



WHITE PAPER · HEALTHCARE PAYMENTS

The Hidden Cost of PCI Compliance for Healthcare Organizations

When “compliant” doesn’t mean protected.

AUTHOR

Kevin Kidd

CEO AND FOUNDER, CRESORA COMMERCE

PUBLISHED

August 27, 2026

CRESORACOMMERCE.COM

Compliance is a continuous state, not an annual event

For many healthcare organizations, PCI compliance is treated as a burden overshadowed by HIPAA and the plethora of other regulatory regimes they must satisfy. Yet the data PCI governs sits directly alongside PHI, and deserves the same priority.

The payment systems used by complex healthcare organizations are typically far less understood than the clinical systems where PHI security is paramount. Given the sensitivity of the information governed by PCI, and how closely it is tied to PHI, payment infrastructure should sit higher on the leadership agenda than it usually does.

Unlike HIPAA compliance, PCI compliance is often handled as an annual milestone rather than an ongoing responsibility. The assessment is completed, the box is checked, and attention shifts elsewhere.

PCI compliance is not a one-time achievement earned through an annual assessment. It must be maintained and demonstrated continuously, because payment environments are constantly evolving; that is true of large, complex health systems and of smaller providers alike.

From a user's perspective these changes look routine. In practice they can fundamentally alter the environment that was originally assessed. Without ongoing oversight, organizations drift out of compliance and increase their exposure, all without realizing it.

WHAT QUIETLY CHANGES YOUR PAYMENT ENVIRONMENT

- New or updated collections software
- Newly deployed payment terminals
- Clinic and practice acquisitions
- Third-party collections partners
- New online payment channels
- Changed integrations and journeys

The pace of change is accelerating. AI adoption alone is driving process and technology shifts faster than most oversight programs can track.

The false comfort of “we are PCI compliant”

PCI provides a framework for protecting payment account data through ongoing technical, operational, and governance controls. It should never be reduced to a checklist; the focus belongs on the security of the data flowing through the systems, exactly as HIPAA requires.

PCI guidance demands an understanding of exactly where payment data lives, and the more complex the environment, the heavier that burden becomes. It is also essential to limiting the risk of a breach in your payment systems, one that could reach the systems holding PHI.

WHERE PATIENT PAYMENTS ARE ACCEPTED TODAY



Many organizations also run parking, retail, and other service businesses, taking payments in non-healthcare software applications, often managed by third parties on their behalf.

Today's healthcare payment ecosystems are far more complex than they once were. Organizations have expanded through acquisitions, grown outpatient networks, introduced digital payment options, and outsourced collections.

Every new channel, integration, or workflow adds another point where payment data must be understood, secured, and managed. Incrementally, these changes make it difficult to hold a complete and accurate view of payment operations.

THE AGGREGATION PROBLEM

Every vendor may be PCI compliant on its own. The aggregation of those solutions (the integrations, the data sharing, the hand-offs) can still create a vulnerability no single vendor owns, but for which your organization is responsible.

Seven questions every healthcare leader should be able to answer

Most healthcare organizations believe they have a compliant payment environment. Far fewer can confidently answer the following.

01

Are all payments handled through systems we are aware of?

And for which a compliance and security review has actually been completed.

02

Are all payment devices part of a currently validated P2PE solution?

Certifications go stale, and you could be running a solution that is no longer compliant.

03

Have software updates, gateway changes, or new integrations altered our PCI scope?

With many vendors in place, scope shifts quietly and often.

04

Do we have an accurate inventory of every payment terminal, in every location?

Including clinics and sites added through acquisition.

05

Do third-party vendors access our systems to handle payments?

And is there a structured compliance program overseeing their use of that technology?

06

Can we clearly explain how payment data moves across every channel?

End to end, from capture through settlement and reconciliation.

07

Who ultimately owns PCI oversight?

Across IT, finance, information security, and revenue cycle management.

None of these questions automatically indicates a compliance problem. But if leadership cannot answer them, it is far harder to demonstrate that the controls and scope reduction you believe are in place still hold.

Are you investing in PCI compliance, or paying PCI fees?

Compliance requires ongoing investment. Organizations dedicate substantial resources each year to HIPAA programs; PCI deserves the same discipline: programs, managed security services, payment technology, device maintenance, and internal compliance effort.

Those investments are necessary to protect sensitive payment environments, but they also create an expectation of measurable assurance. The challenge is that compliance spend alone does not guarantee continued protection.

Without effective governance and validation, organizations assume controls remain effective even as operational realities change. For many, that means assigning internal personnel to manage payment systems long left to vendors.

\$100

per MID, per month: what some processors charge once they determine an organization is no longer compliant.

WHAT REDUCES THAT EXPOSURE

- Proper management oversight of the payment estate
- Deliberate vendor selection and integration control
- A smaller footprint: fewer payment vendors and tools

The greatest risk is not simply having a compliance issue. It is discovering one only after an assessment, an audit, or a security event reveals that protections were never as effective as expected.

THE PRACTICAL TEST FOR A COMPLIANCE BUDGET

Ask whether each dollar buys assurance you can demonstrate (evidence of scope, device inventory, data flow, and vendor oversight), or whether it only preserves the ability to say the annual assessment was completed.

Poor visibility into payment infrastructure creates twice the risk

Limited visibility into payment infrastructure and PCI controls creates risk in two distinct ways.

RISK ONE

Gaps develop unnoticed

Outdated devices, unsupported software, configuration drift, or uncontrolled payment channels may remain undiscovered for long stretches, quietly increasing exposure across the environment.

RISK TWO

Response is slower when it matters

If an incident or cyberattack occurs, that same lack of visibility makes it hard to identify what was affected, contain the disruption, and restore operations quickly.

Consequences extend far beyond payment processing, disrupting patient access, eligibility verification, revenue cycle operations, cash flow, and other critical services. Organizations with limited visibility are both more likely to develop hidden compliance gaps and less prepared to respond when those gaps are exploited.

THE CONTINUITY QUESTION MOST ORGANIZATIONS HAVE NOT ASKED

Limited visibility usually means business continuity has not been considered either. If one vendor fails, or part of the payment estate is breached, can the organization still take a co-pay at registration or an estimated payment at intake? And if the RCM system is down, what does that mean for the provision of care?

Visibility is not a reporting nicety. It is the difference between an environment you can defend and one you can only describe after something has gone wrong.

PCI compliance should build confidence, not complexity

The solution isn't more annual assessments or more security fees. It is payment infrastructure that makes compliance easier and gives organizations the flexibility to evolve without losing control.

Healthcare organizations are complex and will remain so. A flexible payment platform that gives visibility into payment compliance is essential to maintaining compliance, reducing threats, and preserving flexibility in a dynamic environment. In practice, that means reducing dependence on rigid, single-threaded, processor-specific environments.

WHAT MODERN PAYMENT INFRASTRUCTURE SHOULD MAKE POSSIBLE

Modernize processes

Change how payments are taken and reconciled without rebuilding the entire ecosystem around a single processor.

Adopt validated security

Move to validated P2PE and tokenization technologies as certifications and standards evolve.

Integrate new channels

Add payment channels and respond to changing compliance requirements without a full re-platform.

Centralized reporting

One view of payment activity across every location, channel, and line of business.

Automated reconciliation

Less manual effort, fewer breaks, and stronger financial controls across the revenue cycle.

Integrated audit capability

Evidence of scope, data flow, and control effectiveness available continuously, not annually.

Ultimately, modern payment infrastructure shouldn't only support PCI and HIPAA compliance. It should improve operational resilience and protect care delivery by making payment infrastructure easier to understand, manage, and adapt as healthcare organizations continue to evolve.

The goal isn't simply to say you're compliant. Failing a PCI assessment isn't the biggest risk. It's believing you're compliant when your payment environment has already moved on, and being unaware of the resulting risk across your business.

NEXT STEP

Start with visibility. Everything else follows.

If your team cannot confidently answer the seven questions in this paper, the gap is not necessarily compliance; it is visibility. That is a solvable problem, and it is where Cresora starts.

01 · MAP

Build a complete inventory of payment channels, terminals, vendors, and integrations across every location and line of business.

02 · CONSOLIDATE

Reduce the payment footprint: fewer processors, fewer tools, fewer uncontrolled integrations to defend and evidence.

03 · MONITOR

Move from an annual assessment to continuous oversight, with centralized reporting, reconciliation, and audit evidence.



Kevin Kidd, CEO and Founder, Cresora Commerce

Cresora Commerce builds AI-native commerce infrastructure: embedded payment orchestration, automated workflows, and intelligent reconciliation for regulated environments.

TALK TO US

cresoracommerce.com

Request a payment environment review.

