SECTION 04

What secure email looks like

For Paubox, TLS 1.2 or higher is required. All emails either transit over a modern, authenticated TLS session, or fallback to a patented Secure Message Center.

Amazon SES vs. Paubox at every receiver state

Paubox checks each receiver's TLS support before sending. If the receiver offers TLS 1.3 or TLS 1.2 with a valid certificate, the message is delivered over that connection. Otherwise it routes to the Paubox Secure Message Center.[6]

RECEIVER STATE	AMAZON SES (DEFAULT)	AMAZON SES (REQUIRE TLS)	PAUBOX
TLS 1.3 + valid cert	✓ Delivered TLS 1.3	✓ Delivered TLS 1.3	✓ Delivered TLS 1.3
TLS 1.2 + valid cert	✓ Delivered TLS 1.2	✓ Delivered TLS 1.2	✓ Delivered TLS 1.2
TLS 1.1	⚠ Delivered TLS 1.1	⚠ Delivered TLS 1.1	✓ Secure Message Center
TLS 1.0	⚠ Delivered TLS 1.0	⚠ Delivered TLS 1.0	✓ Secure Message Center
No TLS	⚠ Delivered plaintext	✓ Bounced	✓ Secure Message Center
Expired cert	⚠ Delivered TLS 1.3	⚠ Delivered TLS 1.3	✓ Secure Message Center
Self-signed cert	⚠ Delivered TLS 1.3	⚠ Delivered TLS 1.3	✓ Secure Message Center

A hard requirement, not a best-effort

SES treats TLS as best-effort. Paubox treats TLS as a hard requirement. The difference between those two postures is a configuration choice every healthcare sender has to make, and the consequences land directly on the recipient's protected health information.

For Paubox, TLS 1.2 or higher is required. An email containing PHI either transits over a modern, authenticated TLS session, or routes to a patented Secure Message Center.

That approach matches what the HIPAA Security Rule's encryption-in-transit standard was written to describe, and it is the same implementation the proposed reclassification from "addressable" to "required" anticipates.[4]

The Paubox model treats encryption as a precondition for sending, not as a property the sender hopes the network provides. When the receiving server cannot meet modern TLS standards, the message takes a different path entirely. The PHI never crosses the public internet under weak protection.

> "TLS being on is not the same as PHI being protected. 'Require TLS' on Amazon SES enforces neither a minimum version nor certificate validation."
>
> **Hoala Greevy**
> Founder and CEO, Paubox

Send PHI securely, every time.
Paubox requires modern TLS and routes anything weaker to our Secure Message Center. No downgrading. No plaintext.

Talk to an expert

PAUBOX

Secure every email you send and receive

Paubox combines healthcare compliance with AI to protect organizations from the most sophisticated attacks.

Talk to an expert