



WHITE PAPER

Security That Carries the Deal

The operator's vCISO model for health tech, and how three kinds of companies turned security posture into a revenue asset.

Steadfast Partners LLC

Virtual CISO Services for Health Tech

October 2026

Executive Summary

In health tech, security is not a back office function. It is the gate between your product and your revenue. Every enterprise health system, payer, pharma sponsor and investor you want to work with will assess your posture before they trust you with patient data or their own reputation. Most of them will do it before your first demo.

The companies that win in this market treat security as a sales asset. The companies that stall treat it as a compliance project they will get to after the next round. The difference is rarely budget. It is who is in the seat and whether that person has ever sat in yours.

This paper lays out the operator's vCISO model that Steadfast Partners brings to growing health tech companies. It starts with a claim we will defend throughout: a virtual CISO who has run security from inside a regulated organization delivers different outcomes than a consultant with an outside view, because they understand what a miscalculated decision costs in burned goodwill and they build controls around the workflows that make money rather than against them.

We then walk through three archetypes drawn from our work, with identifying details removed: an AI native health data platform selling into pharma and providers, a virtual first care provider carrying PHI at scale into institutional contracts and a clinical trial workflow platform whose every customer runs a formal vendor qualification program. Each faced a different version of the same problem. Each came out with security that closed deals instead of blocking them.

We close with the ceiling of this model, a virtual care company whose posture carried acquisition diligence this spring instead of surviving it, with a practical guide for evaluating any vCISO partner including us, and with the published pricing most firms will not show you.

Operators, Not Observers. | We Deliver Outcomes, Not Reports.

Who this paper is for

- Founders and CEOs of health tech companies whose enterprise deals keep stalling in security review
- COOs and heads of product who own compliance by default and would rather not
- Boards and investors who want to know whether the security spend is protecting the company or just the audit
- Internal security and IT leads who need executive weight behind them without losing ownership of their program

The Health Tech Security Problem

Health tech companies operate under a pressure that most software businesses never feel. Their buyers are among the most compliance mature organizations on earth and their data is among the most regulated. The result is a market where trust has to be proven before it can be earned.

Security is a sales gate, not a checkbox

A hospital system does not sign a Business Associate Agreement on a handshake. A payer does not connect a new vendor to member data on the strength of a slide deck. A pharma sponsor does not route clinical trial workflows through a platform it has not qualified. Every one of these buyers has a procurement and security review process, and every one of those processes has stalled a deal that the sales team thought was closed.

The ask varies by buyer. Health systems want HIPAA evidence and increasingly HITRUST. Enterprise software buyers want SOC 2 Type 2. Pharma and CROs run vendor qualification audits that go deeper than any questionnaire. Investors want to see that the security story survives diligence. What does not vary is the outcome when the answer is not ready: the deal waits, the quarter slips and the competitor with a clean report gets the meeting.

In health tech, the question is never whether you will be assessed. It is whether your posture is an answer or an objection when you are.

The data makes everything heavier

Protected health information changes the stakes on every decision. A misconfigured storage bucket is a breach notification event. A vendor without a BAA is a regulatory exposure. A model trained on data without documented consent is a problem that does not go away when the model is retrained. Add behavioral health records, substance use data or clinical trial financials and the regulatory surface expands again.

Health tech companies also tend to be data intensive by design. AI native platforms ingest clinical data from many sources. Care delivery platforms generate PHI with every visit. Workflow platforms sit in the middle of data flows between organizations that each have their own obligations. Security in this environment is not about protecting a perimeter. It is about knowing where data lives, who touches it and why, across every workflow that generates revenue.

AI has raised the bar again

Enterprise buyers now ask about AI governance alongside security and privacy. Health systems want to know how models are trained, what data they touch and who oversees them. Regulators are moving. Frameworks like NIST AI RMF and ISO 42001 are becoming the language of the conversation. For a health tech company already stretched across HIPAA, SOC 2 and HITRUST, this is a fourth program layered onto three, unless someone builds them as one.

The team is never big enough

Most growing health tech companies do not have a full time CISO and many should not. What they have is a CTO who owns security by default, a compliance manager who owns evidence collection by exhaustion and a founder who fields security questionnaires between fundraising calls. The program lives in a GRC platform that somebody configured once. Nobody owns the strategy and everybody owns the consequences.

Why Outside In Consulting Fails Here

The traditional consulting response to this problem is a gap assessment, a control framework and a remediation roadmap. It produces a report. The report is accurate, well formatted and rarely implemented. Here is why.

Frameworks before business

Most engagements start with a control catalog and work backward to the company. The result is a program that protects things that do not matter and misses things that do, because nobody mapped the revenue engine first. Which products generate cash? Which systems support them? What data flows through, and who touches it? That is the crown jewels list and everything else follows from it. Skip that step and you spend two years defending the wrong assets.

Reports are not outcomes

A findings document does not close a deal, pass a vendor audit or survive diligence. Outcomes do. The gap between a report and an outcome is operational execution: someone inside the organization who owns the roadmap, works the silos, coaches the control owners and makes the trade offs when engineering has a launch and compliance has a deadline in the same week. Outside in consultants deliver the report and leave. The outcome is somebody else's problem.

Burned goodwill is expensive

Security programs fail on politics more often than on technology. A control rolled out without understanding how the clinical operations team actually works gets bypassed within a month. A policy written for the auditor rather than the engineers gets ignored. A vCISO who has never made the tough call from inside an organization does not know what a miscalculated decision costs, or how long it takes to earn back the trust of a team that was steamrolled once.

What sitting in the seat teaches you

You learn that the product team will support security if security supports the launch. You learn that the clinical team will follow the process if the process was built with them. You learn that the board asks three questions and only one of them is about controls. And you learn that a program which inhibits the business gets defunded, no matter how well it scores.

Silos are the real attack surface

In health tech, security touches product, engineering, clinical operations, legal, privacy and sales. Each has its own priorities and its own language. A consultant who parachutes in talks to the security contact and leaves. An operator embeds across the silos, because that is where the data flows break and where the incidents start.

The Operator's vCISO Model

Every Steadfast vCISO has sat in the internal seat. They have owned the program, worked the silos and made the tough calls. That experience shapes a model built around four commitments.

1. Business assessment first

We do not start with a framework. We start with your business. The first engagement deliverable is a map of how your current workflows support your revenue streams, and from there, how data flows through them. Which customers pay you, for what, through which systems, touching which data, handled by which people. That map becomes the risk register, the control scope and the priority order for everything that follows. Compliance frameworks are mapped to it afterward, not the other way around.

2. Controls built with revenue in mind

Every control we design is tested against a simple question: does this protect the business without inhibiting it? Controls that slow down the workflows generating revenue are redesigned until they do not. Controls that exist only to satisfy an auditor are implemented at the minimum viable level and moved on from. The roadmap covers HIPAA, SOC 2, HITRUST and the ISO family where buyers demand them, but the sequence is driven by which deals each one unlocks.

3. Operational execution inside the organization

We sit operationally within your org. That means attending the engineering planning meeting, coaching the control owners, writing the policy in language the team will follow, preparing the evidence and managing the auditor. It means being the person the CEO calls when the enterprise

prospect sends a 300 question security questionnaire on a Friday. The work moves from plan to proof because someone is there to move it.

4. Trust earned, then extended

The first job is to earn the trust of your team, because a program the team does not trust does not survive. The second job is to help your organization become trusted in the markets it targets. Security posture becomes a sales asset: a clean report, a fast questionnaire turnaround, a confident answer in the diligence room. That is the outcome we are measured on.

Business Assessment | Controls With Revenue in Mind | Operational Execution | Trust Extended to Market

What this looks like in the first 90 days

Period	Focus
Weeks 1 to 4	Revenue workflow and data flow mapping. Interviews across product, engineering, clinical and sales. Crown jewels identified. Current posture assessed against what your buyers actually ask for.
Weeks 5 to 8	Prioritized roadmap sequenced by deal impact. Quick wins that unblock active opportunities shipped first. Policy set drafted with the teams who will live it.
Weeks 9 to 12	Operational cadence established. Control owners coached. Evidence collection designed into the workflow. Board and leadership reporting in place. Audit or certification path scoped and scheduled.

Three Archetypes in Practice

The engagements below are composites drawn from Steadfast client work in health tech. Names, locations, platforms and other identifying details have been removed. The shapes are real.

ARCHETYPE ONE**The AI Native Health Data Platform****The company**

A venture backed platform connecting clinical data suppliers, including providers and life sciences organizations, with pharma and research buyers. De-identification, consent management and AI driven matching are core to the product. No dedicated security leader.

The pressure

Every buyer on both sides of the platform demanded proof before integrating. Providers asked for HIPAA evidence and a BAA with teeth. Pharma buyers asked for SOC 2 and increasingly HITRUST. Enterprise prospects were adding AI governance questions to their vendor reviews. The founding team was answering questionnaires personally and deals were slipping a quarter at a time.

What we did

We started by mapping the data supply chain: which sources, under what consent, through what de-identification, to which buyers. That map exposed where the real risk lived, in consent lineage and re-identification controls, not in the perimeter. We built the security program around that flow, scoped SOC 2 to the systems buyers cared about and folded AI governance into the same control set rather than running it as a separate project.

What changed

Questionnaires went from weeks to days. The SOC 2 report landed clean and became the first attachment in every enterprise proposal. The AI governance narrative, backed by real controls, turned a buyer objection into a differentiator. Security stopped being the reason deals waited.

ARCHETYPE TWO**The Virtual First Care Provider****The company**

A multi state telehealth provider delivering clinical care through its own platform and pursuing institutional and payer contracts. PHI generated with every visit. A small operations team wearing the compliance hat alongside everything else.

The pressure

Institutional buyers required a designated security officer, a documented HIPAA program and evidence that the platform could handle patient data at contract scale. The organization had good instincts and no program. A GRC platform had been purchased and partially configured. Nobody owned it.

What we did

Our vCISO stepped into the designated security officer role and built the program around the clinical workflow, from intake through visit through billing. Policies were written with the clinical team, not handed to them. The GRC platform was reconfigured to match the program rather than the other way around, with task owners who had clear expectations instead of just logins.

What changed

The organization could answer institutional security requirements with a documented program and a named executive owner. Contract conversations that had stalled on security moved. The internal team kept ownership of day to day operations with a vCISO carrying the strategy and the accountability.

ARCHETYPE THREE**The Clinical Trial Workflow Platform****The company**

A B2B platform embedded in the operational and financial workflows of clinical trials, sitting between pharma sponsors, CROs and research sites. Because the platform moves money, financial controls stack on top of security controls. Small headcount, heavy counterparty expectations.

The pressure

Every major customer ran a formal vendor qualification program with audits, not just questionnaires. The company needed SOC 1 and SOC 2 running in parallel, with evidence that would hold up to sponsors whose own compliance teams are larger than the entire company. Prior audit work had left gaps and consumed internal hours the team did not have.

What we did

We took on the acting vCISO role and unified the SOC 1 and SOC 2 programs onto a single control set and evidence cycle. The GRC platform was expanded to carry both. Internal hours spent on audit support were quantified and returned to the team, and the engagement was structured so the business case for security spend was visible to the executive who approved it.

What changed

Vendor qualification audits from sponsors became a repeatable process instead of a scramble. Two reports came from one evidence set. The team got its time back. Security posture went from a cost the company absorbed to a capability the company sold.

The Ceiling: When Posture Carries Diligence

Every health tech company will eventually face a diligence process. A funding round, a strategic partnership or an acquisition. In that room, security posture is either an asset the deal team leans on or a liability the other side prices in.

This spring, a virtual care client's security posture carried acquisition diligence instead of surviving it. The acquirer's review found a documented program with a named owner, controls mapped to the workflows that generated revenue, clean audit history and an executive who could answer every question in the room without a follow up. Security was not a line item in the risk schedule. It was part of why the company was worth buying.

That outcome was not the result of a diligence prep sprint. It was the result of a program built the right way from the start, around the business, with someone in the seat who had done this before. The diligence room is where the operator's model pays out, but the payout is earned in the eighteen months before anyone books the meeting.

Diligence does not reward the company with the most controls. It rewards the company that can explain why it has the ones it does, and show that they work.

What diligence teams actually look for

- A named security owner with executive accountability, not a shared responsibility that belongs to nobody
- A risk register tied to the actual business, not a generic framework import
- Audit and certification history without unexplained exceptions or gaps between periods
- Evidence that incidents, when they happened, were handled and learned from
- Vendor and AI governance that shows the company knows what touches its data
- Someone who can answer the question in the room, not promise to get back to them

How to Evaluate a vCISO Partner

Not every vCISO offering is built the same way, and the differences matter more in health tech than anywhere else. Use these questions in any evaluation, including of Steadfast.

Ask	What a strong answer sounds like
Have your vCISOs held the internal role?	Yes, and they can tell you about a decision they got wrong from inside an organization and what it cost. Consultants who have only advised will describe frameworks.
What is the first deliverable?	A map of how our workflows support our revenue and where the data flows. If the answer is a gap assessment against a framework, the program will be built backward.
How do you handle a control that slows down the business?	We redesign it. A partner who says the business needs to adapt to the control has not sat in your seat.
Who owns the program between meetings?	We do, operationally, inside your organization. Beware of models where the vCISO shows up monthly and your team does the work in between.
How do you sequence frameworks?	By the deals each one unlocks. HIPAA, SOC 2, HITRUST and ISO are all real, but the order should follow your pipeline, not the partner's preference.

Ask	What a strong answer sounds like
How do you handle AI governance?	As part of the same control set, built on the privacy and data mapping work that already exists. A separate AI program with its own consultants is a red flag.
What happens in diligence?	The vCISO is in the room and answers the questions. If the partner's plan is to prepare a binder and step back, that is not the outcome you are paying for.
What does success look like?	Deals that stopped waiting on security. Questionnaires that take days instead of weeks. A diligence process the posture carried. Outcomes, not reports.

What It Costs

Most firms in this market quote after three calls. We publish. Pricing this clear is possible because the model is productized: named senior leaders, defined tiers and partner pricing on the platforms we operate.

Engagement	Published starting price
vCISO	From \$10,000 a month. A named senior security leader embedded in your company, owning risk, customer security reviews, AI governance and budget. Managed GRC included.
Managed GRC Essentials	From \$3,500 a month. A compliance operations manager runs one framework on one platform, readiness included, audit prep and liaison.
Managed GRC Professional	From \$6,000 a month. Two or more frameworks from one control set, full audit support, customer and diligence audits managed, vendor risk.
vGRC Build	Fixed fee, scoped on the call. GRC engineering that connects your compliance platform to cloud, identity, code and HR systems, with an evidence repo you own.
Ways to start	Platform Health Check, \$2,500 fixed and credited to month one of any tier. Security Program Assessment, \$7,500 to \$15,000 fixed.

Partner pricing is real money

A recent client audit landed at \$16,100 against a \$25,000 budget estimate. A third under estimate, credited to partner pricing on the platform and a program that was audit ready before the auditor arrived.

Audits run with your auditor of choice. Current pricing always lives at steadfastpartners.io/pricing.

About Steadfast Partners

Steadfast Partners is a cybersecurity and GRC advisory firm serving health tech, healthcare and other regulated industries. Our vCISOs are former internal security leaders who build programs around the workflows that drive revenue, sit operationally inside client organizations and measure themselves on outcomes. We work to earn our clients' trust first, then help them become trusted in the markets they are targeting.

Our approach rests on a simple promise: your success is our success, and we take that personally.

Let's talk about what you need. [Book a call](#). No pressure, just a conversation.

737-210-5503 | sales@steadfastpartners.io | www.steadfastpartners.io