Security

The 2026 healthcare email security report

What 2025 breach data reveals about risk heading into 2026

PAUBOX

PAUBOX

Table of contents

Executive summary

Email remains one of the most common sources of HIPAA-reportable breaches. In 2025, healthcare organizations reported 170 email-related incidents to the HHS Office for Civil Rights.

While the total number of incidents declined compared to the year prior, the underlying conditions that enable email breaches remain widespread and largely unchanged.

Our analysis found that most breached organizations shared the same foundational gaps. Nearly three quarters lacked effective DMARC enforcement — the policy that tells receiving servers whether to reject, quarantine, or ignore emails that fail authentication. Over half relied on permissive or missing SPF records, which verify whether an email was actually sent from a server authorized to send on behalf of that domain. None enforced MTA-STS, which requires encrypted connections between mail servers and prevents attackers from intercepting messages in transit. These controls are baseline protections that have been recommended for years.

Microsoft 365 continued to lead the breach landscape. 53% of breached organizations relied on Microsoft 365 as their primary email platform. The presence of multiple security tools did not consistently correlate with stronger authentication posture or reduced breach risk.

Paubox survey research shows healthcare staff are increasingly using AI tools without formal oversight. As workflows evolve, existing email security gaps carry greater potential impact.

The takeaway for healthcare IT and compliance leaders is straightforward. Email risk is driven by incomplete configuration, and security controls that have not kept pace with modern threats.

BY THE NUMBERS

170
email-related breaches occurred in 2025

53%
of email-related healthcare breaches occured on Microsoft 365

41%
of breached organizations fell into a high-risk category based on their email configuration

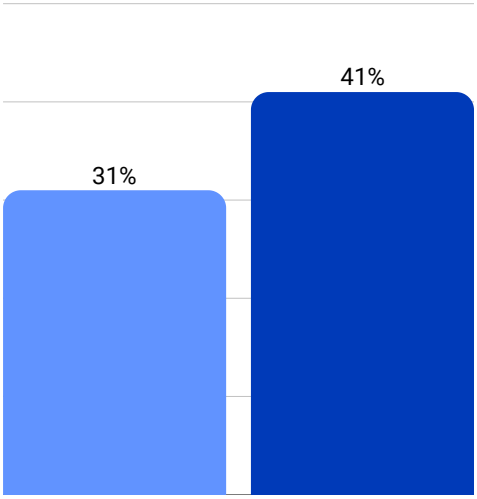
74%
lacked effective DMARC enforcement

Why healthcare email risk is concentrated heading into 2026

Email breaches in healthcare follow predictable patterns. Most incidents involve phishing, credential compromise, spoofing, or improper handling of sensitive information via email. These attack paths are well understood and heavily documented.

The threat landscape hasn't radically changed. What persists are the underlying conditions that make these attacks successful. Organizations with weak authentication controls, permissive sender validation, and unsecured transport appear repeatedly across breach disclosures. In several cases, the same organization reported multiple email-related incidents within a single year.

> "Patients must be able to trust that sensitive, health information in their files is protected to preserve their trust in the patient-doctor relationship and ensure they get the care they need."
>
> **Melanie Fontes Rainer,** OCR Director



41% of breached organizations classified as High Risk, up from 31% in 2024

In 2025, fewer organizations reported email breaches overall, but those that did had weaker security postures. 41% of breached organizations fell into a high-risk category based on their email configuration, up from 31% in 2024. In other words, the organizations still getting breached are the ones with the most ground to make up.

These gaps persist despite increased awareness and investment. Many organizations have added security tools but left foundational controls partially implemented or inconsistently enforced.

The breaches ahead are unlikely to come from novel attacks. They'll come from the same gaps that have been there for years, gaps that organizations have had time to close but haven't.

As healthcare organizations review their security posture in 2026, this concentration of risk matters. It means future breaches are more likely to occur in environments where the same misconfigurations and security gaps have existed for years, rather than as the result of new attack techniques.

Security gaps observed across breached organizations

Authentication and sender validation

DMARC enforcement remains inconsistent across healthcare. In 2025, nearly three quarters of breached organizations either lacked DMARC entirely (41%) or operated in monitoring-only mode (33%).

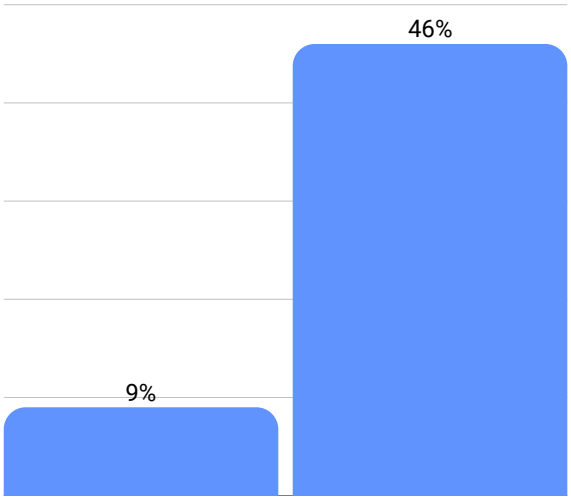
Without enforcement, an attacker can send emails that appear to come from a trusted domain, and the receiving system has no instruction to block them.

> **74% of breached orgs** had missing or unenforced DMARC (41% missing entirely, 33% monitor-only)

SPF adoption was more common, but often permissive. Over half of breached organizations used soft-fail policies (46%) or had no SPF record at all (9%).

A soft-fail policy means that even when a message is sent from an unauthorized server, it may still be delivered to the recipient's inbox rather than being rejected. Tightening SPF to a hard-fail policy ensures unauthorized messages are blocked outright.

These misconfigurations are the specific conditions that allow phishing emails to land, spoofed messages to appear legitimate, and credential harvesting campaigns to succeed.



56% of breached orgs had permissive or missing SPF records (9% missing, 46% soft-fail)

Transport security

None of the breached organizations analyzed enforced MTA-STS. As a result, email delivery relied on opportunistic TLS, a setting that attempts encryption when the receiving server supports it but falls back to sending messages unencrypted when it cannot encrypt.

This means encryption is attempted but never guaranteed. In a downgrade attack, a bad actor intercepts the connection

between two mail servers and forces that fallback, allowing them to read or alter the contents in transit. MTA-STS prevents this by requiring that connections between servers are encrypted, and refusing delivery if they are not.

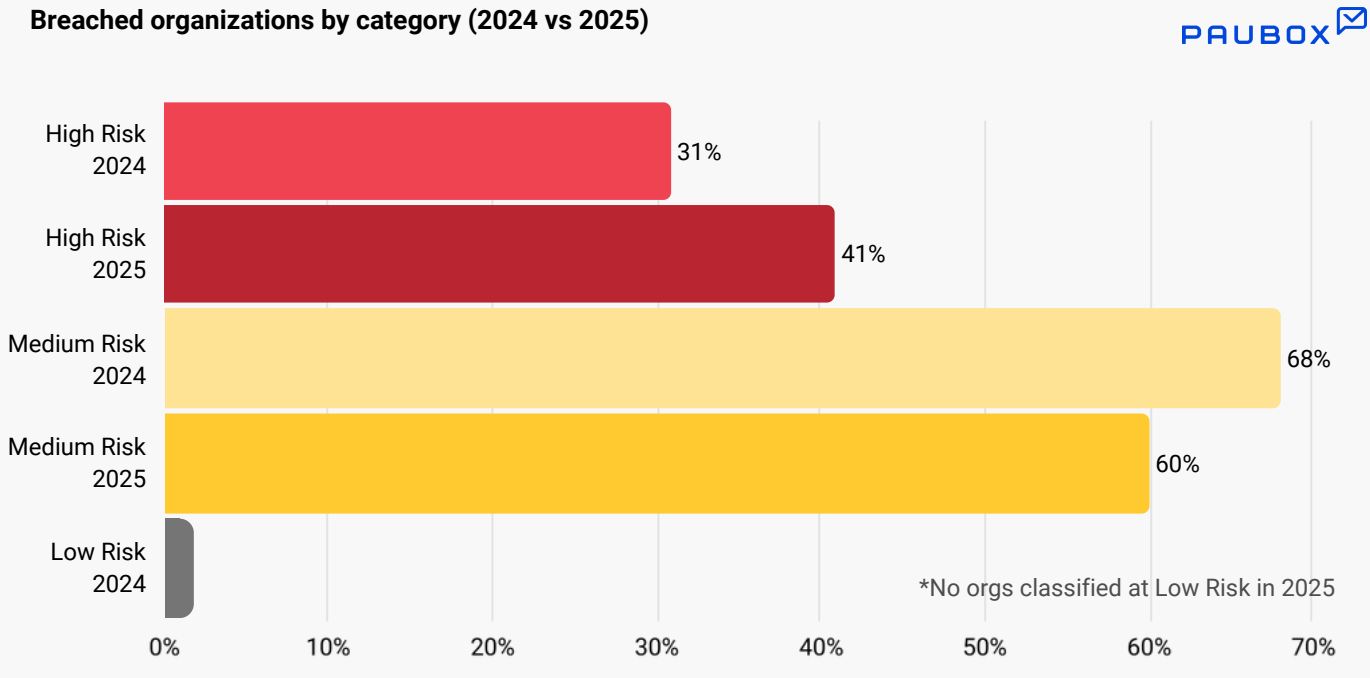
This is a critical but often overlooked gap. Encryption in transit is only as strong as the policies that enforce it.

Reliance on user-driven controls

Many healthcare organizations continue to rely on portals, manual encryption triggers, or staff judgment to protect sensitive email content.

These approaches introduce friction. Over time, friction leads to workarounds. When speed and convenience conflict with security, staff behavior predictably favors speed.

Breached organizations by category (2024 vs 2025)



Microsoft 365 and the reality of shared responsibility

Microsoft 365 is the most widely used email platform in healthcare, adopted by approximately 79% of healthcare orgs. That prevalence makes it the primary attack surface for bad actors.

Roughly half of breached organizations relied on Microsoft 365 as their core email platform. What the data shows is a consistent gap between platform capability and configuration discipline.

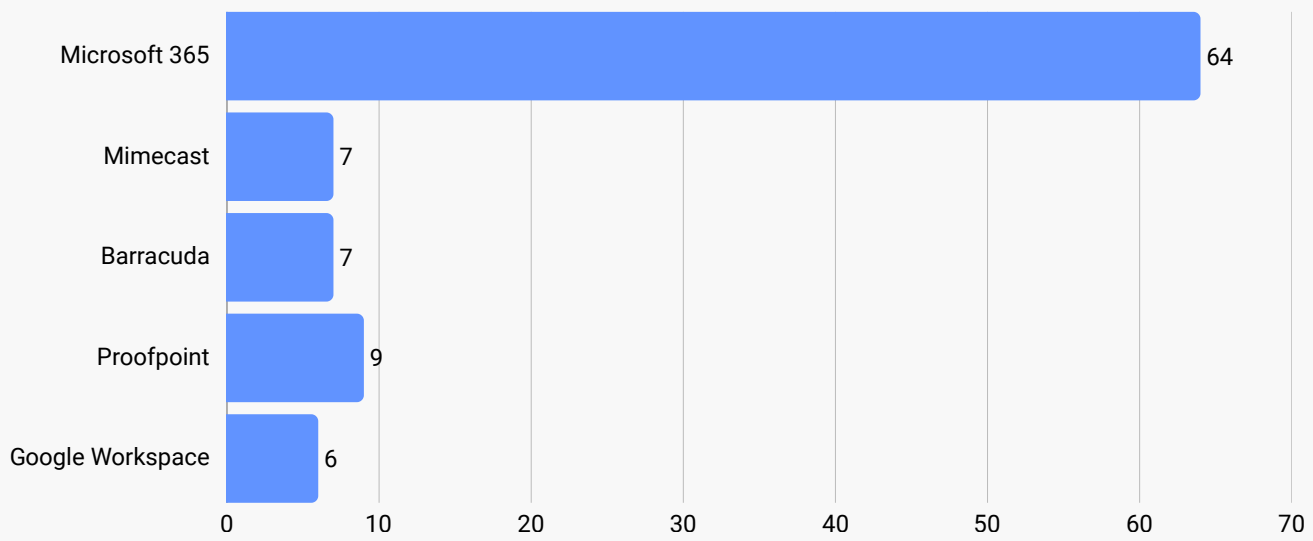
53% of breached organizatons used Microsoft 365 (up from 43% in 2024)

In breached Microsoft 365 environments, the same foundational weaknesses were common. Authentication controls were left incomplete, sender validation remained permissive, and transport security relied on opportunistic encryption.

Microsoft 365 was not the only platform with exposure. 5 of 6 breached Google Workspace organizations were classified as High Risk.

> **31%** of breached Microsoft 365 orgs were classified as High Risk

Email breaches by provider (Jan - Dec 2025)



Organizations running custom or self-managed mail infrastructure fared similarly, with 65% falling into the high-risk category. Smaller organizations managing their own email environments often face the greatest configuration challenges due to a lack of IT resources. Proofpoint appeared in 9 breached organizations, and Mimecast and Barracuda each appeared in 7.

The presence of security tools alone does not substitute for foundational configuration discipline. Email security is a set of controls that require deliberate configuration, ongoing review, and clear ownership across IT and compliance teams.

> Proofpoint, Barracuda and Mimecast accounted for 19% of breaches in 2025

How changing workflows increase the impact of existing email risks

These configuration gaps enabled past breaches and shape how future risk will materialize. To understand future risk, behavioral context is necessary.
In a 2025 Paubox survey of healthcare IT leaders, 85% of respondents said they suspected staff were using unauthorized AI tools, while only 26% reported having visibility into that usage. Over two thirds had already identified instances of unsanctioned AI adoption.

This report does not claim that AI usage caused any 2025 breaches. However, the connection between changing workflows and existing security gaps is worth examining directly.

> **85% of healthcare IT leaders** said they suspect staff were using unauthorized AI tools

As AI-assisted workflows increase the speed and volume of communication, the quantity of sensitive information moving through email systems expands. Manual safeguards, such as deciding when to encrypt or whether to use a secure portal, become less reliable under scaling communication. The margin for error shrinks. From a risk standpoint, AI increases the consequences of existing weaknesses.

What effective email security looks like in 2026

Email will remain a primary attack vector in healthcare. That is unlikely to change.

What is already changing is the volume and velocity of email-borne threats moving through organizations. According to the 2025 KnowBe4 “Phishing By Industry Benchmark Report”, phishing emails have increased by 17%, and there was a 47% rise in attacks that evade native defenses.

HIPAA requires covered entities to assess reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI. In 2026, that assessment must account not only for traditional phishing and spoofing, but also for how emerging tools interact with existing infrastructure.

That means evaluating questions such as:

- Are AI-assisted tools generating or processing PHI outside of sanctioned systems?
- Is sensitive content being drafted, summarized, or reformatted in external applications before being sent via email?

> HIPAA requires covered entities to assess reasonably ancitipated threats to the confidentiality, integrity, and availability of ePHI.

- Do existing authentication controls, such as enforced DMARC and SPF, protect AI-generated outbound communications from spoofing or impersonation risk?
- Is encryption applied automatically, or does it depend on user decisions at higher communication volume?
- Do logging, archiving, and monitoring controls capture AI-assisted communications the same way they capture traditional email workflows?

Risk assessments that focus only on inbox filtering or phishing simulations miss the structural question. As workflows change, the points at which ePHI is created, transformed, and transmitted also change.

Emerging tools increase the speed, volume, and pathways through which sensitive information moves. Security assessments must expand accordingly.

Remove human decision points wherever possible

Effective email security does not rely on employees to decide when protection is required. According to Paubox's recent report "The Dangerous Confidence of Healthcare IT", 86% of healthcare IT leaders said their current email security tools introduce workflow friction, and acknowledged that users bypass security controls to keep work moving.

Choosing when to encrypt. Deciding when to use a portal. Recognizing whether an email contained sensitive information. These approaches do not scale, and fail under real-world conditions.

Paubox is designed around a different assumption. Every outbound email is encrypted automatically by default, without requiring users to change workflows or make decisions about sensitivity. This removes one of the most common sources of accidental exposure and reduces reliance on training alone.

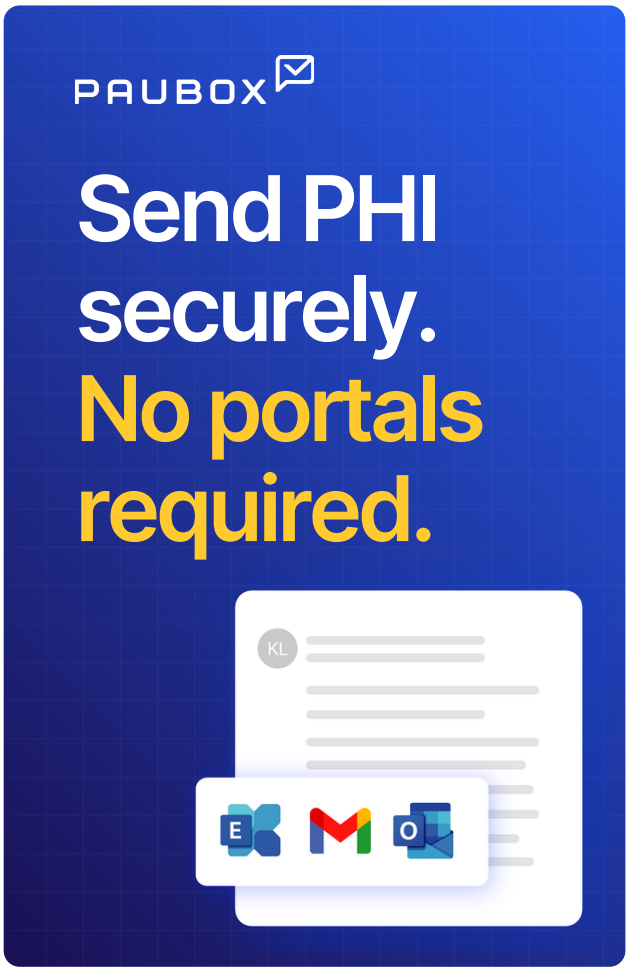
> **86%** of healthcare IT leaders said their current email security tools introduce workflow friction

Enforce baseline protections, not optional ones

Selective security creates gaps. Many email environments rely on conditional rules. Encryption is triggered only when keywords are detected or when users take a specific action. This introduces inconsistency and makes post-incident justification difficult.

Effective programs apply protection broadly and predictably.

Paubox encrypts every outbound email in transit, ensuring HIPAA compliant delivery regardless of sender, recipient, or message content. Messages arrive directly in the recipient's inbox, without portals, passwords, or additional steps. This consistency simplifies compliance and reduces the risk of human error.



Secure every email you send and receive

Many organizations focus heavily on inbound threats while treating outbound email as a compliance exercise.

The 2025 breach data shows that risk exists in both directions. Credential compromise, impersonation, and improper disclosure often span both inbound and outbound channels.

Paubox secures every email your organization sends and receives. Paubox's Inbound Email Security sits in front of Microsoft 365, Google Workspace, or Exchange to analyze messages before they reach inboxes or sync into downstream systems like EHRs, CRMs, or customer support platforms. Paubox Email Suite's outbound encryption ensures sensitive information is protected once it leaves the organization.

Align security with how work happens

When security adds steps, staff find shortcuts. The most effective controls are the ones no one has to think about.

Paubox works seamlessly with Microsoft 365, Google Workspace, and Microsoft Exchange, without plug-ins, training, or new workflows. Email continues to function as expected for staff and patients, while protection is applied in the background.

That operational simplicity is reflected in third-party validation. In recent G2 rankings, Paubox was rated #1 in implementation within its category, reinforcing that security can be deployed without introducing additional workflow friction or administrative burden.

Support defensible risk management

Email security is both an operational safeguard and a compliance obligation.

When an auditor asks how your organization protects email, the answer should be simple: every message is encrypted automatically, threats are filtered before delivery, and none of it depends on whether an employee remembered to click the right button.

Paubox secures every email you send and receive. Trusted by more than 8,000 healthcare organizations and rated #1 on G2 for email encryption software, Paubox is built to reduce risk, simplify compliance, and communicate securely.

Methodology

This report analyzes email-related healthcare breaches reported to the HHS Office for Civil Rights between January 1, 2025 and December 31, 2025.

Each breached organization was evaluated using publicly observable DNS and email configuration data to assess:

- Primary email service provider
- SPF configuration
- DMARC configuration and enforcement level
- Presence of MTA-STS

Organizations were classified into risk categories based on the combination of these controls.

This report analyzes organizations and distinguishes between unique organizations and total breach incidents. Some organizations experienced multiple email-related incidents during the reporting period.

Sources

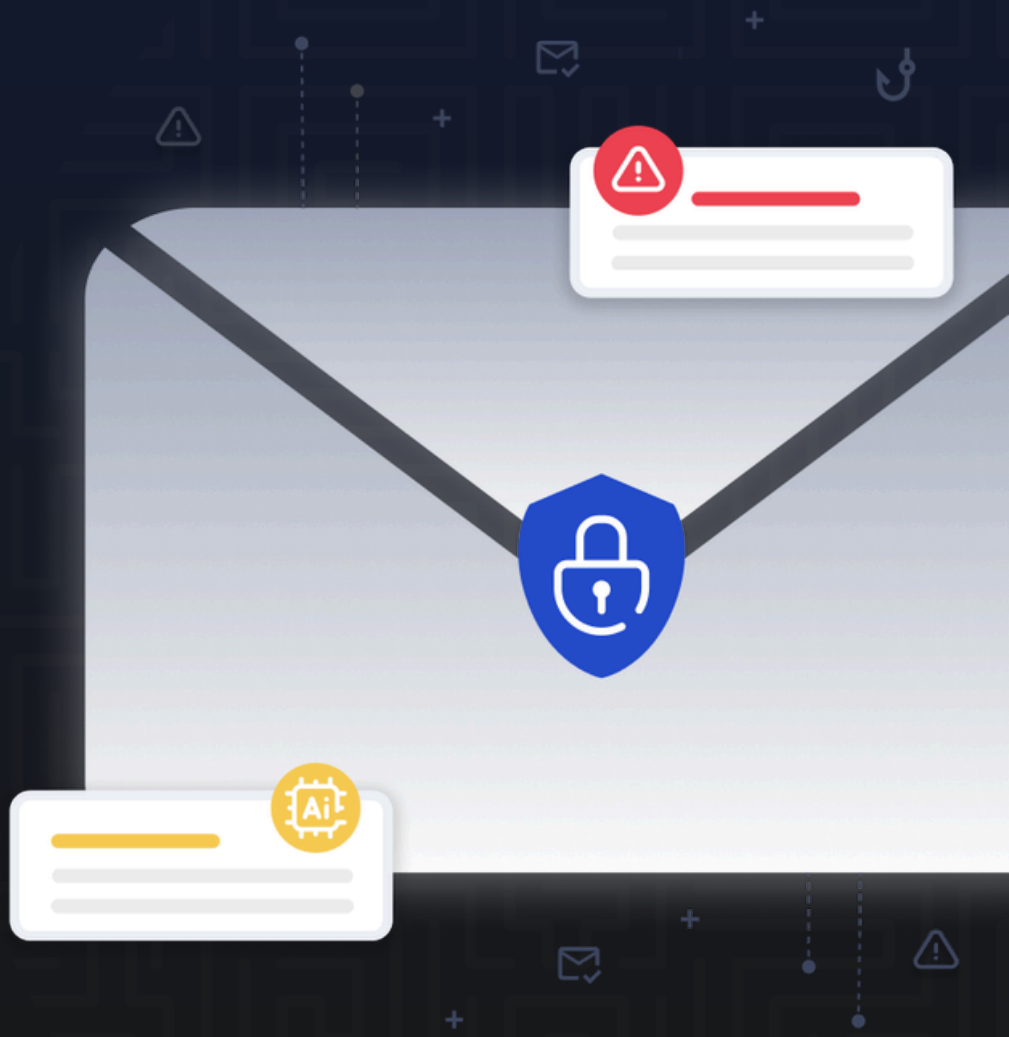
1. U.S. Department of Health and Human Services, Office for Civil Rights. "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." Accessed Jan. 1–Dec. 31, 2025. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
2. Paubox. "Healthcare IT Is Dangerously Overconfident About Email Security." 2025.
3. KnowBe4. "2025 Phishing By Industry Benchmarking Report." 2025. https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report
4. Paubox. “Shadow AI is outpacing healthcare email security.” 2025.

PAUBOX

Stop email phishing attacks with AI security

Surface hidden threats with generative AI email security that learns and evolves.

Talk to an expert



Why old gaps in email security lead to new breaches

Persistent configuration failures cause healthcare data breaches; automated, foundational security controls are the solution

The top 3 attack patterns

75% lacked DMARC enforcement

Three-quarters of breached organizations had no policy to reject or quarantine authorized emails.

0% enforced MTA-STS

Every breached org relied on opportunistic encryption, leaving messages vulnerable to interception.

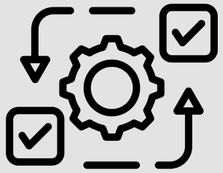
55% had permissive SPF records

Over half of orgs used “soft-fail” policies that allowed unauthorized senders into inboxes.

Default security over human judgement

Remove human decision points

Automate encryption to prevent staff from bypassing security for the sake of speed.



Eliminate workflow friction

Effective security should work in the background without requiring portals, passwords, or plugins.

Secure outbound and inbound email

Default automatic encryption ensures HIPAA compliance, and AI-powered inbound email security protects inboxes from phishing and ransomware.