RECIPROCITY

omada

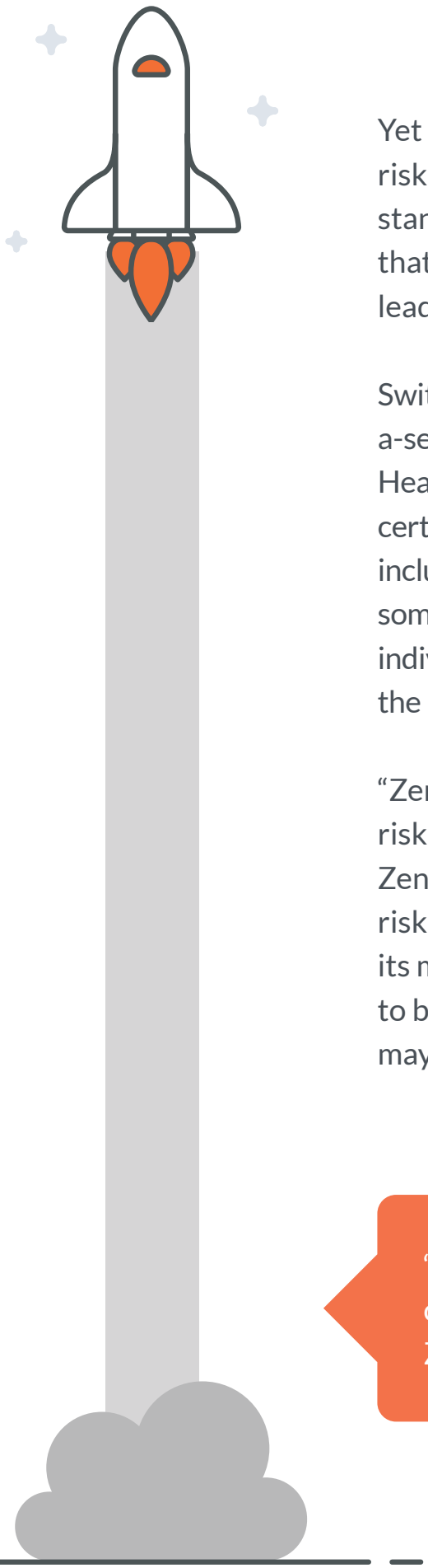
Leading the Digital Healthcare Pack

Case Study

Protecting sensitive data is now top of mind for healthcare providers, and Omada Health is no exception.

The digital health company relies on Personal Health Information (PHI) to drive its health and wellness solutions, and its users rely on Omada Health to keep their data private and secure.

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



Yet a few years ago, Omada struggled to manage risks using spreadsheets, and fell short of meeting standards—extraordinary ones, and self-imposed—that would have positioned the company as the leader in its field.

Switching to Reciprocity's ZenGRC software-as-a-service made all the difference. Today, Omada Health is the first digital health company to achieve certification with a number of security frameworks including SOC 2, and business is booming. Serving some 500 large businesses and over 250,000 individuals since its inception, Omada Health is one of the largest digital healthcare practitioners in the world.

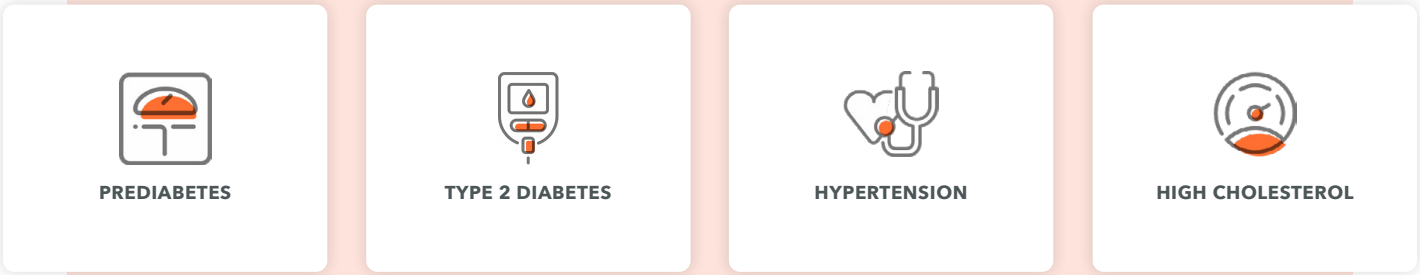
"ZenGRC is our source of truth for all of our controls, risks, and threats," Dougherty says. Omada uses ZenGRC to identify and track third-party vendor risks, too, as well as other critical information about its more than 250 vendors. ZenGRC helped Omada to build its own security program, and the company may expand its certifications to include ISO 27001.

> "We're ahead of the competition when it comes to managing risk and compliance. ZenGRC played a key role in getting us there."

About Omada Health

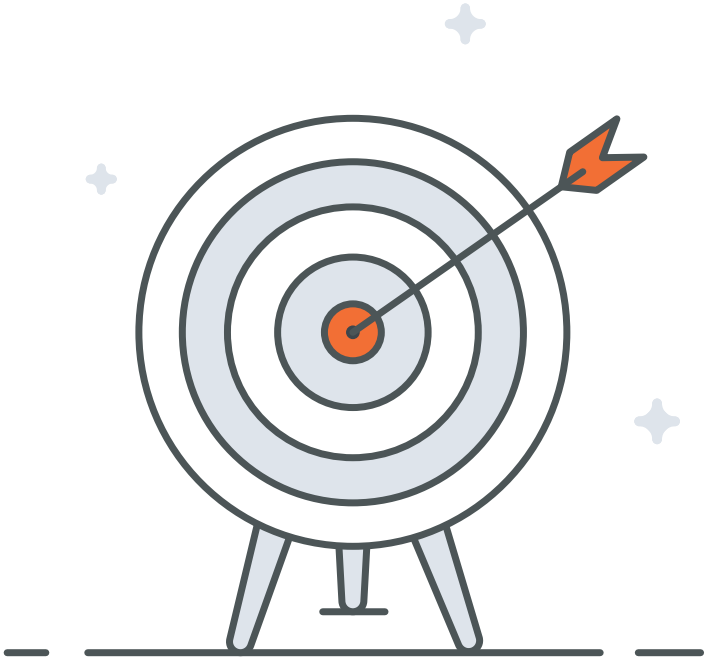
Omada entered the digital health space in 2011 with a program aimed at preventing the onset of type-2 diabetes in people at risk. Today its application uses a combination of digital and human interventions to guide diabetics as well as pre-diabetics to better health choices, and offers programs to help treat high blood pressure (hypertension) and high cholesterol.

One dynamic program for multiple conditions



The bulk of Omada's customers are large employers who purchase the solution for employees, and health plan providers who offer it to their customers. 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, and sleep habits and choices.

"We're dealing with the most sensitive information people have," Dougherty says. "The participant trusts us because their employer or health plan says we're trustworthy." Being able to demonstrate control effectiveness is critical to acquiring new customers, he says.



Spreadsheets Were Their Weakness

Shortly before Dougherty joined the company in 2016, however, Omada Health had fallen short of obtaining one challenging and coveted security-related certification. It was not difficult for him to see why: risk and compliance officers were using spreadsheets to track Omada's controls and compliance activities as well as that of its many vendors. The method was confusing, time-consuming, frustrating, and ineffective.

One of Dougherty's first mandates was to find a GRC solution. He considered about a dozen before choosing ZenGRC. **He liked ZenGRC, he said, because it is:**

User-friendly.

"Zen is simple to use. 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 was tracking and managing. In 2018, the company conducted its annual risk assessment using ZenGRC, tracking:

163
CONTROLS AGAINST
320
STANDARDS

$12M
IN VENDOR EXPENDITURES

731
OBJECTIVES

164
TRACKED VENDORS

42
THREATS

169
RISKS IN
19
RISK CATEGORIES

"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."

Easy to comprehend.

The solution's risk "heat map" clearly showed which of the 169 risks (29 of them) IT security teams should focus on first.

Efficient.

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

> "We wanted a tool that would help us to do our work 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.

"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," he says. "I didn't find another solution that even came close."

Vendor Management Features ‘Invaluable’

Dougherty also finds ZenGRC invaluable for managing Omada’s 250+ 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 itself vulnerable to any threats the rest might pose.

> “Before ZenGRC, we didn’t know what we had,” Dougherty says.

Now Omada actively manages all 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 uses ZenGRC to take this modeling beyond vendors, too, 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 might want to acquire, or something else.

“Threat modeling in digital health is incredibly complex. We need to pay attention to security, privacy and compliance threats. Omada recently published a whitepaper on a new threat model for digital health, called INCLUDES NO DIRT, that attempts to take a holistic view of the threat landscape. We built that model using ZenGRC’s capabilities to evaluate complex threats,” Dougherty said. Using ZenGRC’s surveys and scoring mechanism, Omada built its 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.”

> “This modeling hits on everything we worry about from a risk perspective in digital health,” Dougherty says. “Without a good model, you’re flailing around.”

ZenGRC's vendor module not only helps Omada spot risks, but also to 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, yes, Dougherty says, but the supply chain also poses risks: customers need their glucometers, blood-pressure cuffs, and scales to arrive when and where they are supposed to.

And when problems 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 at onboarding and maintains it as evidence for later retrieval.

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

Dougherty says.

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, Dougherty says.

"The teams are very easy to work with—they have helped me get the most out of the product. They're also very receptive to feature requests, and have made changes that I suggested. I really like calling them!"

Say Good-Bye to ‘Spreadsheet Hell’

Dougherty wouldn’t hesitate to recommend ZenGRC to others, he says, 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.”

ZenGRC helped Omada Health complete its first comprehensive risk assessment in 2017, and to correct deficiencies and fill gaps to become compliant with a number of critical security frameworks including SOC 2—the first digital health company to do so. These certifications, added to those the company already possessed including HIPAA and PCI DSS, add to Omada Health’s peace of mind and to that of everyone the company does business with.

“These are four- and five-way trust models,” Dougherty says. “The employee trusts their employer; the employer trusts us; we have to trust all our vendors using that data. Anybody makes a mistake and we all have a bad day.

“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.

“ZenGRC has helped us turn risk management and compliance into a true differentiator in the market.”

About Reciprocity

Founded in 2009, Reciprocity has reimagined bulky legacy GRC software to meet the demands of today's dynamic data-driven ecosystem. The company is recognized for its forward-thinking cloud platform, ZenGRC, that elevates risk,compliance, and audit from a burdensome expense to a strategic advantage. Reciprocity is headquartered in San Francisco, CA, with offices in Europe and South America.

Contact a Reciprocity expert today to request your **free demo**, and embark on the worry-free path to regulatory compliance—the Zen way.

www.reciprocitylabs.com
engage@reciprocitylabs.com
(877) 440-7971