PAUBOX RESEARCH

PAUBOX

Email incident response for healthcare security teams

44% of organizations with a recent email breach hold an untested email incident plan, against 9% of organizations with no email breach.

What we found

39% of healthcare IT and security leaders don't have a tested, email-specific incident response plan.

A tabletop tests what a written plan can't: whether an email incident reaches the person who decides it's reportable. The survey can't show whether untested plans came before or after a breach.

What it means for security teams

The CIRCIA clock starts at a judgment call

The 2024 proposal set 72 hours from when an entity reasonably believes a covered incident occurred.

Compromised mailboxes held the PHI

24.9% of large 2025 healthcare breaches involved compromised email accounts, as of HIPAA Journal's February 2026 OCR tally.

Recovery often runs past a month

38% of organizations with a recent email breach took more than a month to fully recover.

WHY PAUBOX

9,000+

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

Inbound Email Security catches phishing

Generative AI detects phishing, spoofing, and BEC in inbound email.

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 | Cybersecurity and Infrastructure Security Agency, CIRCIA notice of proposed rulemaking (April 2024) | HIPAA Journal, CIRCIA final rule coverage (October 2026) | HIPAA Journal, 2025 Healthcare Data Breach Report (February 2026).