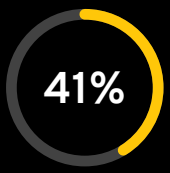
KEEPER
Cybersecurity Starts Here

DATASHEET

Healthcare Industry Brief

Medical Records are Under Attack



of all cyberattacks and data breaches occur in Healthcare[1]

Per capita cost per Healthcare Data Breach[2]

Providers say negligent or careless employees worry them the most[3]

Security

Passwords are often the only thing protecting medical records, but employees use weak passwords, reuse them across accounts and forget them. 81% of breaches start with weak or stolen passwords and poor password management practices.[4] Employee password habits can only be improved with insight into password usage and compliance. Keeper solves this by providing comprehensive reporting, auditing and notifications through the Admin Console.

Productivity

Save employees time, frustration and eliminate the need for them to reuse and remember passwords. The Keeper vault, with a responsive and intuitive UI, is available to employees from any device and location. Everything Keeper does is geared toward quick user adoption and security. Drastically reduce help desk costs because up to 50% of calls are password related.[5]

Two-Factor Authentication

Keeper supports Two-Factor Authentication (2FA) including SMS, Keeper DNA® (smartwatch tap), TOTP (e.g. Google Authenticator and Authy), FIDO U2F (e.g. Yubikey), Duo and RSA SecurID. 2FA may be enforced through role-based controls.

Email Auto-Provisioning

Provision Keeper vaults to thousands of users with a domain match on email addresses. With minimum administration, large-scale deployment can be accomplished using an existing email channel or portal.

HIPAA Compliance

164.308(a)(5) requires “Procedures for creating, changing, and safeguarding passwords” 164.312(a)(1) requires unique user identification, emergency access, and automatic log off. 164.312(b) is about audit controls, including to activity logs.

Every employee is provided a secure digital vault. Keeper will generate strong, random passwords and automatically fill them for users. Keeper enables role-based access controls to enforce least-privilege policies. Folders and records can be securely shared and revoked. The vault of an employee that leaves can be automatically locked and be securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

Keeper’s zero-knowledge architecture ensures that only the end-users have access to the Keeper Vault. Because Keeper security never has access to the data, a business associate agreement (BAA) is not required for HIPAA compliance.

> **“Enterprise Password Management Solutions can Help Manage Password Costs and Realize Compelling ROI.”**
>
> - Forrester[6]

Thousands of Organizations Trust Keeper

SIEMENS
PHILIPS Healthcare
CORNERSTONE HEALTH CARE
RWJBH

Zero-Knowledge Architecture

All encryption and decryption is done on the user's device. PBKDF2 with 100,000 rounds is used for deriving a key from the user's master password. Each record is encrypted using AES-256 with a different and unique key that is randomly generated client-side. RSA encryption is used for secure record sharing between users and teams. Keeper's infrastructure sync's encrypted ciphertext between devices. Key pinning is enforced between client and server. All data in transit and at rest is always encrypted - it cannot be viewed by Keeper Security employees or any outside party.

Microsoft Active Directory Synchronization

Keeper® AD Bridge synchronizes to MicrosoftActive Directory or Open LDAP. This enables rapid user provisioning and automatically adds Nodes (organizational units), Users, Roles and Teams. Keeper enables role-based access control and the ability to track roles as people move throughout the organization. This includes automatically locking vaults of employees that leave.

Azure AD Sync (SCIM) & Provisioning API

Keeper supports the ability to seamlessly provision users and teams from Microsoft Azure AD or other identity platforms using the SCIM protocol. Keeper also supports API-based, command-line provisioning through the use of Keeper® Commander SDK. The Keeper Commander SDK is open source Python code that is available for download from Keeper's Github Repository.

Keeper Integrates with Leading SSO Solutions

Keeper® SSO Connect integrates into your IdP and is the perfect solution for applications that don't support SAML protocols. Keeper also provides users with privileged access, a secure vault to store all of their non-SSO passwords, digital certificates, encryption keys and API access keys.

ADFS · Microsoft Azure · okta · G Suite · JumpCloud · amazon web services · CAS · IBM Security · Ping Identity · onelogin · Centrify · f5

Keeper Third-Party Attestations and Certifications

GSA Schedule 70 Contract 47QTCA18D00C9 · TRUSTe Certified Privacy · AICPA SOC · PCI DSS Compliant

[1] Beazley Breach Briefing, 2019 [2] 2018 Cost of a Data Breach Study, Ponemon Institute [3] Ponemon Privacy and Security of Healthcare Data
[4] Verizon 2017 Data Breach Incident Report [5] Gartner Group [6] Forrester Report: "Best Practices: Selecting, Deploying, And Managing EPM"

Business Sales

Americas & APAC
+1 312 829 2680

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Ireland
+353 21 229 6020

EMEA
+353 21 229 6011

Netherlands
+31 20 262 0932

Iberia & Italy
+34 919 01 65 13

Sweden & Nordics
+46 8 403 049 28

keepersecurity.com

sales@keepersecurity.com

Support

Consumer
+1 312 971 5702

Business (Americas & APAC)
+1 312 226 4782

Business (EMEA)
+353 21 229 6019