A Reciprocity Case Study

RECIPROCITY

Driving Greater Information Security in Digital Healthcare

Partnering with Reciprocity, Omada Health is doing more than improving its information security — it's paving the way for a more secure industry.

Not only does healthcare still top the list of the most breached industries, in 2020, it marked its tenth year in a row claiming the highest average cost of a data breach.

No surprise, information security is top-of-mind for healthcare providers.

For digital healthcare providers, in particular, it's an existential threat.

Yet for leading digital health company Omada Health, it's part of their brand.

Reliant on the protected health information (PHI) customers and members provide to drive its chronic-care solutions, Omada Health knows that ensuring data is private and secure requires more than just check-the-box compliance. And in its quest to build a more secure business, it's hoping to set the bar for a more secure healthcare industry.

"Trust and safety are foundations for everything we do," says William Dougherty, Omada Health's CISO. "Our differentiators in the marketplace include our security, our trustworthiness and our safety."

Identifying the Challenges — and the Opportunity

Flashback to just a few years ago, and Omada Health — one of the largest digital healthcare practitioners in the world, serving some 1,200 businesses and over 400,000 individuals since its inception in 2011 — was struggling to manage risks using spreadsheets. And while the norm for many healthcare providers, this process became a pivotal issue for Omada Health.

The bulk of Omada Health's customers are medium and large employers that purchase the solution for employees and health-plan providers who offer it to their customers. Omada offers solutions for the prevention and treatment of type 2 diabetes, hypertension, behavioral health and musculoskeletal/physical therapy. For the individually tailored programs to work, users must provide accurate, up-to-date information from their medical records and enter honest data about their lifestyle, diet, stress, sleep habits, choices and medications.

"We're dealing with the most sensitive information people have," Dougherty explains. "Our members trust us because their employer or health plan says we're trustworthy." Thus being able to demonstrate control effectiveness is critical to acquiring new customers.

Shortly before Dougherty joined the company in 2016, Omada Health fell short of obtaining the challenging and coveted security-related HITRUST certification they promised their customers and which would have positioned the company as the leader in its field. Once on board at Omada Health, It was not difficult for Doughtery to understand why.

Omada Health's risk and compliance managers were using spreadsheets to track controls and compliance activities as well as those of its more than 250 vendors. On top of that, they didn't have a single repository from which they could see gaps across frameworks, nor did they have a standard way of doing a risk assessment. The process was confusing, time-consuming, frustrating and ineffective.

Herein began Dougherty's quest to find a GRC solution.

"We're dealing with the most sensitive information people have... Our members trust us because their employer or health plan says we're trustworthy."

Finding the Right Fit

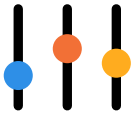
When Dougherty set out to find a solution, his motivation was about much more than just gaining control of his security program — he wanted to make security a competitive advantage and a part of Omada's brand. To accomplish this, he needed an integrated and automated technology solution to make GRC initiatives more streamlined, efficient and impactful, enabling him to pass third-party attestations and customer audits without exceptions.

After evaluating nearly a dozen GRC solutions, Dougherty selected Reciprocity's ZenGRC platform. The decision all came down to five key attributes that make ZenGRC stand out from the rest.

USER-FRIENDLY

"Zen is simple to use," he says. "It's incredibly easy to put data into and retrieve it from—you just import and export your spreadsheets."

Being able to easily transfer data was especially attractive given the number of vendors, controls, risks and threats Omada Health was tracking and managing. In its latest annual risk assessment, the company used ZenGRC to track:



631
CONTROLS

1,347
OBJECTIVES

68
POLICIES

37
BUSINESS PROCESSES

82
RISKS

510
VENDORS

42
THREATS

"Without a good GRC tool, there's just no way to track this many risks, threats and control activities," Dougherty says. "And if you aren't tracking them, you probably aren't doing a good job on your HIPAA risk assessments."

02 EASY TO COMPREHEND

ZenGRC's risk "heat map" clearly shows the 15 risks — out of 82 — security and compliance teams should focus on first.

03 EFFICIENT

With an initial security team of 1.5 people and one internal auditor at Omada Health, Dougherty appreciated that using ZenGRC didn't require hiring more staff.

"We wanted a tool that would help us to do our work and that wouldn't become work."

CUSTOMIZABLE

ZenGRC's templates allow revisions, custom fields and deletions according to the user's needs and desires. "It's a matter of collecting your universe of things you want to track, putting them in and building processes around the end product."

HOLISTIC

ZenGRC's "single source of truth" dashboard provides a big-picture view of compliance, linking frameworks together to make controls management easier and more efficient. ZenGRC maps each control and activity to all relevant standards, as well as to risks, threats and vendors. "I'm a big believer in, 'Audit once for everything,' " Dougherty says.

"I'm a big believer in, 'Audit once for everything.' "

“Zen was easy to use, it matched our mental model for how things ought to be linked together, it had all the compliance programs we needed to deal with available to us as templates and it was extensible,” Dougherty says. “I didn’t find another solution that even came close.”

A Model for Success

Dougherty finds ZenGRC invaluable for managing Omada Health's hundreds of contractors—a nearly impossible task under the old spreadsheet method. In fact, when he came on board, Omada Health only tracked 40 to 50 of its vendors, leaving the company vulnerable to any threats the rest might pose. "Before ZenGRC, we didn't know what we had," Dougherty says.

Today Omada Health actively manages all of its third-party contractors and is establishing a threat model for each, identifying where threats might come from so it can proactively address them. Dougherty also uses ZenGRC to take this modeling beyond vendors to sniff out threats to security, privacy and compliance from any source imaginable: code its developers or vendors have written, new business offerings, a company Omada Health may want to acquire or something else.

"Threat modeling and risk assessment in digital health is incredibly complex," Doughtery says. To that end, Omada Health is pioneering efforts to educate the industry on best practices for security, privacy and threats. In 2019, Omada Health published the whitepaper INCLUDES NO DIRT, which offers a holistic view of the threat landscape and provides a new threat model for digital health designed around ZenGRC's capabilities to evaluate complex threats. By publishing the model for other healthcare companies, including competitors, to use, Dougherty and his co-author, VP of Compliance Patrick Curry, hope to help the entire industry improve. "Healthcare is consistently the most-breached industry. The entire industry must get better, and that can only happen through collaboration and cooperation throughout the ecosystem," says Dougherty.

Using ZenGRC's surveys and scoring mechanism, Omada Health built its NODIRT model around 14 parameters, including authorization, non-repudiation, licensure, anonymity— "a whole range of stuff to try to make sure that we understand how the system is going to be used and where threats may come from," Dougherty clarifies. "This model hits on everything we worry about from a risk perspective in digital health. Without a good model, you're flailing around."

"Healthcare is consistently the most-breached industry. The entire industry must get better, and that can only happen through collaboration and cooperation throughout the ecosystem."

ZenGRC's vendor module not only helps Omada Health spot risks, but it also helps the company focus on the important ones. That's critical for dealing with so many suppliers at once, especially when a single oversight or misstep could become a critical event. Data breaches are the top concern, of course. But Doughtery says the supply chain also poses risks: customers need their glucometers, blood-pressure cuffs and scales to show up when and where they are supposed to arrive.

And when problems do arise, ZenGRC makes it easy to track them to their source: *Who approved the vendor? When and why? What, if anything, has changed since then?* ZenGRC creates the record for each vendor during procurement and maintains it as evidence for later retrieval.

"The ZenGRC vendor module is something I couldn't live without," Dougherty says. "I literally couldn't do my job without it."

Reciprocity's support staff has played a major role in helping Omada Health's security, risk and compliance people use ZenGRC to its fullest extent. "The teams are very easy to work with—they have helped me get the most out of the product," Dougherty says. "They're also very receptive to feature requests and have made changes that I suggested. I really like calling them!"

"The ZenGRC vendor module is something I couldn't live without," Dougherty says. "I literally couldn't do my job without it."

Making Risk Management and Compliance a True Differentiator

During the period since Omada began using ZenGRC, it has more than tripled the number of businesses and members it serves. Doing so required the company to pass numerous security reviews with some of the largest, most security-conscious employers and health plans in the country. Dougherty credits this success in part to the program he built with ZenGRC at its core. “ZenGRC has helped us turn risk management and compliance into a true differentiator in the market,” he says.

ZenGRC helped Omada Health complete its first comprehensive risk assessment in 2017 as well as correct deficiencies and fill gaps to become compliant with a number of critical security frameworks, including HITRUST and SOC 2 —the first digital diabetes prevention company to do so. These certifications add

peace of mind to Omada Health and to everyone with whom the company does business. “These are four- and five-way trust models,” Dougherty explains. “The employee trusts their employer; the employer trusts their health plans and Omada; and we have to trust all our vendors using that data. Anybody makes a mistake and we all have a bad day.”

Dougherty wouldn’t hesitate to recommend ZenGRC to others and, indeed, he already has. “For anybody who’s living in spreadsheet hell—which is most of us—ZenGRC is a sane way of managing your information and keeping it consistent for long periods of time,” he says.

“My CEO often says that when a large employer used to say, ‘We want you to fill out our security questionnaire,’ he would groan. ‘The time and difficulty involved made those requests the bane of everybody’s existence. Now when they ask, he gets excited. Because we have a strong story to tell, a story based on real security and real risk management backed up by real third-party attestation—powered by our use of ZenGRC.”

“...we have a strong story to tell, a story based on real security and real risk management backed up by real third-party attestation—powered by our use of ZenGRC.”

About Reciprocity

Reciprocity is powering the next generation of information security with the fastest, easiest and most prescriptive solutions in the market. Its fully integrated and automated ZenGRC platform delivers a full catalog of compliance, risk and other infosec applications through one simple user interface that drives greater transparency, actionable insights and benchmark reporting.

Recognized for its GRC expertise and its accelerated time-to-value, Reciprocity is transforming risk and compliance from a cost-center to a value-creator for businesses across the globe. The company is headquartered in San Francisco with global offices in Ljubljana, Slovenia and Argentina.

www.reciprocitylabs.com

Powering the next generation of information security.