PAUBOX RESEARCH

PAUBOX

Outbound email encryption for healthcare IT directors

57% of breached organizations that implemented or strengthened encryption policies still don't encrypt all outbound email by default.

What we found

73% of organizations relying on senders to encrypt reported an email breach in the past 24 months, against 52% using default encryption.

If S.3315 becomes law, HIPAA would require encryption of PHI 36 months after enactment, alongside MFA and monitoring.

What it means for IT directors

One missed step sends PHI unencrypted

With sender-triggered encryption, a message holding PHI goes out unencrypted whenever the sender skips the step.

Partial coverage leaves gaps between departments

When only some departments encrypt by default, PHI from the rest still depends on the sender.

Manual coverage is hard to prove

When encryption depends on the sender, showing an auditor that every PHI message was encrypted gets harder.

WHY PAUBOX

100%

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

Nothing for senders to remember

Staff send from Microsoft 365 or Google Workspace as usual, with no extra step.

Archiving preserves email for review

Email is preserved for compliance audits and eDiscovery.

HITRUST certified

Annual third-party audit of every control.

Paubox survey of 170 healthcare IT and security leaders, March 2026 | Health Care Cybersecurity and Resiliency Act (S.3315), Congressional Record, September 30, 2026.