PAUBOX

Executive summary

In 2025, the United States Department of Health and Human Services (HHS) recorded 170 email-related healthcare breaches, affecting more than 2.5 million individuals.[1]

A review of HHS breach data from January through December 2025 shows that nearly every email-related breach falls into one of three attack patterns:

Mailbox takeover after credential theft
Stolen usernames and passwords allow attackers to log into employee inboxes and access PHI as legitimate users. Credential-based mailbox takeovers accounted for the largest share of exposed patient data.

Executive and vendor impersonation
Attackers pose as trusted individuals, executives, vendors, or internal staff, to trick recipients into sharing sensitive information.

Third-party and business associate email exposure
PHI is exposed through compromised or insecure email communication with vendors and partners. Nearly one in three breaches in 2025 involved a business associate.

This report isolates how these three attacks work, where defenses fail, and which email controls reduce risk. The focus is practical. What to fix first. What to stop relying on. What prevents the next breach.

These attacks rely on fast-moving healthcare workflows and email systems that still assume people will catch mistakes before damage occurs. Each of these attack types triggered reportable breaches in 2025. Many remain under investigation. All represent ongoing compliance and operational risk.

BY THE NUMBERS

170
email-related breaches occurred in 2025

28%
of breaches reported last year were from vendor and business associate email exposure

630,000
individuals were exposed in 2025 by phishing-driven mailbox takeovers

2.5 million
individuals were affected by all email-related breaches in 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