CISO GLOBAL

A **CISO GLOBAL** CASE STUDY

A **Health Technology** Startup Uses **Cybersecurity** & Compliance to **Support** Business **Growth**

HEALTH TECH & CYBER

Overview

The health industry is a data-rich, attack-frequent vertical. Personal Health Information (PHI) has become a valuable target of bad actors, while privacy laws and regulatory actions continue to mature, driving more security and compliance needs. HIPAA's passage in 1996 belies the larger industry's struggle to grow in an environment complicated by intense data security compliance. And while health tech companies scramble to both comply and grow, rules evolve, including the most Recent product-focused iteration to the 21st Century CARES Act mandating new interoperability standards for patient data API access.

Moreover, and increasingly, investors want to know their money is secure and that risks are proactively mitigated, including cyber risk. The average cost of a data breach continues to grow each year. And recent history confirms numerous malware attacks aimed at the health space that shut down startups, costing millions of dollars in investor equity while exposing client, vendor and patient data. According to Reuters, one patient healthcare credential – name, address, social security number, birth date and health history – is worth $10 on the black market or 10-to-20 times the value of one credit card.

Why else should health technology organizations secure themselves before a catastrophic cyber event?

- Breaches threaten company enterprise value for investors, vendors and partners alike, as well as longer-term brand reputation and deal flow.
- Compromised business systems overwhelm day-to-day operations, depressing both solution speed-to-market and human capital productivity.
- Insecure environments complicate cash management, forcing business leaders to juggle revenue actions and security reactions.
- Client contracts require HIPAA compliance at a minimum and a tight security program counsel can rely upon.
- Protecting intellectual property is no longer a strategic priority but rather a passive imperative that must not disturb organizational growth.

The oftentimes ignored reality: many of these breaches are preventable with proactive preparation, smart controls, owner-designated response, and an embedded partner that softens cost and implies more active interactions.

Smart Choices

Given the risks associated with third party vendors and supply chain vulnerabilities, health tech organizations are better off using fewer, direct providers. More third-party vendors engaged in a disparate fashion for reactive needs can actually increase the likelihood of an incident. But with most security or IT providers currently on the market, companies have to choose their priorities, then cobble together multiple providers / solutions in order to meet all of their technology, security, and compliance needs.

Authority in the Healthcare, Insurance, & Health Technology Space

CISO has nearly two and a half decades of Healthcare industry experience, which is the primary consumer of Health Tech platforms, products, and services. In this way, the organization is able to help position health technology companies' compliance and security programs to address the needs and intent of buyers and partners in this space: their primary challenges, business priorities, regulatory headaches and underlying missions. In fact, the CISO Risk Advisory team is often enlisted to review their potential partners, vendors, or investments–including health technology companies.

Further, CISO has the benefit of having established itself as a technology provider,

> *"How do you conduct business in a highly regulated and litigated environment in a way that goes beyond 'check the box', and explore the CISO meaning behind security that becomes part of organizational ethos?"*
>
> – General Counsel at a Prominent Health Tech Organization

in addition to its core consultative offerings, so many of the recommendations for tech company program development are rooted in first-hand experiences. This institutionalized sector knowledge in the cyber and compliance contexts, from leadership to service operators, supports the ability to build a well-rounded program.

Understanding the stringent requirements technology startups face from both a compliance and a consumer standpoint when selling into regulated industries has led to CISO's comprehensive services stack, tailored expressly to these unique industry challenges and regulatory hurdles. CISO works across the spectrum of highly-regulated technology industries, porting lessons learned across client sets to maximize efficacy.

Security Programs Must be Tailored to Your Business Objectives

Case in Point: CISO's Partnership With a Prominent Health Tech Startup

The real challenges to security are timing and buy-in. Understanding the client's business objectives must come first; only then can the right partner engineer and manage a security program that adapts to the pace and priorities of a tech startup client. Figuring out how to handle culture, business, and process takes forethought and high touch. And that has been CISO's integration approach to working with this Health Tech data curation platform company from the beginning.

When CISO Global and this Health Tech organization started their journey together, there was a sensitivity to organizational growth priorities. And rightly so: health tech startups are in a highly-regulated, saturated space dealing with complex, private datasets, long sales cycles and bottom-line goalposts that shift with each new piece of legislation passed. CISO brought a practical, small team approach focused on client education first, and pinned execution to the company's specific maturation cycle.

Certifications That Supported Business Growth

That approach focused on certifications critical to growth: HITRUST first and SOC II Type 2 thereafter. As leaders on both sides would admit, these certifications could not be executed ad-hoc, but rather required thoughtful structure, including the creation of an oversight committee to keep the burgeoning security program embedded in business decisioning.

A Virtual CISO Makes High

Quality Security Leadership Accessible

From that first set of certification accomplishments, a virtual CISO relationship emerged, and security thought leadership took a more involved role in the Health Tech startup's maturity. The forward plan became one that considered policy, process and key hires to cement security as an organizational value, all the while sensitive to the cost / value curve to minimize the disruptive perception of "excess IT spend" that so typically reduces security program value to a line item.

In fact, the opposite occurred. The startup's leadership team brought CISO to potential client calls as a technical resource also heavily embedded in business operations. The value-add of a resource who could speak the languages of both cybersecurity and deal flow positively impacted both organizational dimensions. For a startup signing global, enterprise clients who possessed multiple layers of sophistication, this was a tangential, but material way to de-risk both pipeline and portfolio. Decoupling business, data regulation, privacy and security allowed the company to look more deeply at risk and protection along their growth curve and in the context of their mission and drivers.

Building Sustainable

Security for Scale

Today, CISO and this Health Tech data curation company continue their partnership approach to strengthening the company's security and compliance posture with the understanding that this is an ongoing process. Through the Virtual CISO program, CISO's Jerald Dawkins, PhD has helped the organization implement the centralizing force of an automated GRC platform, to support streamlined management of their security and compliance program through the integrated visualization of data, process, insights, actions, and communication … a virtual security balance sheet.

"Security is more than a cost element within a technology department.

It should be structural and cultural and should be pervasive within the organization, both vertically and horizontally."

– Chief Customer Officer
at a Prominent Health
Tech Organization

ABOUT CISO GLOBAL

CISO has walked numerous technology startups through each of the critical phases of security program development, working as an integration partner to manage the breadth of policy, process, system integration, secure operational technology support, revenue support and executive leadership advisory. Maintaining technology experts, certified engineers and an end-to-end approach to cybersecurity program development, CISO has the ability to help Health Tech organizations of all sizes meet their technology, security, and compliance needs through a single provider.

Health Tech Requires Specialized Knowledge

The current landscape of the cybersecurity industry is a disjointed conglomeration of vendors, services and solutions that are delivered in an uncoordinated fashion, leading to implementation inefficiencies and lost business productivity. This "status quo" approach leaves company leadership with little real visibility into their security posture or compliance status.

CISO has the necessary experience and personnel to attack this problem by offering an integrated, end-to-end solution that currently is not prevalent in the marketplace. This unique approach creates a new type of Cybersecurity company: the Managed Compliance and Cybersecurity Provider (MCCP+).

As health care providers increasingly require evidence of mature compliance programs, compliance with the HIPAA Rule is central to securing electronically protected health information. The reality, though, is that HIPAA is nonspecific and complex. CISO shortens that timeline to providing compliance for Health Tech through Consulting Solutions informed by rich healthcare experience and integrated with the various IT, Cybersecurity, and Compliance solutions needed to maintain compliance. Our security-first approach to HIPAA Assessments provides the insight you need to achieve the greatest security program gains while also achieving HIPAA compliance.

CISO's integrated, end-to-end services can support Health Tech startups from the moment you are ready for your own network, through the growth stages where you need compliance support and security program development, finally helping you scale and protect what you have built. Our teams' vast expertise, specialized knowledge, and available resources can support your Health Tech company's needs from beginning to end with a single, trusted partner. Regardless of your stage, our integrated Cybersecurity, IT, and Compliance solutions for Healthcare Technology enable you to achieve your technology goals while managing your operational risk.

SOC 2® Type II Audited

CISO Global Service Areas

- M & A Assessment Services
- Secure Cloud Adoption and Management
- 24x7x365 Cybersecurity Monitoring Services
- Two fully owned, operated, & staffed Security Operations Centers
- Audit Readiness & Assessment Services
- Security Awareness Training
- Incident Response Services
- Security Assessment Services
- Penetration Testing Services
- Vulnerability Management & Remediation Services
- Policy Development & Documentation
- Security & Compliance Management Platform
- Remediation Services

For more information on CISO services or client references, please contact us or visit www.ciso.inc.