

Attack 3. Vendor and business associate email exposure

What the 2025 HHS data shows

Vendor and business associate email exposure was the most common email breach pattern in 2025, responsible for 28% of all email incidents reported to HHS. Breaches involving third-party vendors are also among the most expensive, with an average cost of \$4.9 million per incident, according to IBM.²

In these incidents, the covered entity did not always experience a direct technical failure. PHI was exposed through email communication with a vendor or partner. When business associates are involved, breach sizes are typically larger and impact multiple organizations at once.

How this attack works

Vendor-related email exposure follows two paths:

- A vendor's email account is compromised, exposing PHI from multiple covered entities
- PHI is sent to a vendor using email that is assumed to be secure but is not protected

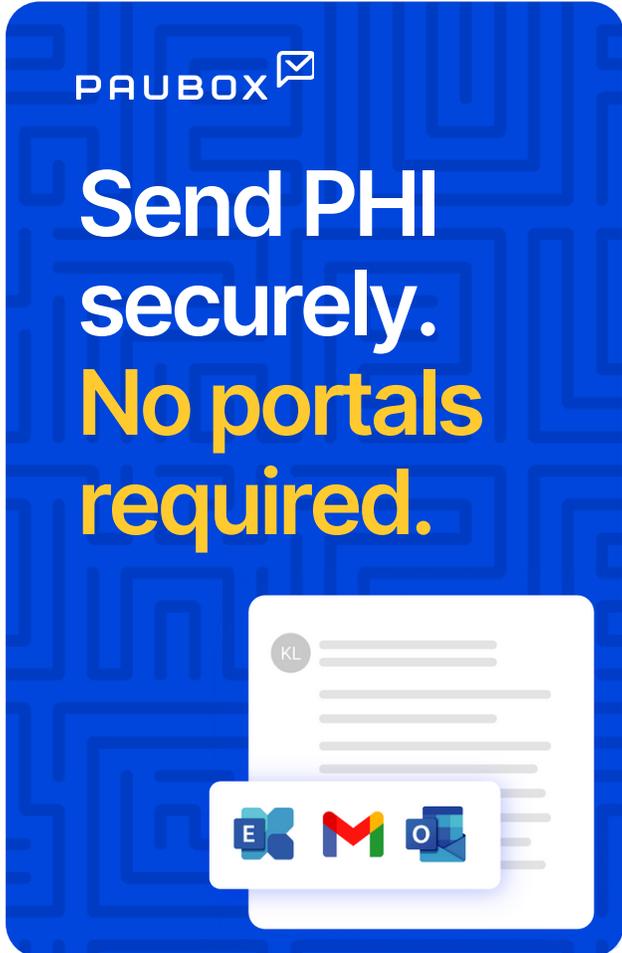
In both cases, the covered entity remains accountable for protecting PHI during transmission.

Where defenses fail

These breaches persist because email security expectations vary across organizations.

Common breakdowns:

- Relying on business associate agreements instead of technical safeguards
- Inconsistent encryption practices across organizations and vendors
- Limited visibility into how PHI is handled after delivery

A blue rectangular graphic with a white maze pattern in the background. At the top left, the word "PAUBOX" is written in white, followed by a white envelope icon. In the center, the text "Send PHI securely." is written in white, and "No portals required." is written in yellow. At the bottom right, there is a white rounded rectangle containing a stylized email interface with a grey header, a circular profile picture with the letters "KL", and several lines of grey text. Below this rectangle are three overlapping icons: a blue "E" icon, a red "M" icon, and a blue "O" icon.

How Paubox reduces risk

Paubox reduces vendor-related email risk by enforcing protection at the point of sending.

With Paubox:

- All email is encrypted automatically
- Protection does not depend on the vendor's email configuration

This ensures PHI is safeguarded in transit, which is the covered entity's responsibility.

Why this attack persists

"Healthcare organizations report limited visibility into third-party cybersecurity controls, despite increasing reliance on vendors for core operations", according to EY.⁶

The 2025 HHS data shows that when email protection varies across organizations, exposure scales quickly. Reducing that risk requires enforcing protection before PHI leaves the sender's control.

"Healthcare organizations report limited visibility into **third-party cybersecurity controls**, despite increasing reliance on vendors for core operations."

EY

HIPAA BREACHES ARE ON THE RISE

Cybercriminals are targeting healthcare

Stop attacks with generative AI that detects subtle anomalies in language, behavior, and context that traditional filters overlook.

[Explore Paubox Email Suite Plus](#)

Stop email phishing attacks with AI security

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

[Talk to an expert](#)

