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.

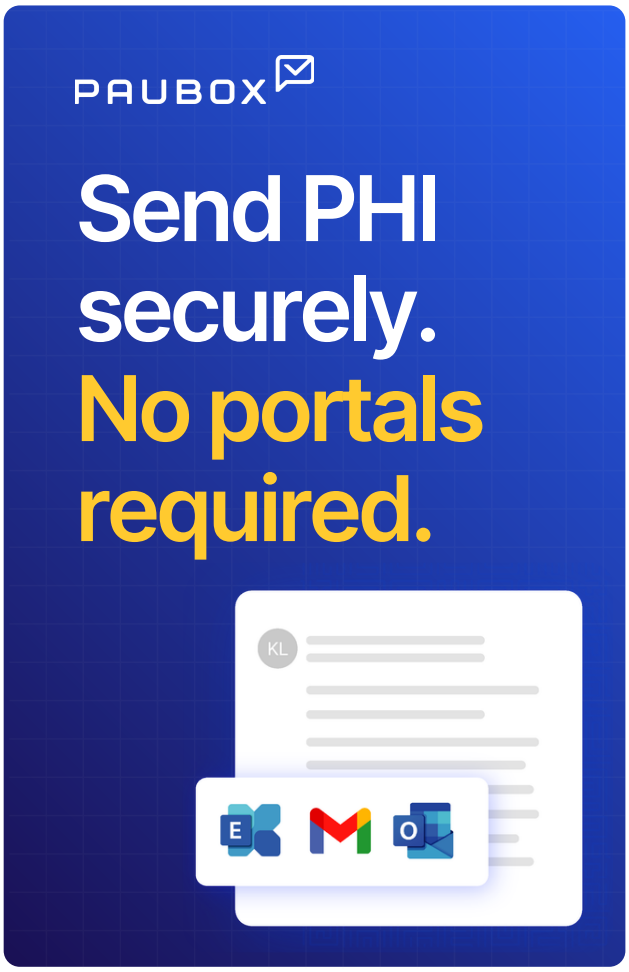
> **86%** of healthcare IT leaders said their current email security tools introduce workflow friction

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.

PAUBOX

Stop email phishing attacks with AI security

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

Talk to an expert