

Why your payments might not be as secure as you think

How to choose a dental payment partner that protects both card and patient data



Margins are tightening. Payment channels multiplying. And even accidentally mishandling [protected health information \(PHI\)](#) can expose dental providers to steep regulatory penalties and reputational damage.

Healthcare payments have never been riskier—or more complex. Yet patient expectations for simplicity and convenience have never been higher.

Other industries have conditioned consumers to expect fast, digital-first payment experiences with every purchase. In healthcare, however, regulatory safeguards make “easy” far more complicated.

Is PCI compliance enough for dental payments?

Most businesses must navigate a growing list of financial and data security standards — [PCI compliance](#) chief among them. For healthcare providers, that list is longer and more complex.

Any payment workflow that involves PHI must also meet HIPAA privacy and security requirements — and depending on the organization, standards like HITRUST may apply as well.

This creates a high-stakes dual obligation: protecting cardholder and patient data. And that’s what makes choosing a healthcare payment processing partner so challenging. How can you ensure the solutions you evaluate meet both sets of requirements?

The following guide and checklist show dental leaders how to choose a payment processor that meets both HIPAA and PCI requirements. But first: why is adhering to both frameworks so critical?

PCI and HIPAA compliance explained: Why dental providers need both

Many providers assume PCI compliance is enough. But since healthcare payments touch both cardholder data and PHI, two separate sets of safeguards must be in place. And this PCI vs HIPAA healthcare payments gap is where many organizations unknowingly fall short.

WHAT IS PCI-COMPLIANT PAYMENT PROCESSING?

PCI protects cardholder data. PCI compliant payment processing adheres to the Payment Card Industry Data Security Standard (PCI DSS) — the technical and operational safeguards organizations must implement to securely process, store, and transmit credit and debit card information.

WHAT IS HIPAA-COMPLIANT PAYMENT PROCESSING?

HIPAA safeguards a patient’s sensitive protected health information (PHI). HIPAA compliant payment processing is the practice of accepting, storing, and transmitting payments in a way that meets all required security, privacy, and regulatory standards for the healthcare industry.

Why HIPAA + PCI both matter for healthcare payments

Digital payments are rapidly accelerating and expanding. Patients today swipe, dip, tap, and click their way through online portals, text-to-pay links, mobile devices, and automated recurring billing cycles.

But more ways to pay also means more ways to be attacked. And whether they realize it or not, organizations that rely on PCI compliance alone are significantly exposed.

PCI protects cardholder data. [HIPAA protects patient data](#). Healthcare payments require both, and violations are costly:

- Financial penalties that can exceed hundreds of thousands of dollars
- Legal exposure tied to PHI breaches
- Operational disruption from system downtime and breach remediation
- Reputational damage that erodes patient trust for years

Payment security used to be considered an IT issue or a back-office function, but now, it's a leadership priority.

Since healthcare payments touch both patient cardholder data and protected health information (PHI), **providers must have both PCI and HIPAA safeguards in place.**

The risks of HIPAA and PCI noncompliance

Since October 31, 2024, HHS has received [374,321 HIPAA complaints](#). Up to [\\$500,000 can be levied](#) for each incident, with maximum penalty caps of [up to \\$1.5 million](#) for all violations of an identical provision during a calendar year.



The high costs of noncompliance

374k

HIPAA complaints
filed to date
(hhs.gov)

\$500k

Maximum fine per incident
for PCI non-compliance
(financial.ucsc.edu)

\$1.5m

HIPAA fines per year
for willful neglect
(ada.org)

The possibility of substantial fines like these is enough for most organizations to prioritize both HIPAA and PCI compliance. But exposure can also lead to revenue interruption, frozen payments, higher insurance premiums, and reputational risk.

Adding insult to injury, [IBM's Cost of a Data Breach Report](#) reports that healthcare breaches can take nearly 280 days to identify and contain, increasing operational disruption and recovery costs.

Beyond compliance: The business impact of HIPAA- and PCI-compliant dental payments

Compliance is required. But the advantages of getting it right go further than avoiding penalties. Here are ways HIPAA- and PCI-compliant payments improve the business of healthcare:

- **Maintains patient trust:** Patients assume their information is protected. A single breach can permanently weaken that trust.
- **Mitigates cyber threats:** Healthcare remains one of the most targeted sectors by cybercriminals. Payments are a high value target.
- **Reduces compliance risk:** HIPAA and state regulators are increasingly aggressive. Violations are costly and highly public.
- **Improves operational efficiency:** Disconnected systems force staff into manual reconciliation, duplicate data entry, and constant oversight.
- **Unlocks cash flow:** Automated, compliant systems accelerate payment posting, reduce errors, and shorten reimbursement cycles.

These benefits are real — but they don't remove responsibility. In healthcare, compliance outcomes ultimately rest with the organization itself.

Warning: HIPAA training doesn't equal HIPAA-compliant payments

Completing HIPAA training and risk assessments doesn't automatically make your practice's payment workflows compliant.

Why? Federal regulations — including [HITECH](#) — extend compliance to every vendor that touches protected health information (PHI), including your payment processor.

Many payment platforms started in retail and later moved into healthcare—without fully addressing healthcare-specific risks. That can leave gaps in safeguards like role-based access, audit logs, and Business Associate Agreements (BAAs).

Bottom line: Internal compliance only goes so far. If your payment software isn't built for healthcare, your practice may be exposed.

The three pillars of HIPAA-compliant dental payments

Here's how to know if the payment solution you're considering covers all the bases.

1. PATIENT DATA (PHI) IS PROTECTED

HIPAA-compliant payment systems must be intentionally designed to minimize and safeguard PHI by:

- Collecting only the HIPAA-defined "minimum necessary" data
- Keeping clinical and financial data strictly segregated
- Maintaining audit logs to trace access, changes, and movement of PHI
- Enforcing documented policies for PHI handling

2. SECURITY PROTOCOLS AND CONTROLS ARE CLEAR

Vendors must demonstrate maturity across multiple layers of security, including:

- Regular security testing and risk assessments
- A signed and actively maintained Business Associate Agreement (BAA)
- Strong authentication and role-based access
- Encryption and tokenization to minimize PHI and card data exposure
- Comprehensive audit logging

Without them, you can introduce organizational risk.

3. WORKFLOWS ARE DESIGNED FOR HEALTHCARE

Healthcare payments require more than secure rails. They must be built specifically for clinical environments:

- No manual rekeying
- Connections to PMS/EHR to reduce manual steps
- Payment networks designed for healthcare
- PHI-safe links, portals, and communications

When systems aren't designed for healthcare, staff end up bridging the gaps with manual workarounds, creating both operational inefficiency and compliance exposure.

The right technology can simplify HIPAA and PCI compliance.
That means the right vendor selection criteria is critical.

Checklist: What to look for in a HIPAA- and PCI-compliant payment partner

Viable dental payments partners must demonstrate clear HIPAA and PCI compliance and operational value. Meeting the criteria below should be non-negotiable.

The following criteria help dental leaders evaluate whether a payment platform is truly compliant and audit-ready.

Beyond regulatory requirements, we've included essential features and functionality to help you confidently choose a best-in-class healthcare payment processing solution.

A printable version of the checklist appears at the end of this guide.

COMPLIANCE AND ACCOUNTABILITY

At the very least, your healthcare payment solution must keep your organization HIPAA- and PCI-compliant. The best partners also demonstrate accountability and audit readiness through BAAs and other documentation.

Some payment vendors may claim healthcare readiness but rely on PCI compliance alone. Others may suggest their platform is appropriate for the healthcare industry, despite not being purpose-built for it. Both gaps can expose organizations to significant risk.

WHAT TO LOOK FOR

- ☐ Addresses HIPAA **and** PCI compliance
- ☐ Demonstrates accountability with a strong Business Associate Agreement (BAA)
- ☐ Documents security testing
- ☐ Documents breach detection, investigation, response, and notification procedures

WHAT TO ASK

- Is your platform designed and purpose built for the healthcare industry?
- Do you have independent assessments that verify HIPAA and PCI compliance?
- How does your software protect PHI?
- How does your platform support breach investigation and incident response if PHI is exposed?

After you're confident compliance is covered, use the following tips to make sure potential partners meet other baseline criteria for best-in-class payment solutions.

CONNECTIVITY AND AUTOMATION

Healthcare organizations [waste \\$760-935 billion each year](#) due to payment and claims inefficiencies. AR (accounts receivable) automation not only eliminates hours of chasing payments; it prevents the inevitable costly errors that arise from even the most rigid manual workflows.

Ask potential payment partners about their ability to automate tasks that monopolize staff time that would be better spent on patient care. Then make sure you understand precisely what the solution automates — and what it doesn't.

WHAT TO LOOK FOR

- ☐ Connects with your PMS/EHR
- ☐ Automates manual tasks like posting
- ☐ Delivers in-depth reporting and audit trails

WHAT TO ASK

- How does the solution eliminate manual payment posting for staff?
- Does the solution connect with your PMS/EMR?
- What work does integration require of your staff?

SCALABILITY

Whether your organization is a fast-growing regional practice or an enterprise expanding into new regions, ripping and replacing technology taps the brakes on growth.

The payment solution you choose should allow you to scale effortlessly and easily adapt to an always-changing regulatory landscape. It also should make it easy to add team members or adjust their roles as needed.

WHAT TO LOOK FOR

- ☐ Built for practices of all sizes
- ☐ Backed by strong training resources
- ☐ Designed to scale with regulation
- ☐ Provides ongoing training and compliance education for staff

WHAT TO ASK

- How will the platform adapt as HIPAA and PCI regulations evolve?
- How do you help our team stay compliant as workflows and regulations evolve?
- Will the platform seamlessly scale as our organization grows and evolves?
- What resources do you offer to quickly onboard or train team members?

DEMONSTRATED OUTCOMES

Evidence builds confidence and reinforces credibility. Ask potential vendors for case studies, customer testimonials, and performance data. [Research reviews](#) from verified users on third-party platforms. And document the return your team should expect from your investment.

WHAT TO LOOK FOR

- ☐ Proven payment lift
- ☐ Workflow efficiency gains
- ☐ Documented compliance posture improvements

WHAT TO ASK

- Do you have case studies and performance data for organizations like ours?
- Where can we find verified, unbiased user reviews?
- What is our projected ROI? Over what period?

Next-level functionality: Reimbursement automation

Patient payments are only half of accounts receivable. Automating reimbursements — processing insurance payments electronically, standardizing Explanation of Payments (EOPs), and automatically posting payments to patient accounts — completes the AR cycle and removes manual follow-up.

[Learn how to automate reimbursement >](#)

The right payment partner is a strategic advantage

Dental payments are no longer just an administrative function — they can be used as a significant strategic advantage. Plus, PCI- and HIPAA-compliant healthcare payments ensure privacy, security, and trust.

The best payment partner for most dental organizations deliver:

- Single healthcare-ready platform
- Built-in HIPAA and PCI compliance by design
- Minimal manual handling
- Clear audit trails
- Vendor accountability baked in

The best leadership teams know better than to delay improvements to payment processes and compliance.

They reevaluate their payment partners to ensure they can support compliance mandates today, strengthen operational efficiency tomorrow, and scale seamlessly as regulations and patient expectations continue to evolve.

KICKSTART YOUR PAYMENT PARTNER SEARCH

Preview the only payment platform that checks all the boxes

Built for dental organizations, Bridge Payments is designed to meet HIPAA and PCI requirements while simplifying payments, automating AR, and reducing operational risk.

[Book a demo >](#)

Payment Partner Evaluation Checklist

Choosing the right dental payment partner is a strategic decision. This checklist is designed to help leadership teams evaluate vendors consistently, identify risk, and compare solutions side by side.

Use it during demos, procurement reviews, or board discussions to ensure nothing critical is overlooked.



Vendor name:

Company website / URL:

Primary product(s) evaluated:

Evaluation date:

Evaluator(s):

Department / role(s):

Current vendor (if applicable):

Stage of evaluation: ☐ Initial review ☐ Shortlist
☐ Finalist ☐ Renewal review

Implementation model: ☐ Standalone ☐ Replacing existing
☐ Integrated with PMS/EHR

Estimated contract term:

Additional notes/context:

1. COMPLIANCE & ACCOUNTABILITY (NON-NEGOTIABLE)

Your payment partner must protect both cardholder data and protected health information (PHI).

Required capabilities

- ☐ HIPAA-compliant payments
- ☐ PCI-compliant payments
- ☐ Provides a signed Business Associate Agreement (BAA)
- ☐ Documents regular security testing and risk assessments
- ☐ Maintains clear audit trails for payment-related data
- ☐ Enforces role-based access and authentication
- ☐ Documented breach detection, response, and notification procedures

Validation questions

Is your platform designed and purpose-built for the healthcare industry?

Do you have independent assessments verifying HIPAA and PCI compliance?

How does your platform protect PHI?

How does your platform support breach investigation and incident response if PHI is exposed?

Additional notes:

2. CONNECTIVITY & AUTOMATION

Disconnected systems create manual work, errors, and compliance exposure. Automation should reduce — not shift — administrative burden.

Required capabilities

- ☐ Seamless PMS/EHR integration
- ☐ Automated payment posting and reconciliation
- ☐ Real-time visibility into payment status and exceptions
- ☐ Minimal manual intervention for staff

Validation questions

What parts of AR are fully automated — and what still require manual work?

How does the solution eliminate manual posting for staff?

What level of effort is required to implement and maintain integrations?

Additional notes:

3. WORKFLOW DESIGN FOR HEALTHCARE

Healthcare payments require workflows built specifically for clinical environments – not retrofitted retail tools.

Required capabilities

- ☐ No manual rekeying of payment data
- ☐ PHI-safe links, portals, and communications
- ☐ Payment workflows designed for healthcare use cases
- ☐ Clear separation of clinical and financial data

Validation questions

Where do staff still need to “bridge the gaps” manually?

How does the solution reduce operational risk in daily workflows?

Additional notes:

4. SCALABILITY & CHANGE READINESS

Payment systems should support growth – not slow it down.

Required capabilities

- ☐ Designed for organizations of all sizes
- ☐ Easy onboarding and role management
- ☐ Ongoing training and support resources
- ☐ Ability to adapt as regulations evolve
- ☐ Provides ongoing training and compliance education for staff

Validation questions

Will this platform scale as our organization grows or changes?

How does the solution adapt to evolving HIPAA and state requirements?

What support is available for onboarding and ongoing training?

How do you help our team stay compliant as workflows and regulations evolve?

Additional notes:

5. DEMONSTRATED OUTCOMES

Claims matter less than results. Evidence builds confidence.

Required proof

- ☐ Documented improvements in collections or cash flow
- ☐ Measurable workflow efficiency gains
- ☐ Demonstrated compliance posture improvements
- ☐ Verified customer reviews and references

Validation questions

Do you have case studies for organizations like ours?

What ROI should we expect — and over what timeframe?

Where can we find unbiased third-party reviews?

Additional notes:

ADVANCED CRITERIA: REIMBURSEMENT AUTOMATION (DIFFERENTIATOR)

Patient payments are only half of accounts receivable. Reimbursement automation completes the AR cycle.

Value-add capabilities

- ☐ Electronic ingestion of EOPs
- ☐ Automated matching of payments to claims
- ☐ Automatic posting to patient accounts
- ☐ Real-time identification of underpayments or discrepancies

Why it matters:

When patient payments and reimbursements are automated together, AR becomes faster, cleaner, and far more predictable.

FINAL EVALUATION

- ☐ Meets all non-negotiable compliance criteria
- ☐ Reduces manual work across AR
- ☐ Supports growth and regulatory change
- ☐ Demonstrates measurable outcomes
- ☐ Positions payments as a strategic advantage — not just a function