medisked

7 REASONS

Health & Human Services Provider Software Should Have Multi-Factor Authentication

WHITE PAPER

Contents

Introduction

In the health and human services industry, where the confidentiality, integrity, and availability of individuals' data are of paramount importance, Multi-Factor Authentication (MFA) offers significant value in safeguarding sensitive information and ensuring data privacy. With the increasing threats of cyber-attacks, insider threats, and regulatory requirements, implementing MFA has become essential in maintaining robust security measures.

What does MFA entail?

MFA is a security mechanism used to protect user accounts by requiring multiple forms of verification before granting access and is composed of the following three types of authenticators:

1. Something you know.

This type of MFA involves verifying the user's identity based on something they know, such as a password, PIN, or security question. It typically requires the user to provide additional information beyond their username and password to prove their identity.

2. Something you have.

This type of MFA involves verifying the user's identity based on something they possess, such as a physical token or a mobile device. The user may be required to provide a code generated by a token, a fingerprint or face scan on a mobile device, or use a smart card to authenticate.

3. Something you are.

This type of MFA involves verifying the user's identity based on something inherent to them, such as a fingerprint, iris scan, or voice recognition. This type of MFA typically requires specialized hardware or software to capture and analyze the inherent characteristic for authentication.

However, true MFA must entail at least two different types (e.g., a password and a code from your authenticator application). Having two instances of the same type (like entering two different passwords) does not constitute MFA.

Why do we need it?

1. MFA provides an additional layer of protection for patient data.

Healthcare organizations store vast amounts of personal and medical information in electronic health records (EHRs) and other digital systems. This data is highly valuable to cybercriminals, who can use it for various malicious purposes. By requiring multiple authentication factors, such as a password and a fingerprint or a smart card, MFA reduces the risk of unauthorized access to patient records, protecting patient privacy and preventing data breaches.

2. MFA helps prevent unauthorized access to Electronic Health Records (EHRs) and other critical systems.

Unauthorized access to EHRs can lead to tampering with patient records, altering medication orders, or stealing sensitive information. MFA ensures that only authorized personnel with the correct credentials can access these systems, reducing the risk of unauthorized access and potential tampering. This helps maintain the integrity and accuracy of patient records and ensures that only legitimate users can access and modify patient data breaches.

3. MFA mitigates the risk of insider threats, which can pose a significant security risk in the healthcare industry.

Insider threats refer to unauthorized actions taken by employees, contractors, or partners who have access to sensitive information. These individuals may intentionally or unintentionally misuse their access, leading to data breaches or other security incidents. MFA can help detect and prevent insider threats by requiring additional authentication factors, making it more difficult for malicious insiders to exploit their access and reducing the risk of insider-related security incidents.

4. MFA enhances the overall security posture of healthcare organizations.

Cyber-attacks, such as phishing, ransomware, and malware attacks, are prevalent in the healthcare industry. These attacks often exploit vulnerabilities in passwords, such as weak or stolen passwords, to gain unauthorized access. MFA adds an extra layer of protection, making it much more challenging for cybercriminals to bypass authentication and gain access to healthcare systems. Even if an attacker manages to steal a password, they would still need to provide additional authentication factors, such as a fingerprint or a smart card, to gain entry, significantly reducing the risk of successful cyber-attacks.

5. MFA supports compliance with regulatory requirements.

The healthcare industry is subject to strict regulations, such as HIPAA in the United States, which mandate the protection of patient data. Many regulatory frameworks require the use of multi-factor authentication as part of the security measures to protect sensitive information. Implementing MFA helps healthcare organizations meet regulatory requirements, ensuring compliance and avoiding potential penalties for non-compliance.

6. MFA promotes user awareness and behavior.

Passwords are often the weakest link in security, as users tend to choose weak passwords or reuse them across multiple accounts. MFA encourages users to choose stronger passwords and adopt better password management practices, as they know that their passwords alone are not sufficient to gain access. This helps improve overall user awareness and behavior towards security, reducing the risk of password-related security incidents.

7. MFA offers flexibility in authentication methods.

MFA allows healthcare organizations to choose from a variety of authentication factors, such as passwords, smart cards, fingerprint scans, retina scans, voice recognition, or mobile devices, depending on their specific needs and requirements. This flexibility allows organizations to implement a multi-factor authentication solution that best fits their unique environment, making it more convenient for users while maintaining robust security measures.

MFA in MediSked Connect

This statement probably elicits some mixed feelings: **Multi-Factor Authentication (MFA) is coming to MediSked Connect.** On the one hand, it means an extra layer of security – which is good. On the other, it's just one more layer between a care provider and their system of documentation – which is not so good. The folks at MediSked Connect understand this, so we want to assure all our current users and future users that we don't take this change lightly.

The increase in cybercrime is inescapable in the news. It is important that we offer our clients a state-of-the-art solution to reduce the risk that cybercriminals can access the data of the individuals they serve. While it absolutely will be a change requiring one additional step to login to MediSked Connect, our solution offers multiple methods of authentication to allow **each user** to choose the best method for them:

- For folks that always have their phone with them – try the Auth0 Guardian Authenticator app. It sends a notification and all it takes is to click "accept" and you're done!
- Already have a Google or Microsoft authenticator on your phone? Those will work too by keying in the 6-digit code.
- Don't want to bother hunting for that code? Have the system call and let you listen to the numbers to type in.
- Always, always have your keychain with you? Consider an investment in a security key – a device that fits on your key ring and with a button click, will verify you and get you logged in right away.

We know that one more step to get logged in to MediSked Connect is inconvenient. We also know that **caring for the individuals you support includes keeping their data as safe as possible.**

Want to get started using MFA right away? If you are a current MediSked Connect client, contact Support. If you're a provider agency in the home and community-based services (HCBS) industry who's looking for the leading all-in-one software solution, get your free demo at medisked.com!

About the Authors

Shayne Champion is the Chief Information Security Officer (CISO) at MediSked by CaseWorthy. With almost 30 years in Information Technology (IT) and Cyber Security industries, Shayne has experience spanning a wide range of technical domains. He has built, worked in, lead, and/or managed a wide variety of IT organizations prior to joining MediSked in 2020.

Heather Barr is a Sr. Project Manager and has been with MediSked by CaseWorthy for over three years. Before joining MediSked, she spent 20 years in the healthcare industry divided evenly between payer and provider organizations. She has a Master of Health Administration from the University of Pittsburgh Graduate School of Public Health.

medisked

MediSked is the leading brand in holistic solutions that improves lives, drives efficiencies, and generates innovations for health and human service organizations that support our community. MediSked solutions combine to provide innovative, person-centered technology that improves outcomes and quality, while reducing costs for individuals receiving home and community-based services and long-term services and supports through government & oversight, care coordination/payer and provider agencies. MediSked has supported clients across the United States since 2003.

Want to learn more? Check out medisked.com!