



CHALLENGE 05

Treating Security, Governance, and Risk as Late-Stage Checkboxes

Part of the Provider-Informed Field Guide

Whose Lens Is Your Health IT Go-to-Market Strategy Built Through?

“Trust is not something you add to the sales process. Trust is part of what you are selling.”



Developed by David Hacker, CPHIMS | Director, Elevate HIT Sales | MEDDPICC® Certified Trainer

A practical chapter for Health IT founders, revenue leaders, and commercial teams selling to hospitals and health systems.

elevate-hit-sales.com



THE CORE IDEA

Trust Is Part of the Buying Decision

A Health IT company can generate strong clinical or operational interest and still lose momentum when the provider begins evaluating security, governance, privacy, integration, or organizational risk.

Hospitals and health systems are not simply deciding whether the technology works. They are deciding whether they can trust the technology, the vendor, and the organization behind it enough to introduce the solution into a complex healthcare environment.

Security review, AI governance, risk assessment, and technical diligence are not hurdles that appear after the “real” selling. For the provider, they are part of the buying decision.

In Health IT, trust is not something you add to the sales process. Trust is part of what you are selling.

SELLER’S LENS VS. BUYER’S LENS

Health IT companies often see security, governance, and risk review as technical approval steps that follow business interest. Providers see them as evidence of whether the organization can safely and responsibly adopt the solution.

SELLER’S LENS	BUYER’S LENS
“We can handle security review when we get there.” • Strong product performance • Enthusiastic clinical or operational users • Demonstrated value • Technical capabilities • Security questionnaires • Compliance documentation • Contracting requirements • An approval process that comes later in the deal	“Can we trust this solution and this company enough to bring them into our environment?” • What data will the solution access? • How is sensitive information protected? • What happens when something fails? • How mature is the vendor’s security program? • Who owns security and risk internally? • How is AI monitored after deployment? • What changes require provider notification? • How transparent will the vendor be when problems occur?
The provider is not only evaluating product risk. It is evaluating vendor risk.	



WHY THIS BECOMES A GTM PROBLEM

Business Enthusiasm Can Outrun Organizational Readiness

When security, governance, and risk are deferred until late in the sales process, the vendor may discover that business enthusiasm has advanced much faster than organizational readiness.

Operational Approval Creates False Confidence The business team says yes just as security and governance review begins.	The Questionnaire Becomes a Fire Drill Documentation is assembled reactively because the company was not prepared.
Security Ownership Is Unclear The provider cannot identify who owns cybersecurity and risk inside the vendor.	AI Governance Appears Late Questions about monitoring, data, oversight, and material changes surface late.
The Vendor Overstates Readiness Answers are optimized to pass review rather than acknowledge gaps and mitigation.	Surprises Reach Contracting Issues that could have been addressed earlier become late legal or commercial problems.
Security review does not interrupt the sale. It is part of the sale.	



PROVIDER PERSPECTIVE

What Provider and Standards Leaders Reinforce

GARY S. CHAN

Chief Information Security Officer, SSM Health

Security Readiness Builds Trust

Provider security teams are evaluating the risk introduced by both the technology and the vendor. Preparation, accountable security leadership, appropriate documentation, and transparent responses create a very different impression from a company discovering expectations during a live deal.

Prepare for provider security diligence before the first security questionnaire arrives.

[Hear the Conversation →](#)

SAM MORHAIM

Co-founder & Chief Innovation/Technology Officer, VantagelO

Hospital-Ready Is Different From Demo-Ready

An impressive demonstration does not automatically mean the technology is ready to operate inside a health system. Integration, architecture, workflow, reliability, and real-world failure conditions still matter.

Do not confuse technical capability with organizational readiness.

[Hear the Conversation →](#)

YASIR TARABICHI, MD, MSCR

Chief Health AI Officer, MetroHealth / Head of Digital & CMIO, Ovatient

AI Governance Does Not End at Approval

Providers need to understand how AI is governed, monitored, changed, and managed after deployment—not merely how the model performed during evaluation. Governance is an ongoing operating responsibility.

If the solution includes AI, be prepared to explain how it will be governed after it enters the provider environment.

[Hear the Conversation →](#)

RAM D. SRIRAM

Senior Science Advisor, Information Technology Laboratory, NIST

Trustworthy AI Requires Evidence

Confidence depends on more than performance claims. Decision-makers increasingly need evidence around uncertainty, measurement, monitoring, and how the system behaves when predictions are incomplete or wrong.

Trust increases when the vendor can explain both capability and the boundaries of that capability.

[Hear the Conversation →](#)



HOW TO DIAGNOSE SECURITY, GOVERNANCE & RISK READINESS

Prepare Before the Review Begins

Do not wait for a live deal to discover what healthcare organizations will ask. Understand your current maturity, document it honestly, and have a plan for known gaps.

- Documented security policies
- Independent assessments
- Penetration testing
- SOC 2 or other relevant certifications
- Privacy practices
- Incident-response procedures
- Data-flow documentation
- Business-continuity plans
- Clearly identified security ownership

Security readiness should be built before the sales process exposes the gaps.

Treat Vendor Security Culture as Part of the Product

Providers are evaluating more than the application. They are evaluating the company behind it: dedicated ownership, employee responsibility, proactive risk management, independent validation, incident handling, and transparency.

The provider is buying your organization's security maturity along with your technology.



HOW TO DIAGNOSE SECURITY, GOVERNANCE & RISK READINESS

Make Governance and Monitoring Explicit

This becomes especially important with AI. The provider may need to understand who governs the technology, how performance is monitored, how changes are communicated, what human oversight remains, and who is accountable when something goes wrong.

Approval answers whether the solution can enter the organization. Governance answers how it will remain there responsibly.

Be Clear About Risk, Limitations, and Failure Modes

Trust does not require pretending risk does not exist. A more credible conversation explains what could go wrong, how it would be detected, what controls reduce the risk, and what happens when the technology does not perform as expected.

For AI, that may include uncertainty, incomplete data, model error, workflow failure, or changing performance over time.

A provider can work with known risk. Unexpected risk discovered late is much harder to manage.

DIAGNOSTIC CONTENT — BOTTOM LINE

Security and governance readiness means giving the provider confidence that the technology, the vendor, and the risks surrounding both can be understood, managed, monitored, and trusted.



BETTER DISCOVERY QUESTIONS

Don't Ask / Ask Instead

Good risk discovery does not ask only how quickly the vendor can get through security review. It helps the vendor understand what the provider must know before it can confidently approve the solution.

DON'T ASK	ASK INSTEAD
"How long does your security review usually take?"	"What security and risk requirements should we understand early so we can prepare the right evidence before formal review begins?"
"Do you require SOC 2?"	"What evidence does your organization rely on to assess the security maturity of a technology vendor?"
"Once security approves us, are we done?"	"What ongoing governance, monitoring, reporting, or change-notification requirements will remain after deployment?"

The objective is not simply to pass the review. It is to understand what the provider needs in order to trust the solution and the vendor behind it.



CHECKLIST + BUYER’S-LENS TEST

From Product Interest to Organizational Trust

Before treating strong business interest as evidence of commercial readiness, the sales team should understand the security, governance, and risk requirements that could determine whether the provider can actually adopt the solution.

1. Questions Health IT Companies Should Be Able to Answer

• What provider data will the solution access? • What security controls protect that data? • Who owns cybersecurity and risk internally? • What independent security evidence is available? • What known gaps or limitations exist? • How are incidents identified and managed?	• What governance requirements apply after deployment? • How is product or AI performance monitored? • How are material changes communicated? • What happens when the technology behaves unexpectedly? • What responsibilities remain with the provider? • Can the company clearly explain its risk-mitigation plan?
---	--

If the sales team cannot explain how the provider’s risk will be managed, the opportunity is not yet commercially ready—regardless of how much the business users like the product.



THE BUYER'S-LENS TEST

Organizational Trust Should Pass Five Tests

A security- and governance-ready opportunity should allow the provider to answer “yes” to each of the following:

✓ **Yes, we understand the risk.**

The organization knows what the technology and vendor introduce into the environment.

✓ **Yes, the vendor demonstrates security maturity.**

There is evidence of ownership, controls, documentation, and responsible practices.

✓ **Yes, the limitations are transparent.**

The vendor can explain what the technology cannot guarantee and how risk is mitigated.

✓ **Yes, ongoing governance is defined.**

Monitoring, reporting, accountability, and change management continue after approval.

✓ **Yes, we trust the vendor to tell us when something changes.**

The relationship is built on transparency rather than surprises.

When those five answers are present, security and governance become evidence that the provider can trust the solution enough to move forward.

DAVID'S GTM TAKEAWAY

Health IT companies sometimes treat security, governance, and risk as obstacles that appear late in the buying process. Providers cannot afford to.

They are introducing technology into environments where patient care, sensitive information, operational continuity, reputation, and regulatory responsibilities may all be affected.

Prepare the evidence. Know the gaps. Understand the risks. Be transparent about what the technology can—and cannot—do.

In Health IT, trust is not something you add to the sales process. Trust is part of what you are selling.

Through the buyer's lens, the question is not simply “Does the technology work?” It is “Do we trust the technology and the company behind it enough to bring them into our organization?”



PART OF THE COMPLETE FIELD GUIDE

Whose Lens Is Your Health IT Go-to-Market Strategy Built Through?

Challenge 05 is one chapter in a 10-part provider-informed field guide examining the most common reasons promising Health IT companies struggle to move from initial interest to predictable revenue and scalable provider relationships.

The strongest Health IT go-to-market strategies are not built around how the vendor wants to sell. They are built around how the provider needs to buy.

01 Problem Importance	02 Pilot ≠ Commercial Validation
03 Payback Period	04 Workflow & Adoption
05 Security, Governance & Risk	06 The Buying Committee
07 Procurement, GPOs & Contracting	08 Policy, Standards & Interoperability
09 Scaling Sales Too Early	10 Pipeline vs. Commercial Readiness

[Explore the Complete Field Guide →](#)



ABOUT THE AUTHOR

David Hacker, CPHIMS

Director, Elevate HIT Sales | MEDDPICC® Certified Trainer

David Hacker brings more than 30 years of experience across healthcare delivery, Health IT, sales leadership, and go-to-market strategy. His provider-side and vendor-side experience shapes Elevate HIT Sales' practical approach to helping Health IT companies sell more effectively into complex healthcare organizations.

www.elevate-hit-sales.com

© 2026 Elevate HIT Sales. All rights reserved.