Klizer
by DCKAP

# Navigating the **Payment Challenges** in the **Healthcare** Industry

copyright@klizer.com

info@klizer.com

The finances in the healthcare industry are more complicated than ever. The idea of convenience with digital payments is driving businesses and patients to adopt digital payments more than ever. However, healthcare organizations, including doctors, insurance companies, and suppliers, face unique challenges.

They need to optimize their patient care ecosystem for best-in-class services while handling complex financial tasks under strict regulations. Traditional paper-based payment systems don't cut it anymore as they not only rely on manual labor, which is prone to more errors, but also complicate things, are time-consuming, and take energy away from patient care.

Payment gateways are the solution to all this. They help handle electronic payments safely and efficiently, whether dealing with patients (B2C) or their businesses paying each other (B2B). In this eBook, we are digging deep into each of the challenges associated with payments in healthcare commerce and how having the right technology partner beside you can help organizations deal with it better.

## Solving Healthcare Payment Challenges

While payment processing is a challenging area for every industry, it's even more tricky for the healthcare businesses. Besides technological challenges like online fraud, interaction with legacy systems, and more, the industry is riddled with strict regulations. Here's what these various challenges look like.

## Challenge 1: Managing HIPAA and PCI DSS compliance

Healthcare businesses need to comply with dual compliance requirements:

- **HIPAA (Health Insurance Portability and Accountability Act), enforced by the Office of Civil Rights (OCR),** protects patient health information (PHI), covering anything that connects a patient to their medical care or billing. It applies to providers, insurance companies, and vendors handling PHI.
- **PCI DSS (Payment Card Industry Data Security Standard)** is enforced by the card networks such as Visa and Mastercard. It secures cardholders' data, like credit card numbers and security codes, during transactions. It applies to any organization that processes or stores card data.

# HIPAA vs. PCI DSS

| Feature | HIPAA | PCI DSS |
|---|---|---|
| Main Purpose | Protects patient privacy and health information | Protects credit/debit card information during payment |
| Data Covered | Patient health records and billing details (PHI) | Cardholder data like card numbers and security codes |
| Who Must Follow It | Doctors, hospitals, insurers, and vendors who handle patient data | Any business that handles card payments, regardless of size |
| Who Enforces It | U.S. Dept. of Health & Human Services (HHS) / Office for Civil Rights | Payment card companies and the PCI Security Standards Council |
| How It's Verified | No official certification; compliance is ongoing; random audits are possible | Self-checks or formal audits, regular security scans may be required |
| Penalties | Fines up to $50,000 per violation, required changes, official monitoring | Monthly fines, higher processing fees, or losing the ability to take cards |

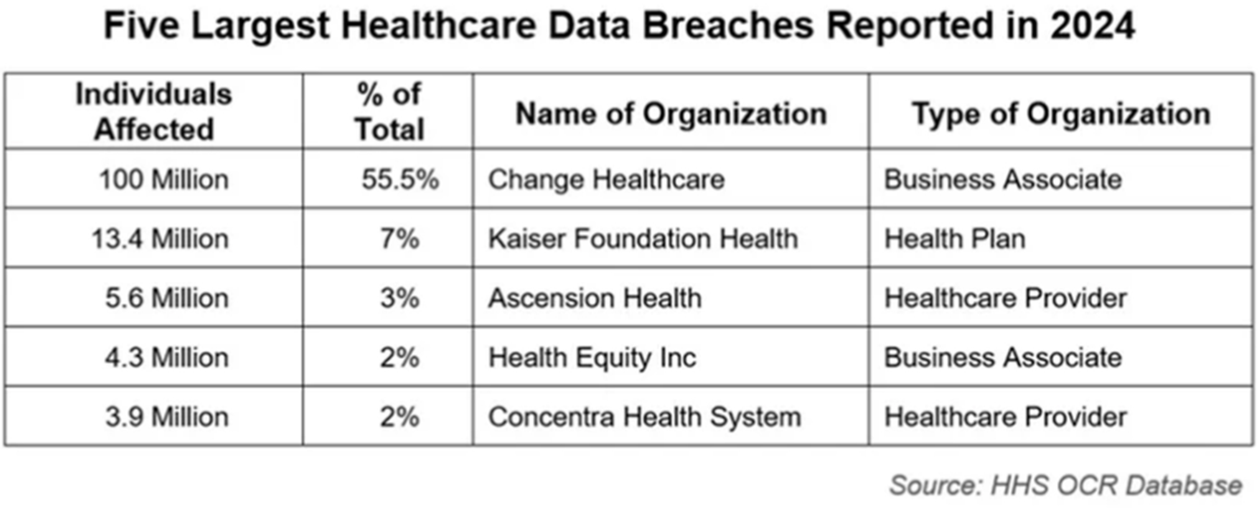
Healthcare payment combines both PHI and payment card data in a single transaction, which is what creates the compliance challenges. Healthcare software such as EHRs, EMRs, billing platforms, etc., must be fully secured to manage payments and share data without violating either of the compliance standards.

Healthcare IT infrastructure is often built on legacy systems, making it difficult to meet key PCI DSS requirements, like network segmentation. To add to it, the healthcare regulatory standards are advancing at such a pace that it's tougher for brands to keep track. For example, the PCI DSS 4.0 update, with 64 new requirements, was supposed to be applied to all systems by 31 March 2025.

## The Cost of Non-Compliance

The cost of falling short of complying with these standards is extremely high.

- In 2024 alone, **180 million healthcare records** were breached (Source).
- The **average cost of a healthcare data breach** reached **$10.93** million, more than double the cross-industry average (Source).
- OCR has issued over **$143 million in HIPAA fines,** including a record $16 million penalty to Anthem Inc. (Source)
- PCI DSS non-compliance can result in fines between **$5,000–$100,000 per month,** in addition to legal fees, card reissuance costs, and even the loss of card processing privileges (Source).



**Five Largest Healthcare Data Breaches Reported in 2024**

| Individuals Affected | % of Total | Name of Organization | Type of Organization |
|---|---|---|---|
| 100 Million | 55.5% | Change Healthcare | Business Associate |
| 13.4 Million | 7% | Kaiser Foundation Health | Health Plan |
| 5.6 Million | 3% | Ascension Health | Healthcare Provider |
| 4.3 Million | 2% | Health Equity Inc | Business Associate |
| 3.9 Million | 2% | Concentra Health System | Healthcare Provider |

*Source: HHS OCR Database*

**Continuous Compliance and Staff Training are Essential**
With constantly advancing regulatory standards and cyber threats increasing, just having an annual checklist for compliance isn't enough.

Healthcare organizations need a proactive and ongoing approach. PCI DSS 4.0 emphasizes constant and continuous monitoring to mitigate any security threats.

Additionally, human error is one of the weakest links in such issues. Lack of staff training, resistance to change, and accidental data handling are some of the most common causes of data breaches. That's why having the following as part

- Comprehensive staff training
- Clear security policies
- Easy-to-follow workflows that check secure behavior at each step

## Challenge 2: Fighting Healthcare Payment Fraud

Healthcare payment fraud is one of the major challenges that is draining money from the ecosystem. Estimates show that payment fraud makes between 3% and 10% of healthcare spending, which means tens or even hundreds of billions of dollars every year (Source). Since 1987, over USD 54 billion has been recovered from healthcare fraud in the US. (Source).

- **Fake services:** Billing for services that were never provided or adding extra, unnecessary services to legitimate claims.
- **Upcoding:** Changing for services to a higher cost compared to what was done
- **Unnecessary tests:** Performing tests or procedures just to receive the insurance payments.
- **Misleading claims:** Claiming non-covered services, such as cosmetic procedures, as medically necessary
- **Identity Theft:** Stealing information and using it to submit fake claims
- **Payment Fraud:** Targeting weak payment systems, like check fraud or breaking into online payment gateways

Payment fraud not only causes financial loss but also harms patients by adding unnecessary diagnoses to their medical records. This false information impacts their future care and adversely impacts their medical insurance eligibility.

These cases also lead to higher insurance costs for everyone and can damage the reputation of healthcare providers. According to **market reports,** the financial loss from fraud cases can range from $100,000 to millions.

## Challenge 3: Traditional Manual Processes & Paper Chains

It is needless to say that the healthcare industry is overdependent on traditional paper-based manual processes for invoicing and payments. Studies have shown that over 85% of healthcare procurement is still paper-based, where 70% of the suppliers are still sending invoices via mail or email. Adding to the issue, most of half of the healthcare organizations are paying these suppliers via check (Source).

Let's talk about what this is costing the healthcare industry overall. The losses of these paper-based payment communications are estimated at $22 billion. Breaking it down further, each manual invoice or paper check costs up to $31, and each transaction takes about 9 minutes longer than a digital transaction. Which means that besides the direct costs, physicians spend over 20 hours a week on paperwork and invoice approvals (Source).

All this aside, manual processes are always susceptible to erroneous payments, invoicing errors, and payment delays. This all impacts the cash flow, making it difficult for healthcare stakeholders to ensure financial stability.

Payment fraud not only causes financial loss but also harms patients by adding unnecessary diagnoses to their medical records. This false information impacts their future care and adversely impacts their medical insurance eligibility.

These cases also lead to higher insurance costs for everyone and can damage the reputation of healthcare providers. According to market reports, the financial loss from fraud cases can range from $100,000 to millions.

The risk of fraud is also higher because healthcare organizations rely on third-party vendors for things like billing, payment processing, and IT support. The first step is to ensure that all this software is backed by strong data policies and security standards.

Healthcare organizations are tackling these issues with AI and data analytics. By having these technology systems in place, companies can spot suspicious activities in real-time and mitigate the fraud risk altogether.

## Tackling Healthcare Payment Fraud Head-On

### WHO

**Is behind healthcare payment fraud?**

Fraud can originate from a range of sources, including billing departments, third-party vendors, providers, or even cybercriminals targeting vulnerable systems.

### WHAT

**Does healthcare payment fraud look like?**

It includes inflated claims, billing for services not rendered, identity theft, duplicate claims, unbundling, and unauthorized access to patient billing data.

### WHY

**Take action against payment fraud?**

Payment fraud drains billions from the healthcare system annually, risking compliance penalties and trust loss. Proactive detection and secure integrations protect patients and your bottom line.

## HOW KLIZER HELPS

**Klizer** enables secure data flows, real-time monitoring, and AI-based anomaly detection across billing and financial systems-empowering healthcare brands to stop fraud before it spreads.

# 5 MANUAL PROCESS PAIN POINTS HEALTHCARE BRANDS FACE

## Integration Gaps

Manual data movement between systems creates disconnects.

- Patient, billing, and supply data live in silos
- Increased delays and duplicate work

DID YOU KNOW?

**66%** **of healthcare execs say lack of system integration limits their digital transformation.**

(Source: Deloitte)

## Human Error Risks

Manual input leads to mistakes in patient records and billing.

- Incorrect insurance info
- Missed care coordination

DID YOU KNOW?

**45%** **of claims denials stem from manual data entry or errors.**

(Source: MGMA)

## Slow Decision-Making

Data isn't real-time, making fast care and financial decisions harder.

- Delayed reporting
- Missed revenue opportunities

DID YOU KNOW?

**Manual reporting can delay operational insights by up to 48 hours.**

(Source: HIMSS)

# 5 MANUAL PROCESS PAIN POINTS HEALTHCARE BRANDS FACE

## Security Exposure

Paper records and spreadsheets are easily accessed or misused.

- HIPAA violations
- Fraud exposure

DID YOU KNOW?

**21%** **of healthcare data breaches are linked to physical record mishandling.**

(Source: HHS OCR)

## Scalability Limits

As patient and partner data grows, manual systems buckle.

- Can't support growth or automation
- Staff overwhelmed

DID YOU KNOW?

**58%** **of healthcare providers say manual workflows limit their ability to**

(Source: Becker's Hospital Review)

## Challenge 4: Integrating Payment Systems with Existing Healthcare Software (EHR/EMR, Billing)

Healthcare uses various types of software systems. While doctors use Electronic Health Records (EHR) or Electronic Medical Records (EMR) to manage patient information, administrative staff use Practice Management Software (PMS) for tasks like appointment scheduling and tracking, apart from other things.

Smoother payments require all these systems to work together. Failure in achieving this interoperability can result in payment delays, which in turn harm the cash flow in the organization. Having seamless data communication across these systems also ensures that data is easily accessible for the patients and staff to avoid errors caused by manual steps.

However, there are still challenges to it:

- **Interoperability Issues:** Since there are multiple system types, even the data format varies for each. This makes it challenging for the systems to integrate well and provide the desired results.
- **Legacy Systems:** Over 73% of healthcare providers are still using legacy systems, which cannot work well with current technology.
- **Complex Workflows:** Billing and payment processes are often specific to each healthcare provider. Integrating payment systems into this requires customization, which is time-consuming and complicated.
- **Data Migration:** Due to multiple data formats, moving historical data to modern systems can be tricky and lead to data loss.
- **Security and Compliance:** It is evident that security and compliance is a major issue when dealing with healthcare data, which further complicates the process.

While these are some of the technology-related challenges, there are multiple other issues, such as budget, resistance to change, and poor planning.

## Challenge 5: Meeting Changing Patient Payment Expectations (B2C)

There is a massive shift in how patients are perceiving their relationships with healthcare providers. They are thinking of themselves as a consumer rather than patients, and expect the same convenience, transparency, and digital tools they get from stores, banks, or other services. How patients feel about the billing and payments now plays a big role in how they see overall care.

**NRCHealth's study** shows that **80%** of patients would switch providers for more convenience, and **61%** would switch just for a better payment experience.

Let's talk about the common issues patients face with the current payment systems:

- **Confusing Bills:** About **70% of patients** find their medical bills hard to understand. Less than half say they know what they owe and why. This confusion causes stress and slows down the payment, affecting the cash flow.

- **No Price Transparency:** Price transparency is a major issue in the healthcare industry. Patients are unaware of the treatment costs, but getting accurate estimates is still difficult. Even less than half of care providers give clear estimates in advance, leading to "sticker shock" when the bill arrives.

- **Outdated Communication and Payment Options:** Nearly **half of patients** are frustrated that healthcare still uses paper bills. Digital options like email, patient portals, and text reminders aren't available everywhere.

- **Inconvenient Payment Methods:** Most **patients (93%) prefer to pay online.** They want digital tools like secure portals, mobile payments (Apple Pay®, Google Pay™), auto-pay plans, and instant payments. About **77% say they'd choose instant disbursements** if offered.

When providers don't keep up with these expectations, it leads to problems like slow payments, higher collection costs, and unhappy patients. Confusing bills and limited digital options can drive patients to look for care elsewhere. A bad billing experience can affect the whole patient relationship.

Clearer bills and better cost estimates help patients pay faster and with less frustration. Giving patients the tools to understand and manage their medical costs improves satisfaction and helps providers get paid more quickly.

## Challenge 6: Complex B2B Healthcare Payments

Besides patients, hospitals, clinics, suppliers, insurance companies, distributors, and other service providers are also sending and receiving payments regularly. These payments are even more complex than the ones made by individual patients.

This is what makes healthcare B2B payments more complicated:

- **Matching Orders to Invoices:** Payments need to match with purchase orders and invoices, which adds time and complexity.
- **Contract-Based Pricing:** Prices aren't fixed. They're often based on negotiated contracts, discounts, or agreements with purchasing groups, which systems handle.
- **Multiple People Involved:** Approvals often have to go through different departments like procurement, finance, or clinical teams, which slows things down.
- **Special Payment Methods:** B2B payments use traditional payment methods like bank transfers (ACH), wire transfers, virtual cards (one-time card numbers), and even paper checks.
- **Large Payment Amounts:** These transactions involve big amounts, like payments for equipment, medicine, or large supply orders.
- **Hard to Reconcile:** With different invoices, payment types, and remittance info (what the payment is for), it's tough to track payments, especially when done manually.
- **Slow Payment Times (High DSO):** Because of all the steps and possible errors, payments take a long time, which hurts cash flow for suppliers.

Healthcare processes add even more complexity, like needing to track payments across different hospital departments, sticking to contract terms, and making sure everything follows regulations.

All of this leads to hidden costs. Manual processes use up time, paper, postage, and staff resources. Mistakes and delays can strain relationships with suppliers, create cash flow problems, and waste staff time fixing issues.

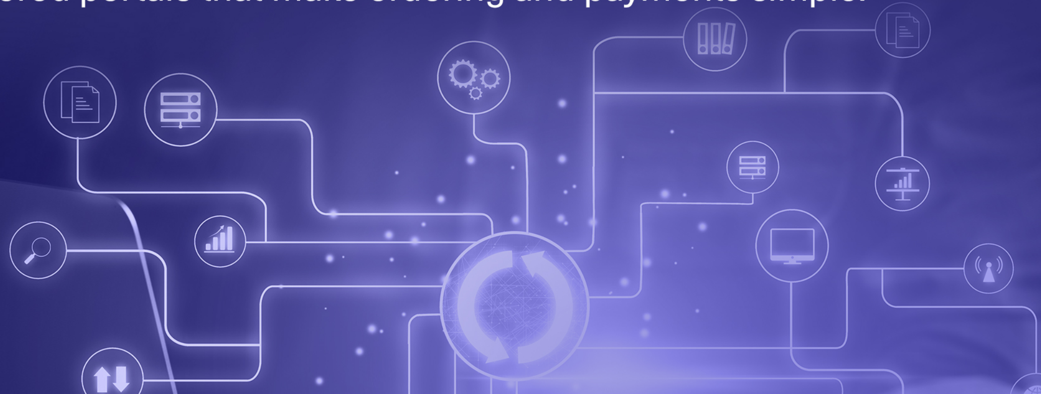
Most B2B payments in healthcare are still done manually. That means there's a big opportunity to improve. Going digital can make payments faster, clearer, and easier to manage. Hospitals and other healthcare buyers now expect the same kind of digital tools and self-service options they get in other industries.

## Introducing Klizer

**Klizer** is a reliable technology partner with a strong track record of delivering custom **healthcare commerce solutions.** With over **18 years** of experience in secure integrations, compliance, and B2B commerce, we have helped healthcare organizations improve their operational efficiency, minimize fraud, and deliver better patient care and partner experiences through **custom software and automation.**

Addressing challenges with us

- **Compliance Made Simple:** We ensure to comply with the most latest regulatory standards, including PCI DSS 4.0, by using secure APIs, tokenization and custom solutions designed with privacy and security.
- **Fraud Prevention:** We use strong authentication, payment tokenization, and real-time fraud detection to minimize payment fraud risk.
- **Seamless Integration:** We help you ensure seamless integration among all the systems in your organization, including ERPs, CRMs, EMRs, RCM, etc, to enable secure, compliant, and efficient data communication.
- **Automated Workflows:** By automating approvals, reconciliations, and B2B transactions, we build systems that reduce manual work and speed up payment processing.
- **Better Patient Payment Experience:** We create easy-to-use, mobile-friendly portals that support modern payment methods and clear billing information, reducing confusion and improving satisfaction.
- **Streamlined B2B Commerce:** We help healthcare organizations run efficient B2B operations with custom ecommerce platforms, ERP integration, and tailored portals that make ordering and payments simple.

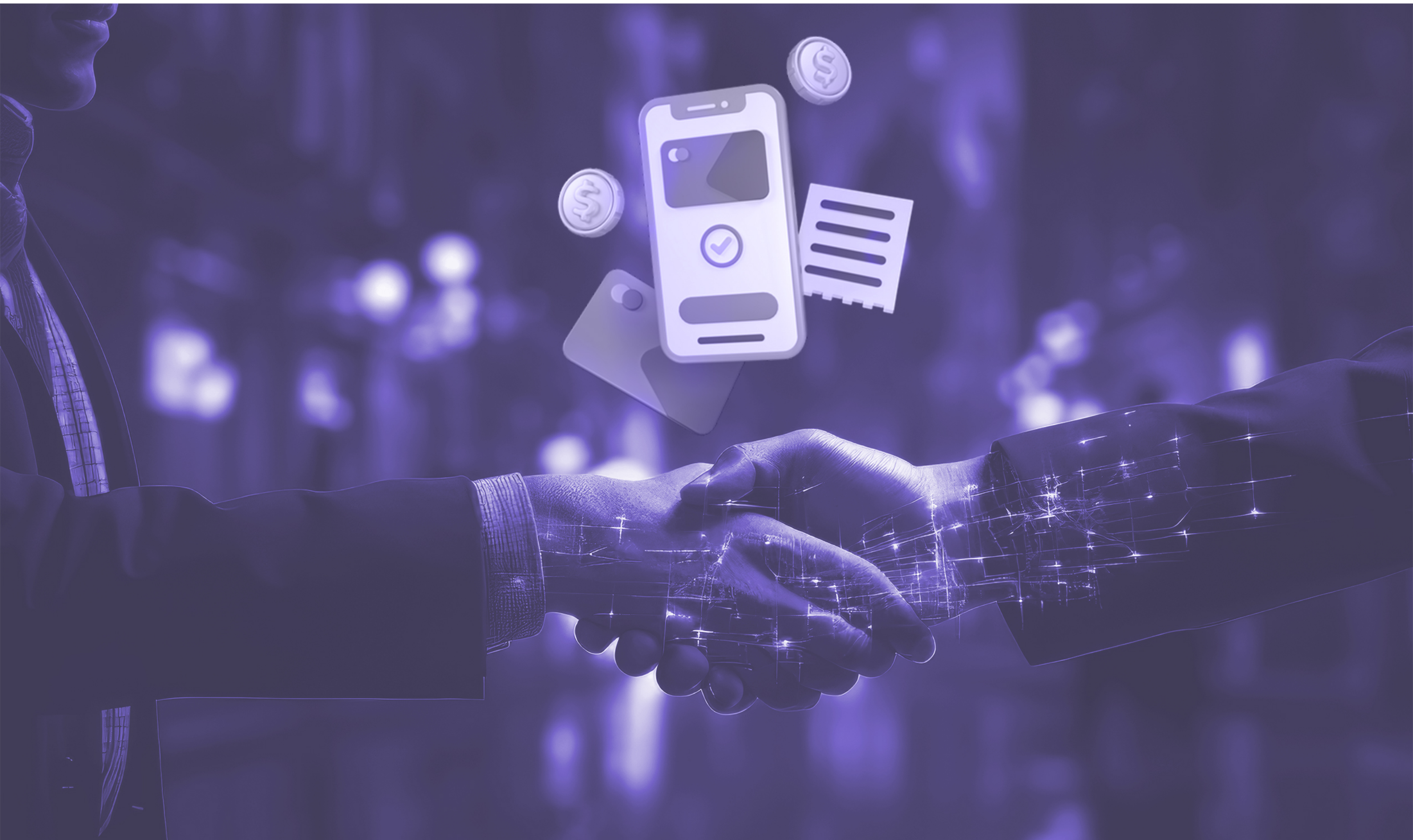


## Simplifying and Securing Healthcare Payments with the Right Technology Partner

Modernizing healthcare payments is a complex. Organizations deal with strict rules like HIPAA and PCI DSS, while also staying ahead of increasing payment fraud. Many still rely on traditional, slow, manual systems and paper processes, which waste time and resources. Connecting payment systems with core platforms like EHRs and billing software remains a major obstacle. At the same time, patients expect fast, digital, and transparent payment experiences, similar to what they get in retail.

Solving all these challenges takes more than just installing a payment gateway. It requires a complete solution and a technology partner who understands healthcare, knows how to build secure, custom systems, and can automate processes effectively. Klizer offers this kind of partnership.

If you are looking to explore more or have questions for us, our team would be happy to assist you. Just fill out the form here, and we'll get on a non-obligatory call with you to help you.



Klizer
by DCKAP

*Your digital transformation journey starts with Klizer.*

Follow Us

www.klizer.com | info@klizer.com

info@klizer.com