policy enforcement	✓	
SSO integration	✓	



About Imprivata

Imprivata® (NYSE: IMPR), the healthcare IT security company, provides healthcare organizations globally with a security and identity platform that delivers authentication management, fast access to patient information, secure communications, and positive patient identification. Imprivata enables care providers to securely and efficiently access, communicate, and transact patient health information to address critical compliance and security challenges while improving productivity and the patient experience.

For further information please contact us at:

1 781 674 2700

or visit us online at
www.imprivata.com

Offices in:

Lexington, MA USA
San Francisco, CA USA
Santa Cruz, CA USA
Tampa, FL USA
Uxbridge, UK
Melbourne, Australia
Paris, France
Nuremberg, Germany
Den Haag, Netherlands