

The healthcare CISO's guide to vendor vetting

56% of mid-market healthcare IT and security leaders tie an incident directly to a vendor's email security. 57% of those organizations stop short of a formal assessment.

What we found

56% of mid-market healthcare IT and security leaders say a vendor's email security directly contributed to a breach or security incident.

Among those 75 organizations, 57% evaluate a vendor's email security before a BAA with a basic questionnaire or the BAA itself, rather than a formal security assessment.

What it means for CISOs



44 state AGs required vendor verification

A 2026 settlement requires one lab company to verify vendor compliance and keep an officer-level CISO over its security program.



Check the method behind BAA reviews

Across organizations, 70% of CIO, CTO, CISO, and VP respondents report formal assessments, versus 36% of IT and security directors.



Vendor security is part of breach risk

In Verizon's 2026 data, third parties were involved in 32% of 1,438 healthcare breaches.

WHY PAUBOX

9,000+

healthcare organizations trust Paubox to secure every email they send and receive.



Evidence a formal review can use

HITRUST certification means an annual third-party audit of every control.



Encryption by default

Every outbound email is encrypted automatically, with nothing for staff to do.



BAA included

Paubox signs a business associate agreement with its customers.