PAUBOX

2025 REPORT

60% of healthcare orgs admit email security failure

Why legacy email systems are failing healthcare-and what must change to protect patient privacy.

Table of contents

Executive summary

60% of healthcare IT leaders reported breaches or security incidents involving email last year—and 73% expect breaches to continue in 2025. Why? This isn't about one hospital or one breach—this is about a broken infrastructure used across the country, exposing millions of patients to preventable risks.

Modern healthcare relies heavily on email for patient care communication, administrative processes, and sensitive information sharing. However, this crucial channel has become dangerously vulnerable. Our research reveals the reality: email security in healthcare is at a critical breaking point.

Based on new data from 150 healthcare IT leaders, this report pulls back the curtain on an overlooked risk in healthcare technology—legacy email systems. These systems are quietly undermining HIPAA compliance, straining operational efficiency, and exposing protected health information to cybercriminals.

Healthcare organizations currently allocate only 11–20% of their IT budgets to email security, despite email being

Key insights

60%

of healthcare organizations experienced email-related security incidents

73%

anticipate increased security challenges in the coming year their top cybersecurity vulnerability. In comparison, the financial services sector dedicates approximately 6–14% of overall IT budgets[1] specifically to cybersecurity, reflecting a proactive stance toward protecting sensitive financial data. Yet, despite healthcare's comparable or even slightly higher proportional spending, 74% of healthcare IT leaders still report dissatisfaction with their current email security solutions. This gap results in overworked security teams, ineffective protections, and substantial financial and operational risk, highlighting an urgent need to reassess and enhance healthcare email security investments.

> Despite rising cybersecurity budgets, only 11–20% of IT spending is directed toward email security

Top 3 ways emails get hacked

Phishing

Phishing occurs when a recipient clicks a link in an email and then enters their credentials on a fake website. Emails may also ask a recipient to download something that ends up being malware.

Man in the Middle Attack (MITM)

An MITM attack is when a hacker secretly relays communication between two parties who believe they are communicating directly. Unless both parties use encryption, the message can be read by anyone who intercepts it.

Password guessing

Personal information on social media makes it easier for a hacker to find information often used as passwords and security questions.

[1] " The cyber clock is ticking: Derisking emerging technologies in financial services ", www.mckinsey.com

Systemic security gaps beyond a single incident

The healthcare sector has always been a prime target for cybercriminals, but 2024 was a wake-up call. 180 healthcare organizations reported violations involving email breaches last year. 60% of IT leaders in healthcare organizations reported experiencing email-related breaches or security incidents, and 73% believe 2025 will bring even more breaches. Legacy email systems are no longer just an inconvenience—they represent a critical security vulnerability.

This isn't just about one-off phishing attacks or overlooked misconfigurations. It's about a fragile email infrastructure built on legacy systems and reactive processes that can no longer keep up with the speed and sophistication of modern threats.

Legacy platforms—once "good enough" for internal communication—are now liabilities. They're costly to maintain, incompatible with emerging security standards, and lack the flexibility needed to scale securely across complex healthcare networks.

"These breaches reveal a pattern of preventable failure," said Rick Kuwahara, Chief Compliance Officer at Paubox. "Like most industries, Healthcare relies on email, but most organizations are using tools that were never designed for today's cyberthreats."

Without a shift toward purpose-built, HIPAA-compliant platforms and proactive threat detection, the industry risks normalizing these breaches as the cost of doing business. In healthcare, that cost includes patient trust, regulatory penalties, and operational disruption.

> 60% of IT leaders in healthcare organizations reported experiencing breaches or security incidents involving email

The real human cost of email vulnerabilities

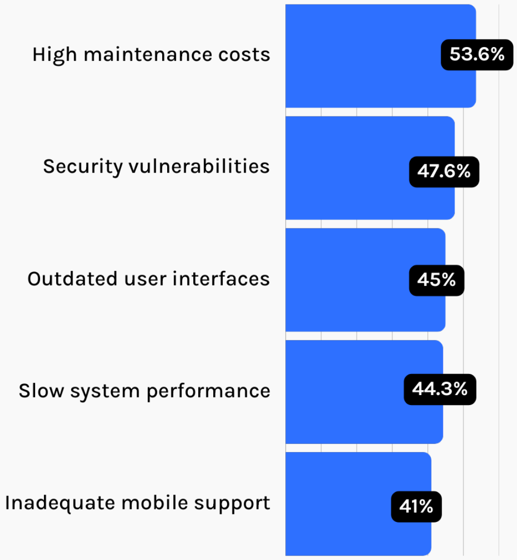
"Cyber attacks are an increasing threat to the Health and Public Health (HPH) sector," says Andrea Palm, Deputy Secretary of Health and Human Services. "These attacks can directly compromise patient safety."

Healthcare IT teams aren't just dealing with spam or hackers—they're dealing with infrastructure that undermines their mission. 83% say legacy systems disrupt day-to-day operations. "I've seen firsthand how legacy email platforms can quietly—but critically—undermine operational stability and efficiency across healthcare organizations," says Matt Murren, CEO of True North ITG. And in larger healthcare networks, the problem is amplified by scale and complexity.

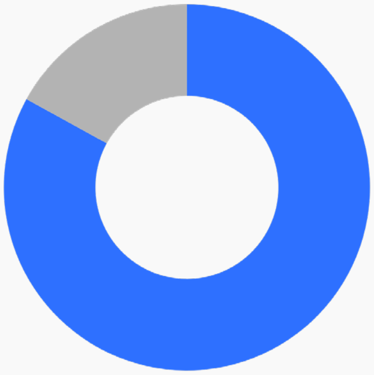
The most common challenges include:

- High maintenance costs that drain IT resources
- Persistent security vulnerabilities
- Outdated and complex user interfaces
- System performance bottlenecks
- Limited mobile and remote work support

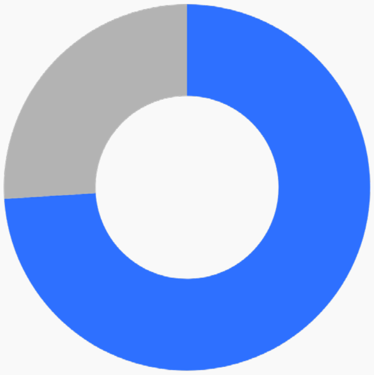
Top 5 legacy system complaints



Email security statistics



83% say legacy systems disrupt day-to-day operations



74% of healthcare IT leaders still report dissatisfaction with their current email security solutions

20% securing email communication has improved operational efficiency by over 20% for half of healthcare organizations

“HIPAA compliance is non-negotiable. Legacy email systems often lack features like end-to-end encryption, audit logging, or robust access controls—putting both patient data and institutional reputations at risk,” said Matt Murren, CEO of True North ITG, “The bottom line is legacy email platforms cost more than they save. They erode productivity, increase exposure to cyber threats, and ultimately compromise the quality of patient care."

Solutions like Paubox Email Suite are designed to reduce the friction that slows down secure communication in healthcare. Blanket encryption ensures that every message containing PHI is automatically secured—eliminating the need for extra authentication steps and portals. Features like Paubox [Tags] help bring instant clarity to your inbox by tagging subject lines based on sender—so you know what’s legit at a glance. And with ExecProtect+, phishing and spoofed emails are blocked before they reach inboxes, helping reduce human error and IT workloads.

With IT teams already stretched thin, this is a simple way to cut down on noise and reduce the number of “Can you check this email?” messages.

Legacy platforms weren’t designed for the speed, security, or scale modern healthcare demands. And that’s a risk no one can afford to ignore. Outdated systems are directly endangering patient care, operational stability, and organizational security.

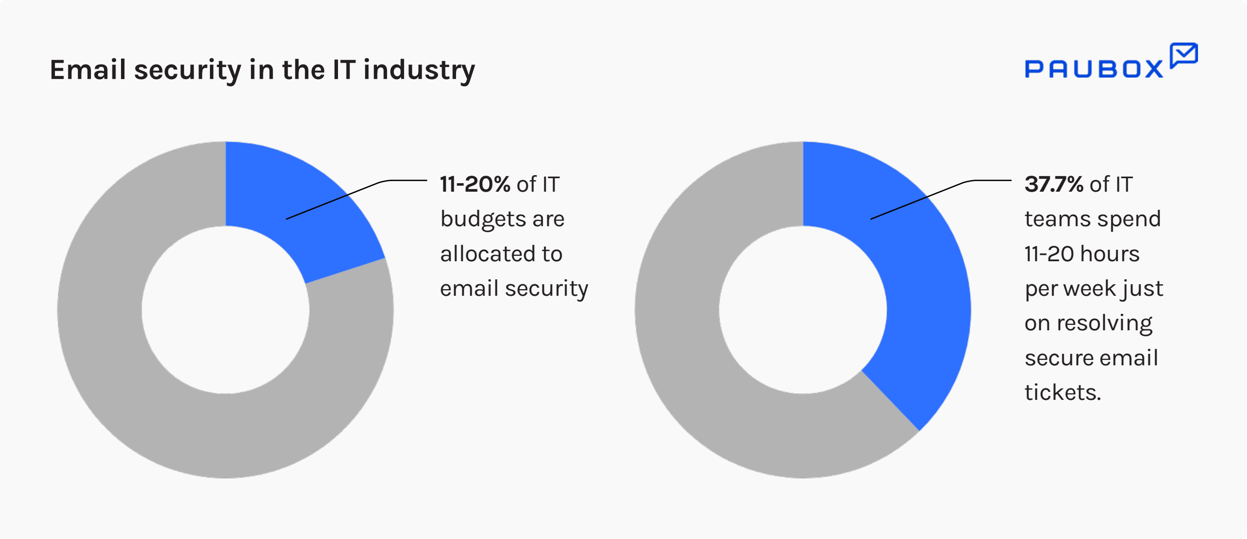
Email is underfunded and overexposed

Email accounts for half of threats, but only 11-20% of healthcare IT budgets are allocated to email security, despite a 50% increase in cybersecurity spending since 2019[2].

Meanwhile, the tools currently in place aren’t meeting expectations. 74% of IT leaders say they are not fully satisfied with the security features of their current email platforms. Dawn Kendall, Vice President of Programs and Services for Easterseals Louisiana shares bluntly, “We got a lot of pushback from email recipients using our previous encryption solution. Funders were asking us to resend things constantly because they weren’t able to open it.”

The result is reactive firefighting: with about 37% spending 11–20 hours per week just resolving secure email tickets. That's time that could be invested in proactive security measures or infrastructure improvements.

But there is hope. According to our survey, securing email communication has improved operational efficiency by over 20% for half of healthcare organizations.


Email security in the IT industry

[2] " 2025 healthcare email security report ", www.paubox.com

Patient privacy at risk

HIPAA compliance is non-negotiable—93% of survey respondents say it matters specifically when it comes to email. Still, 86% of IT leaders worry about their organization’s HIPAA compliance status.

Nearly 70% of IT leaders surveyed estimate that a HIPAA violation tied to email would cost their organization more than $250,000. However, recent enforcement actions by the HHS Office for Civil Rights (OCR) proves the opposite, with email-related HIPAA violations frequently resulting in penalties exceeding $1 million.

“Healthcare organizations must move to modern, cloud-hosted email systems as a baseline for security,” says David Chou, Founder of Chou Group Healthcare Technology Advisory Services. “Equally important is ongoing education to protect staff from phishing and social engineering, which continue to be the most effective tactics used by attackers.” According to OCR data, inadequate email security consistently ranks among the top reasons healthcare organizations face enforcement actions and hefty fines.

> Only 5% of known phishing attacks and 4% of known HIPAA email violations are reported to security teams.

Employee reporting remains dangerously low. Only 5% of known phishing attacks and 4% of known HIPAA email violations are reported to security teams. You might think that the gap between incidents and reporting points to a critical training or culture issue. However, 90% of healthcare organizations conduct regular employee training on email security best practices.

As CareM Director of Information Technology, Ryan Winchester puts it, “No amount of training can completely eliminate human error, so businesses must have safeguards in place. That’s why we need companies like Paubox to leverage AI for defense—because even one mistake can have serious consequences.”

Proactive protection and modernization: AI, automation, and encryption

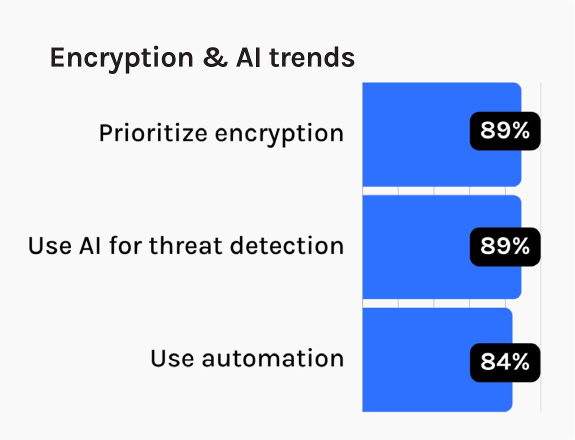
The inbox is healthcare's most neglected attack surface—but it doesn't have to stay that way. 89% of healthcare IT leaders believe AI and machine learning are critical for detecting email threats. AI tools now actively block spam, detect malware, flag phishing, and analyze suspicious behaviors, dramatically reducing breaches.

Paubox's ExecProtect+ is a frontline example, blocking phishing and spoofed emails instantly, ensuring threats never reach staff inboxes.

> "Healthcare doesn't need more patchwork fixes—it needs a mindset shift. Patients expect secure, convenient communication, and it's on us to meet that standard."
>
> **Hoala Greevy,** CEO of Paubox

Hoala Greevy, CEO of Paubox, states: "Healthcare doesn't need more patchwork fixes—it needs a mindset shift. Patients expect secure, convenient communication, and it's on us to meet that standard. With AI, automation, and built-in encryption, we can proactively defend patient data before threats ever hit the inbox. That's exactly what we built ExecProtect+ to do—eliminate risk at the source, not after the damage is done."

In addition, 84% say email automation improves both security and efficiency—a double win in a resource-constrained environment. And 89% of healthcare organizations are now prioritizing encryption in their secure email strategies.



Top 5 strategic recommendations

Reduce your risk, strengthen compliance, and bring email security up to today's standards.

Sunset legacy systems

The longer outdated portals remain in place, the more vulnerable your organization becomes.

Choose built-in HIPAA compliant platforms

Transitioning to HIPAA compliant solutions reduces compliance risks and simplifies security management.

Invest in automation and AI

Leveraging these technologies reduces manual workloads, proactively detects threats, and mitigates potential breaches.

Train smarter, not just more often

Effective training leads to higher employee reporting rates, significantly reducing unnoticed incidents.

Budget based on risk

If email is half your attack surface, your security budget should reflect that reality.

Methodology

Paubox partnered with independent research firm TrendCandy to survey 150 U.S.-based healthcare IT leaders in early 2025. The study targeted senior IT decision-makers at small, medium, and large healthcare organizations. The margin of error is +/- 7% at a 95% confidence level.