PAUBOX RESEARCH

PAUBOX

Vendor email exposure was the most common breach pattern

28% of 2025 email breaches involved a vendor or business associate, the single most common pattern in the HHS data.

What we found

28% of 2025 email breaches involved a vendor or business associate.

PHI is exposed when a vendor account is compromised or when email sent to a vendor is assumed secure but is not. The covered entity stays accountable for protecting PHI in transit. Third-party breaches are among the most expensive, at an average of $4.9 million per incident.

What it means for buyers

Vendors were the most common path
28% of 2025 email breaches involved a vendor or business associate.

Assumed secure, actually not
PHI is sent to vendors over email that is presumed protected but is not encrypted.

Agreements are not safeguards
Relying on business associate agreements instead of technical controls leaves PHI exposed.

WHY PAUBOX

100%

of outbound Paubox email is encrypted by default, secured at TLS 1.2 or higher.

Encrypted at the point of sending
All outbound email is encrypted automatically, whatever the vendor's configuration.

A business associate that passes vetting
Paubox meets the technical safeguards covered entities are accountable for.

HITRUST certified
Annual third-party audit of every control.

Sources: Paubox 2026 research, Top 3 Healthcare Attacks in 2025 | IBM Cost of a Data Breach Report 2025 | EY U.S. Healthcare Cyber Resilience Survey 2025 | U.S. HHS Office for Civil Rights breach portal (January to December 2025).