

Transforming Identity Security in the Passwordless Future Using Passkeys for Healthcare

Mahendra Krishnapatnam

Cybersecurity Professional, Leading Consulting Organization, Chicago, Illinois, United States

Abstract

The healthcare sector faces increasing cybersecurity threats, particularly those targeting identity and access management (IAM) systems reliant on traditional passwords. Passkeys, built on FIDO2 and WebAuthn standards, offer a passwordless authentication solution that enhances security, mitigates phishing and credential-based attacks, and improves user experience. This paper explores the technical implementation of passkeys in healthcare environments, emphasizing their role in securing electronic health records (EHRs), patient portals, and medical devices. We analyze their cryptographic architecture, device-bound authentication mechanisms, and interoperability across healthcare systems, ensuring compliance with HIPAA and other regulatory requirements. Additionally, we address deployment challenges, including identity recovery, multi-device synchronization, and integration with existing IAM frameworks. By transitioning to passkey-based authentication, healthcare organizations can establish a more resilient, efficient, and patient-friendly security model, significantly reducing authentication risks while maintaining seamless access for clinicians, staff, and patients.

