PAUBOX RESEARCH

PAUBOX

# By default, Amazon SES sends PHI in plaintext

Amazon SES attempts encryption without requiring it. When the receiving server offers none, the message goes out in the clear.

## What we found

**In default tests, Amazon SES delivered PHI in plaintext whenever the receiver offered no TLS.**

Amazon SES uses opportunistic TLS. It tries to encrypt every message, and when the handshake cannot complete, it sends anyway. The receiver does not need to be malicious. A small clinic or partner running an outdated mail server is enough, and the sender still sees a normal delivery.

## What it means for buyers

**Encryption is optional by default**
Default SES tries TLS, then sends in plaintext when the receiver offers none.

**Delivery looks successful regardless**
The sender sees a normal delivery even when PHI went out unencrypted.

**The receiver doesn't have to be hostile**
An outdated partner or clinic mail server is enough to expose PHI.

WHY PAUBOX

**0**

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

**A hard encryption requirement**
Paubox sends PHI only over authenticated TLS, or to a patented Secure Message Center.

**No plaintext fallback**
PHI never leaves over an unencrypted connection. The secure path is the only alternative.

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

*Sources: Paubox 2026 research, How Amazon SES puts PHI at risk | Amazon SES Developer Guide (April 2026).*