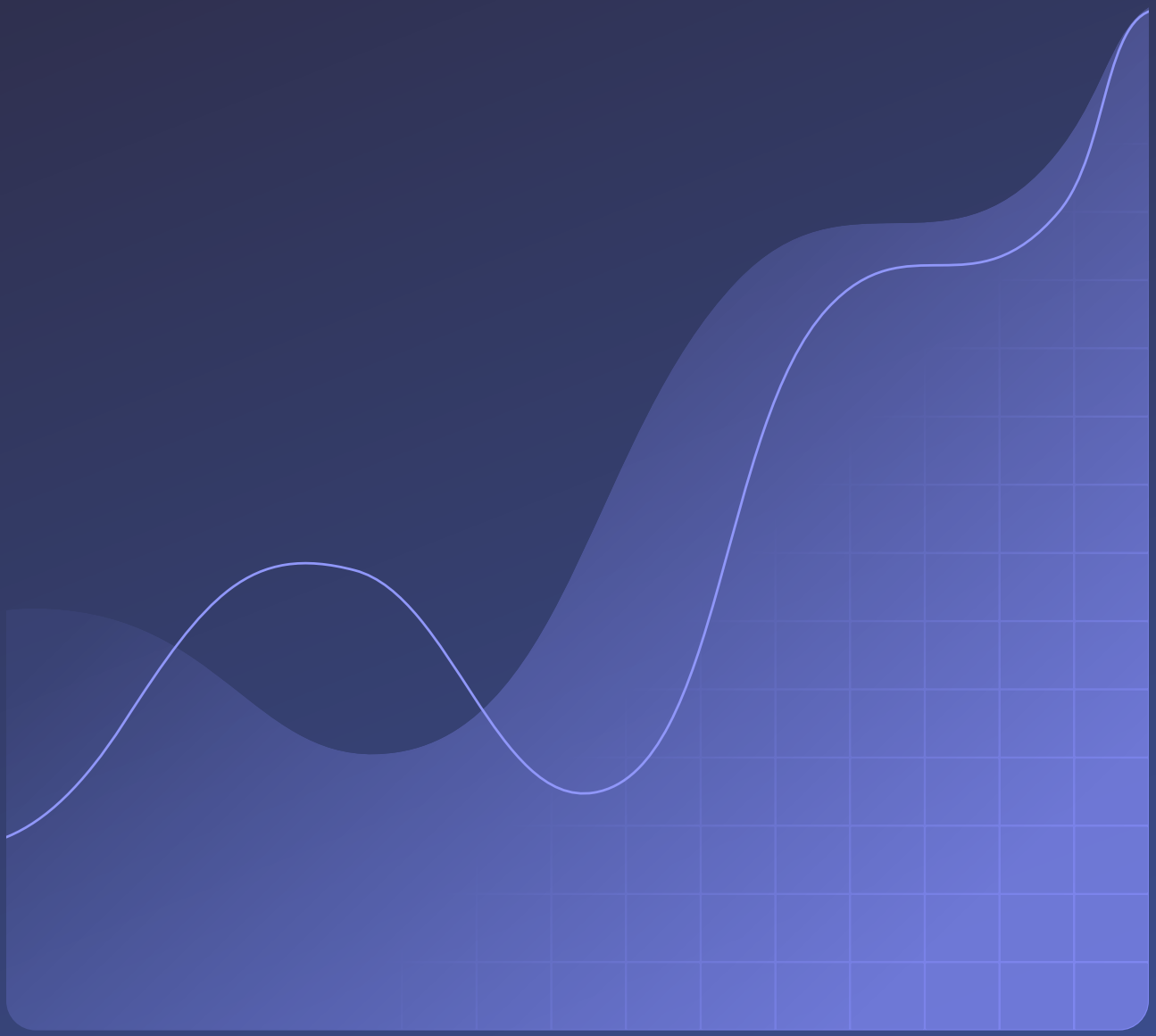
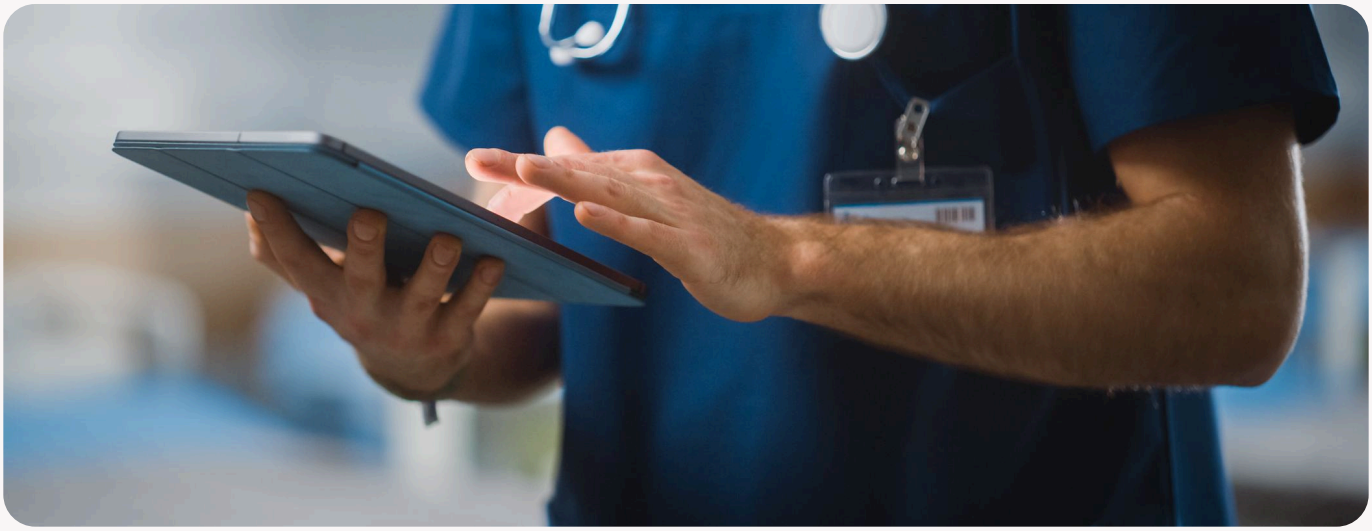
DASHLANE

CASE STUDY

How a Healthcare Tech Company Ensures HIPAA Compliance for a Nationwide Workforce





KOVO

Industry

Headquartered in Canada with operations in the U.S., Kovo HealthTech is a healthcare technology and Billing-as-a-Service company.

Industry

Technology

Company size

200 employees

The challenge: Streamline offboarding and mitigate remote work security risks using a HIPAA-compliant solution

In the dynamic landscape of healthcare technology, Kovo HealthTech stands out as a provider of innovative solutions, including cutting-edge healthcare software and Billing-as-a-Service offerings. Headquartered in Canada with operations in the U.S., the organization has been experiencing rapid growth, marked by 14 successful acquisitions. Together, Kovo subsidiaries process over $80 million in medical billing claims annually, catering to the needs of approximately 3.5 million patients.

Kovo works with protected health information and must be HIPAA compliant. In the event of any HIPAA breach, they would incur up to a $25,000 penalty for each patient's file that is improperly accessed. Leaked data could put patients' security at risk and damage Kovo's reputation by reducing clients' and prospective clients' trust in the organization.

> "Even a perceived lack of safety could hurt our business."
>
> **Nicole Statley**, Compliance Coordinator, Kovo HealthTech

The U.S. Department of Health and Human Services Office for Civil Rights offers cybersecurity tips without imposing strict HIPAA enforcement methods. Kovo was meeting security requirements and following HIPAA guidelines, but they wanted to do more to protect their clients and their organization.

Additionally, as a publicly traded entity, Kovo must prioritize shareholder interests, necessitating robust security measures to maintain trust and shareholder value. Kovo started looking for a credential management solution to roll out across the organization and keep access points secure.

With over 75% of their employees working remotely and using diverse servers and systems, Kovo faced access management challenges, with onboarding and offboarding proving to be particularly difficult.

Granting secure access to new hires was tricky, but Kovo's primary concern lay in offboarding because they needed to swiftly revoke access for ex-employees, including remote ones. Former employees had to return their computers by mail to Kovo, which took time and introduced additional risks because delaying offboarding procedures could afford former employees the chance to continue accessing sensitive data.

> "We needed to know who was accessing confidential information and when, which required stricter control."
>
> **Nicole Statley**, Compliance Coordinator, Kovo HealthTech

In addition, Kovo was growing and wanted to establish a compliance program and stronger security practices as they scaled. Previously, employees could use any method of storing credentials, which ranged from spreadsheets and shared digital documents to handwritten hard copies and free digital tools—all of which raised security concerns. Nicole points out, "Free credential managers don't have the same level of encryption or security." For example, anyone who uses a computer can access credentials saved in website browsers.

To help navigate the intricate realm of protected health information, Kovo's ideal credential manager would provide:

- Fast onboarding and offboarding
- Clear oversight
- Secure, HIPAA-compliant access
- Strong UX

The solution: Streamlined access and intuitive credential management

Around the same time that Kovo started their search for a solution, their CEO shared that he uses Dashlane to protect his personal accounts. Nicole evaluated several credential managers, and she was also drawn to Dashlane.

She appreciates the solution's ease of use, including how it creates and stores credentials, saying, "Password Generator is my best friend. When we use Dashlane's Password Generator, we know we're getting the most secure password possible."

Nicole recognized that Dashlane would help Kovo surpass compliance requirements and gain the robust cybersecurity the organization wanted. She knew that as long as everyone at Kovo was using Dashlane, they were meeting HIPAA's password requirements.

Now, Kovo benefits from a variety of features:

- Password Generator creates strong, random passwords automatically
- The secure credential vault safely stores and encrypts an unlimited amount of passwords
- Dark Web Monitoring alerts users when their passwords have been compromised and provides recommended next steps to secure those passwords
- The web extension allows employees to work seamlessly and securely access their logins without repeatedly opening a separate desktop app
- Technology versatility means that employees can collaborate while using their preferred operating system
- The Admin Console offers one centralized credential management system, including simple employee management and auditing when required

The results: Leveling up security and ease of use with a reliable solution for the entire organization

Kovo didn't want to make any security compromises, so they rolled Dashlane out to their entire organization. After using Dashlane for the last two years, Kovo has been very impressed with the solution's reliability and ease of use.

Nicole shared, "Very few people have had trouble with Dashlane." When one-off concerns do arise, Kovo has found Dashlane Customer Support to be incredibly responsive.

Today, the solution is used by Kovo employees located across the United States and abroad. Nicole loves that Dashlane simplifies onboarding and offboarding.

"When I'm training people, I tell them not to be nervous if the solution is new to them. Dashlane just works."

Dashlane has helped Kovo develop stronger policies and procedures beyond what they had initially hoped for, increasing the scope of their security transformation. Kovo now has robust security without complicating employees' lives.

> "Our cybersecurity is broader and deeper because of Dashlane."
>
> **Nicole Statley**, Compliance Coordinator, Kovo HealthTech

Dark Web Monitoring has played an important role in tracking Kovo's handful of domains. Kovo employees also feel more secure now that they can monitor their professional and personal email addresses for security breaches. Thinking about the impact of the solution, Nicole feels that everyone within Kovo's sphere of influence is benefiting from Dashlane.

"With Dashlane, we have a ripple effect: We're safeguarding our company and our employees as well as the doctors we serve and their patients."

Kovo is more secure than ever before because Dashlane offers a higher level of security compared to the solutions employees were previously using. With Dashlane's Admin Console, it's easy for Nicole to see if people are leveraging the solution. Dashlane's Password Health score enables additional credential oversight, and Nicole can ensure that all organizational passwords are strong and original. With Dashlane's zero-knowledge architecture, no one, not even Dashlane, can see users' passwords or other data.

"Dashlane's security is the best. I love the solution's architecture," says Nicole.

Kovo's employees appreciate that the Dashlane app and extension save them from opening additional tabs. They've found that information stored in Dashlane is effortlessly available from any location and device. By installing Dashlane on their phones, they can seamlessly access their credentials even when their normal device is unavailable, like when they're traveling for work.

Nicole adds, "Our executive leadership team is particularly fond of Dashlane."

Today, Kovo has a very intentional cybersecurity strategy and continues to turn to Dashlane for leading credential management solutions. As Dashlane introduces more security features, Kovo remains proactive, embracing those that align most effectively with their compliance and organizational requirements.