PAUBOX

2025 REPORT

What small healthcare practices get wrong about HIPAA and email security

HIPAA failure is skyrocketing in small healthcare practices

Table of contents

1. Executive summary.....1
2. Small practices think they’re compliant. The data says otherwise.....2
3. Audit trails, encryption, logging—most SMBs skip the basics.....4
4. Small means safe? Not anymore.....6
5. HIPAA violations don’t scale down with company size.....8
6. A better path forward.....9
7. Sources.....10

Executive summary

Patient data is at risk—and most small practices have no idea. Our survey of IT leaders and Practice Managers at healthcare organizations with less than 250 employees reveals a dangerous mix of outdated tools and deep misunderstanding of HIPAA requirements.

HIPAA compliance failure is hiding in the inboxes of small healthcare practices all over the country. Small and midsize healthcare practices make up the vast majority of U.S. care delivery. The National Plan and Provider Enumeration System (NPPES) shows that over 90% of healthcare providers are affiliated with small organizations, such as solo or group practices, clinics, and community-based care settings.[1] Yet, when it comes to email security, these same organizations are operating with outdated assumptions and minimal safeguards.

It's not all bad news, though. Most compliance gaps have straightforward fixes that don't require major IT overhauls or additional staff.

GETTING IT WRONG

83%

believe that patient consent removes the need for encryption

64%

believe portals are required for HIPAA

20%

of SMBs don't utilize any form of email archiving or audit trail

10 months

is the average amount of time to detect and contain healthcare breaches

Small practices think they're compliant. The data says otherwise.

Ask any small healthcare organization if their email is HIPAA compliant and most will say yes. In fact, more than 80% of the practices we surveyed expressed confidence in their current compliance posture.

But that doesn't hold up to scrutiny.

Our survey found that nearly all small practices (98%) say their platform "encrypts emails by default." Most are using common platforms like Microsoft 365 or Google Workspace—but these tools often fall short on enforcement and visibility.

In practice, that means a provider may believe every email is encrypted when in reality, encryption may drop if the recipient's server doesn't support modern protocols—without any alert to the sender. In those cases, HIPAA-required safeguards aren't actually applied, and there's no audit trail to prove compliance. Nearly half of healthcare email breaches stem from Microsoft 365 alone, and Gmail misconfigurations, while less frequent, still create exploitable gaps.

AVERAGE COST OF A HIPAA BREACH

\+ OCR fines
Legal fees
Patient notification costs
Class action lawsuits

$11 million

83%

believe patient consent removes the need for encryption

64%

believe portals are required for HIPAA

This false sense of security leaves small practices exposed to both cyber attacks and compliance violations.

Melanie Fontes Rainer, Director of the HHS Office for Civil Rights, has noted: "Every organization, no matter the size, is required to comply with the HIPAA Security Rule. Risk assessments are not optional—they're foundational."[2]

Many SMB leaders genuinely believe they're following the rules—because the rules are often misunderstood. More than 8 in 10 think patient consent removes the need for encryption, and 64% believe portals are still required. These beliefs are creating compliance gaps that no platform can fix.

HERE'S WHAT THEY'RE GETTING WRONG

Patient consent does not replace encryption requirements
While the Privacy Rule allows covered health care providers to communicate electronically with their patients, "covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C."[4] Patient agreement to communicate electronically doesn't waive the requirement for appropriate safeguards—HIPAA still mandates encryption or documented risk-based alternatives under 45 CFR § 164.530(c).

Portals are not required
The regulations are clear: "an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable" (45 C.F.R. § 164.522(b)).[5] While patient portals are one option, HIPAA explicitly permits secure, direct email and other reasonable alternatives if the appropriate safeguards are in place.

REALITY CHECK

If you can't easily pull up logs showing which emails were encrypted last week, you may not be as protected as you think.

BREACHES AT SMALL PRACTICES (<100 EMPLOYEES) FROM THE PAST 12 MONTHS

Organization	Type of breach	Breach affect
Solara Medical	Phishing	$9.76 class-action settlement[14]
Sunrise Community Health	Email compromise	54,000+ patients affected
Salud Family Health	Phishing	80,000+ records exposed

Audit trails, encryption, logging—most SMBs skip the basics

HIPAA compliance doesn't require complicated software stacks or a dedicated security officer. But it does require a system that can protect PHI in transit, prove that protections were applied, and maintain traceability in the event of an incident.

That's where most small healthcare organizations fall short, and the consequences compound quickly. In 2025, healthcare breaches took an average of 224 days to detect and another 84 days to contain—over 10 months total.[6] The longer it takes to spot a breach, the higher the cost—and many small organizations lack the systems to see it coming. Without audit trails, it's impossible to spot—or stop—PHI leaks.

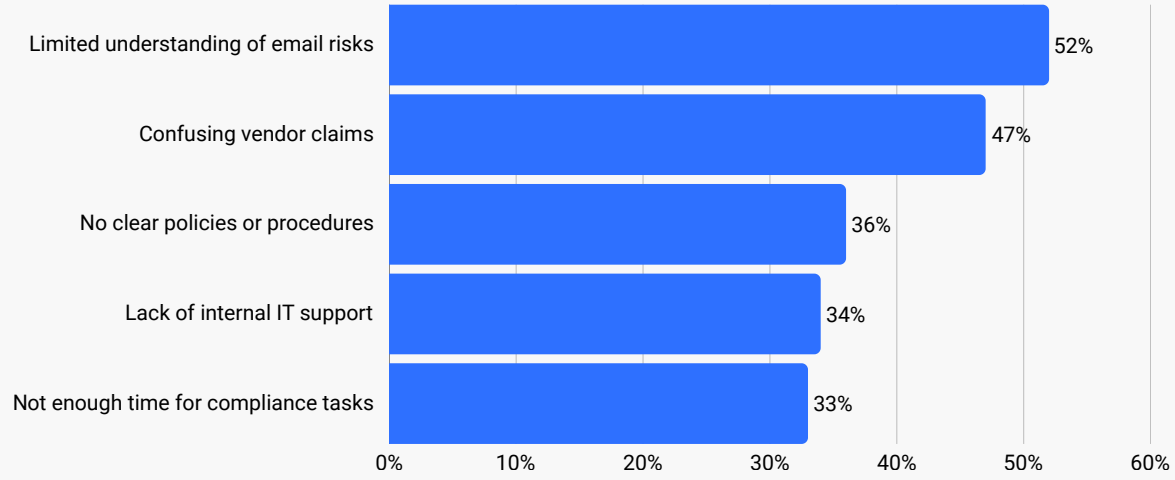
- The average SMB healthcare employee has access to more than 5,500 sensitive files, including PHI, billing data, and internal documents.[7]
- 20% of SMBs don't utilize any form of email archiving or audit trail, leaving 1 in 5 unable to investigate incidents after they happen
- Many are stretched thin—one third report not having enough time for compliance tasks, and the same number have no clear policies or procedures in place
- Only half have phishing or spoofing protection enabled, despite rising impersonation threats

KEY TAKEAWAY

Even basic visibility tools like email logging and secure archiving are missing in 1 in 5 small practices. That gap means breaches often go undetected until it's too late.

Paubox rated #1 in HIPAA compliant messaging software

Top 5 challenges small providers face in managing email security and HIPAA compliance



WHAT THE HHS IS LOOKING FOR

- **Proof that PHI was encrypted in transit** - not just that your platform "supports" encryption
- **Audit logs showing who sent what to whom** - and whether it was properly protected
- **Evidence of risk assessments** - documentation that you understand your vulnerabilities
- **Incident response procedures** - what you do when something goes wrong

> "Confidence without clarity is what gets organizations breached. We don't just need encryption—we need evidence."
>
> **Rick Kuwahara**
> Chief Compliance Officer, Paubox

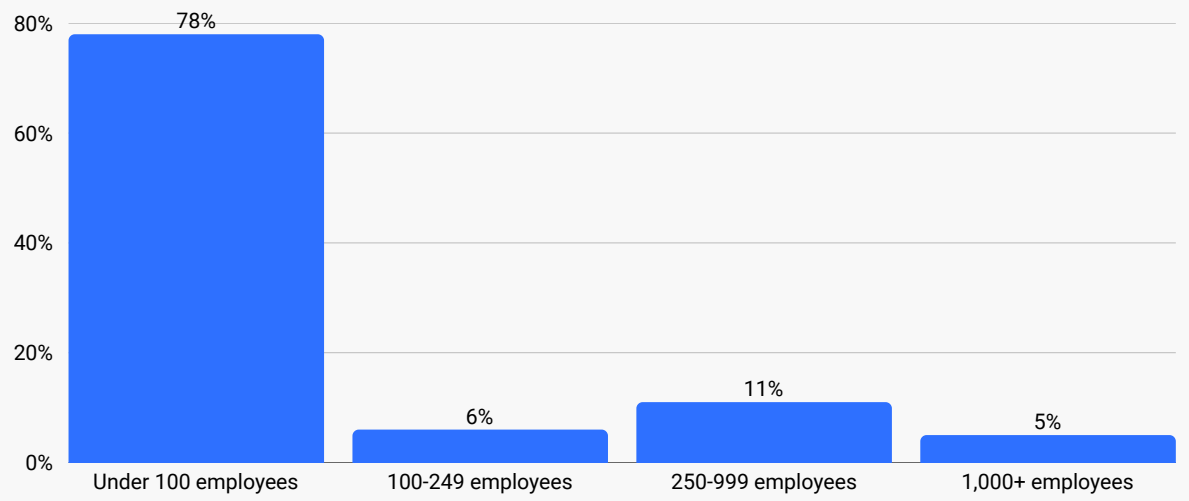
Small means safe? Not anymore

Phishing is the leading cause of healthcare breaches. As of 2024, over 70% of healthcare data breaches originated from phishing attacks.8 These attacks don't discriminate by size—in fact, 43% of SMB healthcare orgs reported experiencing a phishing or spoofing incident in the past year. Attackers increasingly target small practices because they often lack formal training programs, technical defenses, or dedicated security staff.

Adding to the problem: overworked staff are more likely to click on phishing emails. One study found that workload—not awareness—is the most consistent driver of phishing vulnerability among healthcare employees.9 Another found that 88% of healthcare workers have clicked on a phishing link at least once.[10]

> "Phishing attacks have evolved—they're faster, smarter, and relentless. It's not about one-off scams anymore; it's deception at scale."
>
> **Hoala Greevy**
> CEO, Paubox

Breakdown of U.S. healthcare providers by organization size (est.)



Cybercriminals know small organizations:

- Lack dedicated security staff
- Use default Gmail or Outlook and don't layer additional security
- Rarely use phishing or spoofing protections

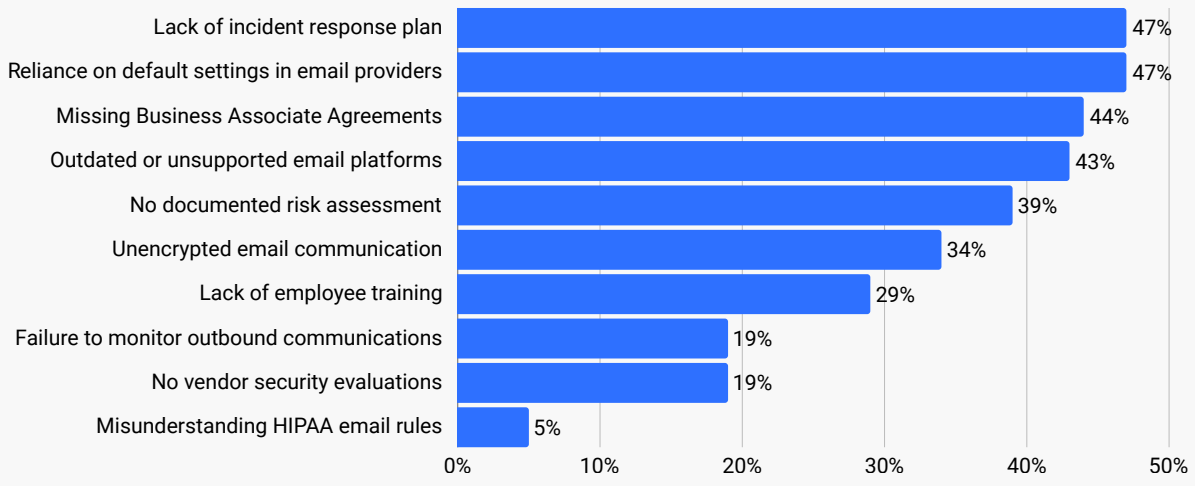
About 50% of SMBs lack anti-phishing controls beyond default spam filters. Nearly all (99%) have not implemented secure email transfer protocols like MTA-STS. These gaps are easy for attackers to exploit.

A 2023 KnowBe4 industry study found nearly 1 in 3 employees clicked during phishing simulations in SMB healthcare.[12] Newer threats are even harder to detect: QR-code phishing (known as quishing) now rivals email-based attacks in effectiveness.[13]

> **50%**
> of SMBs do not have phishing or spoofing protection beyond default platform settings

Rather than invest in proactive safeguards, many SMBs default to legacy solutions—faxing or sending unencrypted attachments. These workarounds open the door to HIPAA violations. Survey respondents noted that patients often struggle with secure portals or login-based message systems.

Top reasons cited why small practices fail HIPAA email compliance audits



HIPAA violations don’t scale down with company size

When a small practice fails to meet HIPAA standards, the consequences are just as serious as those for their enterprise peers. Even smaller fines come with major reputational and operational costs. Agape Health, a North Carolina FQHC, paid $25,000 for emailing PHI unencrypted to the wrong recipient. OCR penalized the clinic for having no encryption or HIPAA Security Rule procedures in place.[15]

In May 2025, Vision Upright MRI, a small California-based radiology provider, was fined $5,000 by OCR after unauthorized access to their medical imaging server exposed the protected health information of over 21,000 individuals.[16]

While the monetary penalty may seem modest, the settlement required two years of OCR monitoring and comprehensive compliance overhauls—costs that can easily exceed the fine itself for small practices.

It's also important to consider the potential legal exposure. HIPAA itself doesn’t provide a private right of action—but breaches almost always trigger downstream litigation. The scale of email access can also magnify the damage. According to NexusConnect, the average SMB healthcare employee has access to 5,500+ sensitive files, making every inbox a high-risk asset.[7]

THE ROI OF GETTING IT RIGHT

Immediate benefits

- Eliminate HIPAA email compliance risk
- Reduce staff frustration with clunky security
- Improve patient communication experience
- Clear audit trails for any future investigations

Long-term benefits

- Competitive advantage in patient communication
- Foundation for other digital health initiatives
- Staff efficiency improvements
- Peace of mind

The better path forward

Small practices need security that works automatically, in the background, without adding burden to already stretched teams.

The healthcare industry can't afford to treat HIPAA as a checklist—especially at the SMB level, where the majority of patient care happens. As attack vectors evolve and enforcement grows sharper, visibility, automation, and evidence-based safeguards are no longer optional. The silent assumption of safety is what's putting patients at risk—and it's time to address it head-on.

Compliance doesn't have to be complicated. But it does have to be provable.

The practices getting this right aren't necessarily spending more money—they're spending it more strategically. They've chosen tools that protect by default rather than hoping their staff will always make the right security decisions.

That means

- Encrypting every message by default—not just when triggered
- Logging and archiving email for compliance visibility
- Blocking phishing and spoofed messages before they hit inboxes

FRAME IT THIS WAY

"We're currently at risk for HIPAA violations that could cost us in fines, plus legal fees and patient notification costs. For $X per month, we can eliminate this risk and actually improve our patient communication."

PAUBOX EMAIL SUITE

The best HIPAA compliant email experience

- Setup in 15 minutes
- HITRUST certified since 2019
- No portals, no passwords
- Top rated U.S. support

Let’s chat!

PAUBOX

Sources

1. National Plan and Provider Enumeration System and CMS Provider of Services file analysis, 2024. https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/NationalProvIdentStand
2. Fontes Rainer, Melanie, director of the HHS Office for Civil Rights. Statement on HIPAA Security Rule compliance requirements. https://www.hhs.gov/hipaa/for-professionals/security/index.html
3. "How Microsoft and Google Put PHI at Risk," Paubox, 2025. https://www.paubox.com/blog/microsoft-google-phi-report
4. "HIPAA Encryption Requirements - 2025 Update," analysis of 45 C.F.R. Part 164, Subpart C and 45 C.F.R. § 164.530(c). https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C
5. "HIPAA Encryption Requirements - 2025 Update," analysis of 45 C.F.R. § 164.522(b). https://www.ecfr.gov/current/title-45/section-164.522
6. "Cost of a Data Breach Report 2025," IBM Security, 2025. https://www.ibm.com/reports/data-breach
7. "Data Access and Exposure in Small Healthcare Organizations," Nexus, 2022. https://www.nexusconnect.com/healthcare-data-access-report
8. "Healthcare Cybersecurity Report 2024: Phishing Trends and Impact Analysis," Jericho Security, 2024. https://www.jerichosecurity.com/healthcare-cybersecurity-report
9. Jalali, M.S., et al. "The Impact of Workload on Phishing Susceptibility in Healthcare Settings," Journal of Medical Internet Research, 2020. https://www.jmir.org/2020/7/e20429
10. "Healthcare Worker Cybersecurity Behavior Survey 2024," HealthStream, 2024. https://www.healthstream.com/resources/cybersecurity-survey
11. Greevy, Hoala, CEO of Paubox. Quote from "Dangerous Confidence Report," Paubox, 2025. https://www.paubox.com/blog/dangerous-confidence-report
12. "Phishing by Industry Benchmarking Report 2023: Healthcare Sector Analysis," KnowBe4, 2023. https://www.knowbe4.com/phishing-by-industry-benchmarking-report
13. Weinz, A., et al. "QR Code Phishing (Quishing) in Healthcare: Emerging Threats and Detection Methods," Cybersecurity in Healthcare Quarterly, 2025. https://www.cybersecurityhealthcare.com/quishing-threats
14. "Solara Medical Supplies Data Breach Settlement," ClassAction.org. https://www.classaction.org/news/solara-class-action-settlement
15. "Resolution Agreement with Metropolitan Community Health Services (Agape Health)," U.S. Department of Health and Human Services Office for Civil Rights. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/agape/index.html
16. "HHS Announces HIPAA Settlement with Vision Upright MRI," U.S. Department of Health and Human Services press release, May 2025. https://www.hhs.gov/press-room/hhs-hipaa-investigate-vum.html