EBOOK

Payment Security Pitfalls: How Some Payment Systems Still Risk Data

Beyond the Checkmark: Why SOC 2 Type II Attestation with HIPAA/ HITECH Scope Is Critical for Secure, Compliant Payment Approaches

pcipal.com

PCI Pal™

Executive Summary

Payment security is now a board-level issue shaping procurement decisions, brand trust, and an organization's ability to scale. Yet some organizations continue to rely on certain legacy implementations that satisfy compliance on paper while still leaving agents, infrastructure, and data exposed. According to the HIPAA Journal's 2024 Healthcare Data Breach Report, 275 million healthcare records were exposed, stolen or impermissibly disclosed in 2024, equivalent to 82% of the US population by record volume.

The gap this report addresses is not between compliant and non-compliant systems. It's between systems that achieve compliance through procedural controls, and those designed so that sensitive data never enters the contact center environment at all. Architecture, not compliance status alone, is what separates genuinely secure payment systems from ones that only appear secure.

Best-in-class vendors maintain PCI DSS validation and SOC 2 Type II attestation with HIPAA/HITECH scope, providing independent evidence that controls support covered entities' HIPAA compliance requirements. Together, they validate not just the payment transaction but the full operational environment: security, availability, processing integrity, confidentiality, and privacy. This independently evidenced posture transforms vendor selection from a compliance checkbox into a strategic trust decision.

When architecture and independent assurance align, the benefits extend beyond risk reduction. Secure-by-design solutions (using DTMF masking, tokenization, and secure IVR) keep card data out of agent reach, reduce compliance scope, support accessibility, and improve the customer payment experience. Security and experience are not competing priorities. The right system delivers both.

275M

Healthcare records exposed, stolen or impermissibly disclosed in 2024.

- HIPAA Journal's 2024 Healthcare Data Breach Report

Compliance is now a trust conversation

Payment security now spans legal, procurement, IT, customer operations, and brand reputation, particularly in healthcare, where HIPAA and HITECH requirements intersect with everyday payment handling. Security and compliance decisions directly affect an organization's legal standing, buying relationships, and ability to scale.

Modern buyers have moved past surface-level claims and compliance labels. They expect independent evidence. The evaluation centers on three things: **assurance** (independently validated controls), **architecture** (how data flows and where it can be captured), and **operational reality** (what actually happens in practice). Vendors who can demonstrate all three — with an unqualified SOC 2 Type II attestation with HIPAA/HITECH Attestation — transform the conversation from audit compliance to strategic partnership.

Assurance

Independently validated controls

Architecture

How data flows and where it can be captured

Operational reality

What actually happens in practice

Vendors who can demonstrate all three transform the conversation from audit compliance to strategic partnership.

Why “compliant” does not always mean low risk

A narrow compliance focus (for example, ensuring call recordings are clean) can leave agents, desktops, telephony, and back-end workflows still exposed or in scope. The real question for decision-makers is not “Is this compliant?” but “Where does sensitive data actually go?”

It is this analysis of data flow and access control that reveals the meaningful differences between vendors. A system that relies on agent discipline to manage risk is architecturally weaker than one designed to remove sensitive data from the environment entirely, regardless of what either claims on a compliance form.



Where legacy approaches fall short

Manual pause-and-resume recording is widely used in contact centers to meet compliance standards. In practice, it creates more risk than it resolves.

The pause doesn't protect what you think

Depending on the underlying telephony and recording architecture in use, there are instances where even when pause-and-resume is active, sensitive data (full PANs, cardholder names, CVVs) can persist in memory buffers, logs, or intermediate storage layers. An attacker exploiting a separate vulnerability during that window can still exfiltrate the data the pause was meant to protect.

Human behavior is not a reliable control

Agents forget to pause before a customer reads their card number. They resume too early. A fatigued, distracted, or disgruntled employee can bypass the mechanism — deliberately or by accident. The result: an organization that is technically "compliant" on paper but operationally exposed.

The compliance burden doesn't shrink

At best, pause-and-resume keeps recordings clean. Agents and underlying infrastructure still remain in PCI DSS scope, with ongoing implications for broader frameworks such as SOC 2 Type II attestation and HIPAA compliance obligations — a burden made significantly harder in remote work settings.

Legacy approaches succeed in removing one visible risk: card data in a recording file, while still preserving many hidden ones. One major UK motor insurer found **20–30% of phone payments were failing at first attempt. After switching to PCI Pal Key to Pay, allowing customers to key payment details directly while the agent remained on the call, drop-out fell to just 1–2%.**

No card data entered the infrastructure. No agent heard or saw the details. PCI DSS scope was reduced.



Major UK motor insurer found:

98-99%

payment completion rates achieved after implementing PCI Pal Key to Pay

Why SOC 2 Type II Attestation with HIPAA/HITECH Scope Matters Beyond the Transaction

PCI DSS is the foundation. That secures the payment event itself. But it addresses only one dimension of a complete security posture for high-stakes verticals. SOC 2 Type II attestation with HIPAA/HITECH scope goes further by examining the full operational environment against the five Trust Services Criteria: **Security, Availability, Processing Integrity, Confidentiality, and Privacy.**

SOC 2 Type II attestation is independently verified evidence that a vendor's systems are thoughtfully designed, formally documented, and consistently operated. It demonstrates continuous operational excellence maintained over the entirety of the defined audit timeline, not just a compliance snapshot. The inclusion of HIPAA/HITECH Attestation within the SOC 2 scope provides independent evidence that a vendor's controls are designed and operating effectively to support HIPAA compliance requirements.

For buyers, this combination transforms vendor evaluation. It moves the discussion past feature parity and compliance checklists toward independently evidenced, operational trust. For vendors, it is a genuine differentiator, one that is hard-won and difficult to replicate.

Five Trust Services Criteria

Security
Availability
Confidentiality
Privacy
Processing Integrity

Reducing exposure by design

The most robust approach to payment security keeps sensitive data from the contact center environment rather than trying to control what happens to it once it arrives.

This is descoping by design.

Payment Link / Secure Form

For non-voice channels, the agent sends the customer a unique, time-sensitive link to a secure, externally hosted payment form. No card data touches internal systems.

DTMF Masking

This technology protects card information by intercepting keypad tones during phone payments. The agent hears silence or a flat tone, not the customer's card number, while the masked data stream is transmitted securely to the payment gateway. No card details are heard, seen, or stored within the contact center.

Tokenization

Sensitive card data is replaced immediately at capture with a non-sensitive token. Useless to an attacker, but functional internally for refunds and transaction tracking.

Secure IVR

When a payment is initiated, the call transfers to an external, validated payment gateway before the customer enters their details. Card data is captured and transmitted directly to the payment processor without passing through agent or recording systems. The agent receives only a token or confirmation.

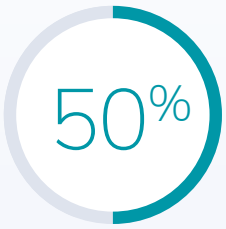
Together, these technologies are engineered to restrict cardholder data access from agents and internal systems during standard operations. The compliance footprint shrinks, the audit scope reduces, and the organization is protected against both external attacks and insider threats.



Security should also improve accessibility and experience

In their 2024 Trends in Healthcare Payments Report, J.P. Morgan found that 50% of consumers would switch providers, or already have, for a better healthcare payments experience — making it clear that friction in the payment journey has direct commercial consequences. The good news: secure-by-design systems do not create friction, they reduce it.

Solutions that let customers choose to key or speak their payment details, while keeping the agent present and helpful but unable to access the data, support accessibility for users with physical limitations, reduce call abandonment, and maintain service continuity. The agent experience improves too: agents are relieved of the burden of handling sensitive data and the compliance pressure that comes with it.



of consumers would switch providers, or already have, for a better healthcare payments experience.

- J.P. Morgan Healthcare Payments, Trends in Healthcare Payments: Fifteenth Annual Report, 2024.



What decision-makers should ask

Any vendor evaluation should go beyond compliance claims to examine assurance, architecture, and operational reality. Key questions:

01.

What independent assurance does the provider hold? PCI DSS validation? SOC 2 Type II attestation with HIPAA/HITECH attestation?

02.

What happens to sensitive data during collection? Does it enter your infrastructure?

03.

Can agents hear, see, or access payment details at any point?

04.

Can call recordings, desktops, or internal systems capture card data?

05.

How much of the environment remains in PCI scope after implementation?

06.

Does the solution support all channels and customer preferences you actually use?

07.

How does it integrate with your telephony, CCaaS, payment, and desktop stack?

Compliance should build trust, not friction

The most effective payment strategy keeps sensitive card data out of agents' reach, out of call recordings, and out of internal systems, supports customer choice across channels, and is backed by a transparent, independently evidenced security posture. Not all compliant payment approaches are built the same. The best ones do more than satisfy an audit. They help organizations build trust.

About PCI Pal: Supporting Covered Entities' HIPAA Compliance

PCI Pal enables secure, compliant payment capture across voice, digital, and AI-powered interactions. Cardholder data is protected from exposure that can put compliance at risk. Built to fit your existing environment, PCI Pal integrates seamlessly into your existing healthcare ecosystem, minimizing disruption while strengthening security across your workflow.

From complexity to control, see how PCI Pal tackles healthcare payment challenges.

Book a demo →

PCI Pal™

Discover the PCI Pal Trust Center

Explore **PCI Pal's Trust Center** to review our security posture and compliance credentials, or speak with our team about how to create a secure payment experience that reduces exposure and supports your customer journey.

Explore PCI Pal's Trust Center →

pcipal.com → info@pcipal.com →