PAUBOX RESEARCH

PAUBOX

# Shadow AI multiplies the risk of existing email gaps

85% of healthcare IT leaders suspect staff use unauthorized AI tools, but only 26% have visibility into that use.

## What we found

**85% of healthcare IT leaders suspect staff are using unauthorized AI tools.**

Only 26% have visibility into that use, and more than two thirds have already found unsanctioned AI adoption. As AI raises the volume of email, more PHI moves through the same systems, and manual safeguards like deciding when to encrypt grow less reliable. AI widens the consequences of gaps already there.

## What it means for buyers

**Unauthorized AI is widespread**
85% of healthcare IT leaders suspect staff are using unauthorized AI tools.

**Almost no visibility**
Only 26% have visibility into that AI use, and most have already found unsanctioned adoption.

**Manual safeguards stop scaling**
As email volume rises, choosing when to encrypt grows less reliable and PHI slips through.

WHY PAUBOX

**0**

plaintext sends. Every outbound Paubox email is encrypted by default.

**No human decision to encrypt**
Every outbound email is encrypted automatically, so protection never depends on staff judgment.

**Inbound Email Security**
Behavioral AI catches AI-generated phishing and impersonation in inbound email.

**HITRUST certified**
Annual third-party audit of every control.

*Sources: Paubox 2026 research, 2026 Healthcare Email Security Report (analysis of 2025 healthcare email breaches).*