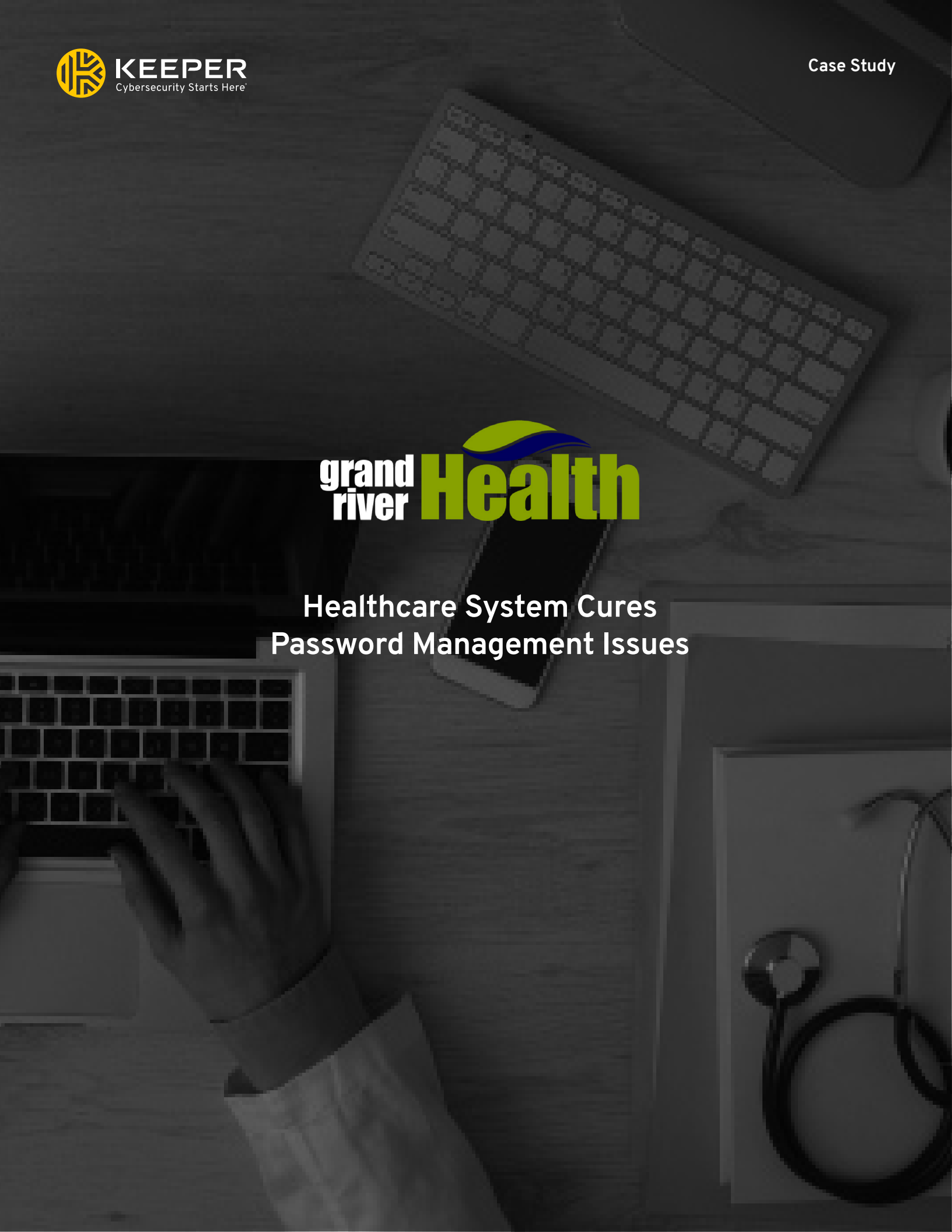
KEEPER
Cybersecurity Starts Here®

Case Study



grand river Health

Healthcare System Cures Password Management Issues

KEEPER®

A growing regional healthcare system needed a reliable way to manage role-based permissions for passwords amid healthcare's stringent privacy and security rules.

Challenge

- Strict requirements for data privacy and security
- Paper password list no longer viable
- Heavy volume of password-related calls to help desk

Solution

- Role-based password manager
- Zero-knowledge security and 2FA protection against unauthorized access
- Customizable to organizational structure and policies

Results

- Stronger data security
- Increased efficiency
- Better data access controls

About Grand River Hospital District

Grand River Hospital District is a local healthcare system serving patients in a 1,500-square-mile territory around Rifle, Colorado, in the western part of the state. The district has more than 550 employees and 100+ affiliated physicians who work in five medical, long-term care and student health facilities.

The Challenge

Since opening its first hospital in 1962, Grand River Hospital District (GRHD) has grown into a vital part of the community, employing hundreds of employees and caring for thousands of patients each year. As GRHD expanded and healthcare data privacy and security requirements increased, the information technology (IT) department realized the way they managed passwords for the organization no longer worked.

> **As privacy and security requirements increased, the old way of managing passwords no longer worked.**

"We outgrew our paper master password list," said Daniel Wilson, GRHD Network Engineer. "With our systems becoming more complex, we needed role-based permission for passwords and a better way to keep them secure. The paper list just wasn't viable." Password resets were another problem. As in many organizations, about half the calls to the IT help desk were the result of forgotten passwords, placing a heavy burden on Daniel's busy staff.

When Daniel and his team started looking into password management software, they had several functional requirements in mind. Security and role-based permission topped the list, but they also wanted to be able to easily import and export passwords; access the password manager from all platforms, especially mobile; and access the password vault offline.

The Keeper Solution

Keeper's configurable roles, role-based permission and administration privileges, all assignable according to organizational hierarchy, were a perfect fit for GRHD. Daniel and his team can fully customize employee permissions through fine-grained access controls based on their roles and responsibilities.

> **The Keeper solution is built on zero-knowledge architecture.**

On the security front, Keeper stood out immediately. The solution is built on zero-knowledge architecture, which means no one except the user has access to records and full control over their data. With Keeper, encryption and decryption happen only on the user's device when they log in to the vault.

Keeper's two-factor authentication (2FA) was another strong plus for Daniel and his team. Keeper partners with DUO Security to provide an extra layer of protection when users log in to websites or applications. GRHD's IT administrators can monitor login attempts by any user, in any location, from any device to prevent unauthorized access.

Daniel's team found Keeper to be the only password manager with an excellent mobile experience that passed GRHD's strict security criteria. No matter what device or platform employees use, records automatically sync and provide full online and offline access. The Keeper solution also eases the burden of password reset calls to GRHD's IT help desk by adapting service to the healthcare system's organizational structure and policies.

The Results

The Keeper password manager solution allows GRHD to keep pace with stringent HIPAA requirements and gives the IT team an easy and efficient way to manage passwords for the organization's growing staff. "The Keeper vault allows us to securely manage the lifecycle of privileged account credentials," said Daniel. "When a new person starts, IT can gradually give them access to what they need, and we can also retract it at any time. Keeper gives employees on-demand access to passwords, websites and applications, which increases their productivity while protecting GRHD and our patients with best-in-class security.

The Impact

As the primary healthcare provider in the region, GRHD has a responsibility to protect patients' privacy and health data. With weak passwords accounting for 81% of data breaches,[1] strong, reliable password management is essential to earning patients' trust and maintaining a positive reputation.

> **Weak password security leads to more than 80% of data breaches.**

Keeper gave GRHD a practical, scalable approach to password management that allows them to protect valuable information as the organization grows.

About Keeper

Keeper Security develops leading password manager and security software for protecting businesses and client information. Keeper works with companies of all sizes across every industry to mitigate the risk of data breaches, bolster data security and privacy, increase employee productivity and strengthen cybersecurity reporting and compliance.

To learn more about Keeper Security's leading password manager and security software, visit **keepersecurity.com**.

[1] Verizon Data Breach Investigations Report, 2017