PCI Pal + RingCentral

The Trusted Transaction Layer

Whitepaper

Overcoming the Healthcare Payments Catch-22:

Balancing Security, Compliance, and Patient & Member Payment Experience

pcipal.com

Executive Summary

Healthcare organizations face a payments problem that is costing them on practically every front: revenue, compliance, and patient trust.

Despite widespread digitization, 86% of healthcare payments still involve human interaction. Patients facing large, complex, or insurance-complicated bills need assistance. And that assisted payment moment is here to stay. But it is also where the risk lives. Every phone-based payment exposes sensitive card data, personal health information, and personally identifiable information (PII) to agents, call recordings, and disconnected systems — creating compliance exposure that most organizations have not yet fully addressed.

The scale of that exposure is significant. Healthcare has ranked as the most expensive industry for data breaches for 12 years running, with average incident costs now exceeding $7.4 million. At the same time, payment workflows have fragmented across contact centers, billing teams, clinics, and remote workers; expanding PCI scope and making continuous audit readiness increasingly difficult to achieve.

The financial stakes compound the problem. Rising deductibles have shifted more cost to patients, making collections a top-line revenue issue. Yet friction in the payment experience is driving abandonment, and 50% of patients say they would switch providers for a better payment experience.

The solution is not to eliminate assisted payments. It is to secure them at the source; removing card data from the environment at the moment of capture, without disrupting workflows or patient experience.



Healthcare has ranked as the most expensive industry for data breaches for 12 years running with average incident costs now exceeding

$7.4 Million

Why Healthcare Payments are Still Stubbornly Human — and Why That's a Challenge

Healthcare payments are stubbornly, necessarily human.

Unlike retail or banking, where digital self-service has become the default, healthcare payments resist full automation. Large unexpected bills, insurance complexity, and the sensitive nature of clinical conversations mean patients routinely need assistance to navigate and complete payments. Only 14% of healthcare payments are fully resolved through self-service channels. The other 86% involve human intervention.

That human element is not a design flaw, it's a feature. Assisted payment conversations drive collections, resolve disputes, and maintain patient trust. But they also create risks that most organizations have not fully accounted for.

Every assisted payment interaction is a potential exposure point. During these conversations, patients share:

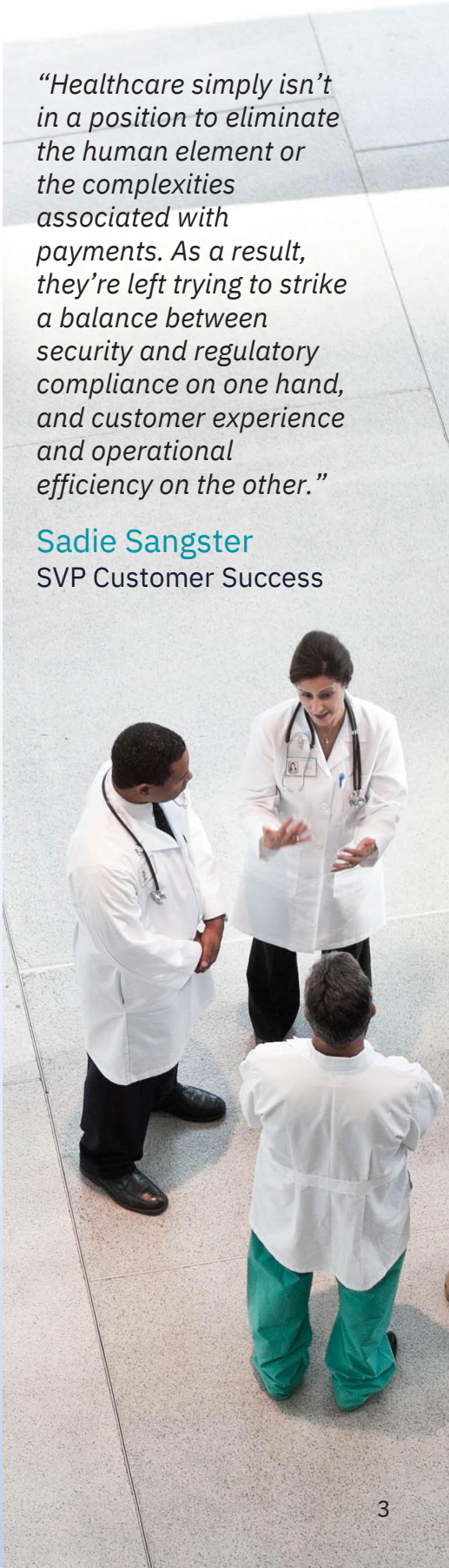
- Payment card data (PAN) — in scope for PCI DSS
- Personal health information (PHI) — in scope for HIPAA or NHS DSP requirements
- Personally identifiable information (PII) — subject to GDPR and broader data protection obligations

That data doesn't stay in one place, either. It moves widely, heard by agents, captured in call recordings, entered manually into systems, and processed across platforms that were never designed to handle it securely. And as payment activity has decentralized across billing departments, clinics, administrative staff, and remote workers, the number of exposure points has multiplied.

The result is an expanding attack surface that most organizations are managing reactively, if at all. This is occurring within a broader cybersecurity landscape that disproportionately impacts healthcare. According to IBM's Cost of a Data Breach Report, healthcare has experienced the highest average breach cost of any industry for over a decade, reaching approximately $10.9 million per breach in recent years.

"Healthcare simply isn't in a position to eliminate the human element or the complexities associated with payments. As a result, they're left trying to strike a balance between security and regulatory compliance on one hand, and customer experience and operational efficiency on the other."

Sadie Sangster
SVP Customer Success



PCI Pal™ + RingCentral®

And there's no reason to believe this trend will go away in the foreseeable future. Healthcare organizations are prime targets for cybercriminals for precisely the same reason operations are so sensitive: the exceptionally high volume of personal, financial, and clinical data they retain.

The Payment Experience is the Patient Experience

For most patients, the payment interaction is the last impression a healthcare provider leaves. And, increasingly, it is the one that determines whether they come back.

The data is clear. 56% of patients say they would likely switch providers after a poor billing experience, and nearly 90% of patients who switched providers in the past year did so because the organization was hard to do business with. Even if the clinical experience is excellent, patient satisfaction and loyalty can be severely undermined if the payment process is confusing, slow, or cumbersome.

Meanwhile, thanks to new standards set by sectors such as retail and banking, what constitutes a satisfactory payment experience has evolved significantly. 62% of consumers now prefer to pay their medical bills online, yet 74% are still receiving bills via traditional mail. This gap between what patients expect and what providers deliver is directly driving dissatisfaction and attrition.

The financial implications compound further when payments are delayed. 71% of providers report it takes over 30 days to collect payments after a patient encounter, which is a gap that grows harder to close the longer it remains open. Friction at the payment moment is not just a patient experience problem, it's a collections problem.

The solution is not simply digitizing the bill. It is removing friction from the entire payment interaction; whether that occurs through a self-service portal, a secure payment link, or an assisted phone conversation. A smooth payment process directly influences patient satisfaction and loyalty. Patients are more likely to return to a provider who offers convenient and stress-free billing experiences.

56%

of patients say they would likely switch providers after a poor billing experience.

Fragmented Payments, Expanding Risk

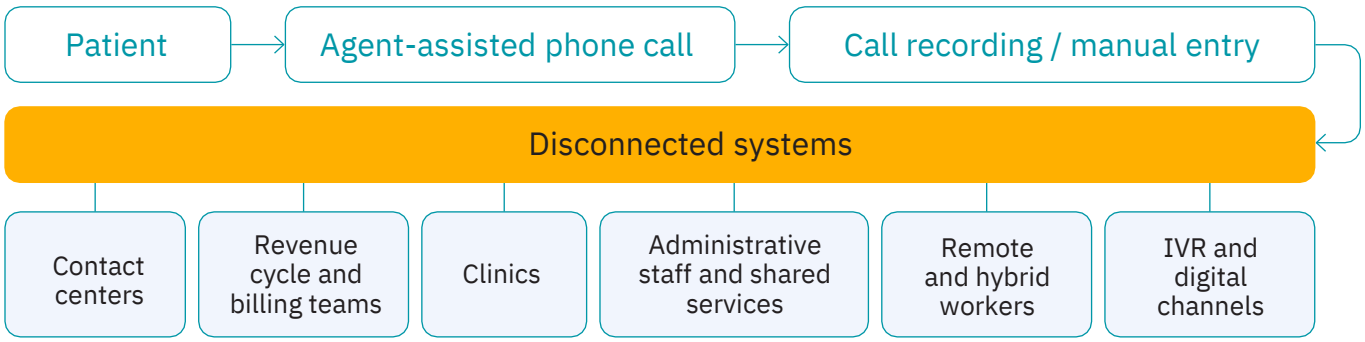
Modern healthcare payments don't flow through a single system. They move across electronic health records, billing platforms, telephony environments, and administrative workflows — often entering the organization through a live phone conversation before passing through systems that were never designed to handle payment data securely.

The result is cardholder data that is difficult to track, harder to control, and exposed at multiple points along the way: heard by agents, captured in call recordings, entered manually into disconnected systems, and processed across distributed teams spanning contact centers, clinics, billing departments, and remote workers.

Each of those touchpoints expands PCI scope. And expanded scope means greater compliance complexity, larger audit footprints, slower reconciliation, and higher operational cost. Staff are forced to navigate multiple tools in a single interaction, extending handling times and reducing efficiency. Patients, meanwhile, experience the friction directly as they're redirected between channels, asked to call back, and left with unresolved balances. Nearly a third of healthcare organizations that have experienced a breach have raised the cost of goods and services by 15% or more to offset losses. This results in a downstream consequence that ultimately lands on the patients themselves.

This fragmentation isn't just a compliance problem. It's also a patient experience problem, a revenue problem, and increasingly, a brand problem.

The Flow of Sensitive Information Across Fragmented Payment Environments



The Regulatory Stakes Have Never Been Higher

The compliance landscape surrounding healthcare payments has become significantly more complex, and the consequences of falling short more severe.

Organizations must now navigate a web of overlapping frameworks: PCI DSS v4.0 for payment data, HIPAA for health information in the United States, GDPR and NHS DSP Toolkit requirements in the United Kingdom, and SOC 2 as a baseline expectation in enterprise procurement. Each framework demands that organizations demonstrate active control over how sensitive data is handled, minimized, and protected. And not just at a point in time, but continuously.

The numbers behind non-compliance are sobering. In 2024 alone, the protected health information of more than 275 million Americans was exposed or stolen — more than 63% greater than the year before. In 2025, healthcare topped IBM's breach cost league table for the twelfth consecutive year, averaging $7.42 million per incident. And the damage extends well beyond the bottom line. Breaches can make headlines and tarnish a brand for years, impacting patient acquisition and retention.

This last point deserves emphasis. In healthcare, trust is not a soft metric. It is a business-critical asset. A breach can expose private patient information, cause delays and disruptions to care, and result in declining loyalty and satisfaction — effects on provider-patient relationships that can linger for years after the breach itself has been resolved.

For organizations navigating fragmented payment environments, the question is no longer whether compliance is important. It is whether their current approach to payment security is sufficient to protect not just their data — but their reputation.

Quantifying Cyber Risk in Healthcare Environments

Healthcare remains the number one target for cybercriminals of any industry

276 Million

people's protected health information was exposed or stolen in 2024 alone (more than double that of 2023)

$7.42M

per breach marked the highest average incident cost in healthcare in 2025, the 12th year in a row

92%

of healthcare providers rank cybersecurity as a high priority for their organization

Revenue, Collections, and the Cost of Friction

Compliance may be the most visible driver of payment modernization, but it is not the only one. For most healthcare organizations, the more immediate pressure is financial.

In the United States, rising deductibles have fundamentally shifted the collections equation. Patient collections have become the primary revenue concern for providers, a figure that has increased 133% from 2011 to 2024. Yet the infrastructure for capturing those payments has not kept pace. 71% of providers report it takes over 30 days to collect payments after a patient encounter, and the wider this window gets, the likelihood of recovery declines.

In the UK, the rapid growth of private and self-pay models is creating parallel pressure. As more patients take on direct financial responsibility for their care, the payment experience itself becomes a defining moment in the provider relationship.

Patient expectations have shifted dramatically. As consumers embrace digital wallets and online bill pay, healthcare providers must modernize their payment and communication systems to match expectations in other sectors, or risk losing patient satisfaction and loyalty. The stakes of failing to do so are concrete: Over 50% of patients say that poor payment experiences would motivate them to switch providers, while 72% of those under the age of 35 say they would switch providers, or already have, for a better payment experience.

These are not abstract loyalty metrics. Every abandoned payment, every frustrated patient, every bill left unresolved is both a revenue loss and a relationship loss. And in a market where patient acquisition costs are rising, retaining patients through a better payment experience is one of the highest-return investments a healthcare organization can make.

Operational complexity only makes these challenges all the more difficult. Healthcare organizations must now manage payments across distributed teams, remote workers, and multiple communication platforms. Ensuring consistency, efficiency, and compliance in such an environment is no small feat, no matter how mature the organization.



"Healthcare costs are skyrocketing, and insurance companies are shifting more of those costs onto the consumer. This means collections is becoming a top-line issue for providers struggling to maintain revenue. In such an environment, organizations quite literally can't afford unnecessary friction at the point of payment."

Sadie Sangster
SVP Customer Success

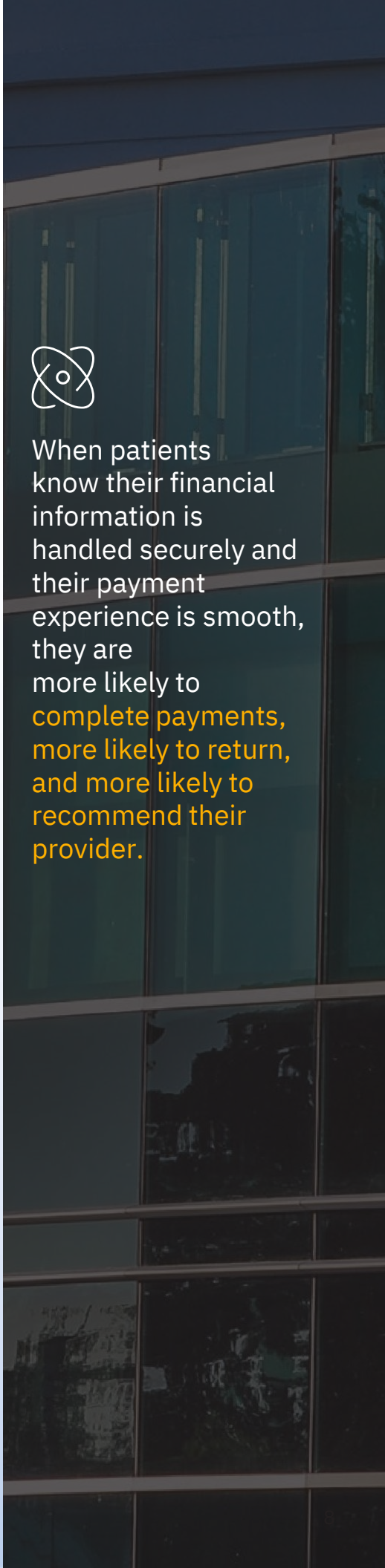
The end result is a game of spinning plates. Organizations must secure payment data, maintain positive human interaction, improve collections, and reduce operational burdens; all at the same time. Traditional approaches are simply no longer enough to make this balancing act feasible.

The Path Forward: Securing the Payment Moment

The solution to healthcare's payment challenge is not to remove the human element. It is not to consolidate all payments into a single digital channel. And it is not to undertake a costly overhaul of existing systems. It is to secure the moment at which payment data is captured; and to do so in a way that reduces risk without disrupting the workflows, patient relationships, or revenue performance that organizations depend on.

By removing cardholder data from the environment at the point of capture, organizations can dramatically reduce PCI scope, simplify compliance, and eliminate the exposure that fragmented workflows create. Payments can occur across any channel (e.g., contact centers, billing teams, clinics, remote workers) without sensitive data entering internal systems, call recordings, or staff workflows. What's more, all this happens without disrupting or complicating or altering the patient and agent experience.

Critically, this approach also protects something less easily quantified but equally important: patient trust. When patients know their financial information is handled securely and their payment experience is smooth, they are more likely to complete payments, more likely to return, and more likely to recommend their provider. A smooth payment process directly influences patient satisfaction and loyalty — patients are more likely to return to a provider who offers convenient and stress-free billing experiences. In a market where experience increasingly drives loyalty, payment security and patient satisfaction are two sides of the same coin.



When patients know their financial information is handled securely and their payment experience is smooth, they are more likely to complete payments, more likely to return, and more likely to recommend their provider.

PCI Pal™ + RingCentral®

How PCI Pal Helps Healthcare Organizations

PCI Pal is built for the realities of modern healthcare payments: distributed, complex, and resistant to full digitization.

Rather than attempting to control every system or secure every workflow, PCI Pal protects the organization's environment from interacting with cardholder data at the moment of capture. Sensitive payment information is never heard by agents, captured in recordings, or stored in internal systems. As a result, organizations can eliminate the exposure that fragmented environments create and significantly reduce PCI scope.

Critically, this is achieved without disruption. PCI Pal integrates directly into existing telephony platforms, UCaaS and CCaaS environments, billing systems, payment gateways, and EHRs including Epic. This way, organizations enhance security without replacing infrastructure.

While the vast majority of healthcare payments continue to depend upon human assistance, increased digitization and automation are slowly gaining ground. Whether replacing or integrating automated and self-service processes into their payments workflow, organizations can rely on PCI Pal to deliver the very same benefits as they do through their live payment channels (e.g. digital chat, over-the-phone).

Meanwhile, for patients, PCI Pal enables flexible, intuitive payment options: voice, keypad, or secure digital link, all within the flow of the existing interaction. Friction is reduced, completion rates improve, and the payment moment becomes a positive touchpoint rather than a source of frustration.

For the organization, the benefits compound: earlier revenue capture, reduced reliance on third-party collections, lower compliance cost, and a stronger foundation for patient trust and long-term loyalty.

Case Study

Real-World Example

A real-world example of this illustrates the true impact of PCI Pal's solutions. NFP Health, which operates multiple health insurance exchanges in the United States, faced growing PCI audit pressure as payment volumes increased and operations expanded to a remote workforce.

By implementing PCI Pal within its existing communications platform, the organization was able to keep payment card data out of its environment while maintaining uninterrupted collections. The result was reduced risk, improved operational efficiency, and a better member experience.

+ RingCentral®

Turning Healthcare Payments from Liability to Competitive Advantage

Healthcare payments have moved from back-office function to front-line strategic priority. The organizations that recognize this shift (and act on it) will be better positioned on every dimension that matters: financial performance, regulatory readiness, operational efficiency, and patient loyalty.

Those that continue to rely on fragmented, unsecured payment workflows face a compounding set of risks. Compliance costs will rise. Revenue will leak. And in an era where patients hold providers to the same standard as retailers and banks, a poor payment experience will increasingly cost organizations not just a transaction, but a relationship.

Payment security, done right, is no longer just about protecting data. It is about protecting trust — and turning a moment of financial vulnerability into a moment that reinforces why patients chose you in the first place.

Contact PCI Pal Today

Make security and compliance healthcare payments effortless for you and your patients both. PCI Pal integrates into existing telephony, CCaaS, UCaaS, EHR (including Epic), billing, and payment gateway environments. This allows healthcare organizations to secure payments without disrupting existing workflows or overhauling core systems.

PCI Pal

pcipal.com → info@pcipal.com →

Drop the balancing act. Reduce complexity, compliance risk, and customer friction in one fell swoop.

Get in touch with PCI Pal today:

Contact us →