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

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.

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

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.

PAUBOX

Stop email phishing attacks with AI security

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

Talk to an expert