# 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 |

THE TOP-LEVEL FINDINGS

# What we found

Fourteen controlled tests surfaced four patterns in how Amazon SES handles healthcare email.

## Plaintext

DEFAULT BEHAVIOR

SES attempts Transport Layer Security (TLS) but does not require it. When the receiving server offers no TLS, PHI sends in plaintext.

## 2021

YEAR IETF RETIRED TLS 1.0 AND 1.1

SES still delivers over both retired protocols, even with the "Require TLS" configuration enabled.[2]

## 0 of 4

CERT FAILURE TESTS BLOCKED BY SES

Self-signed and expired certificates all delivered, including with "Require TLS" enabled.

## Contradicts

SES DOCS SAY ONE THING. SES DOES ANOTHER.

SES documentation states the service "requires TLS 1.2 and recommends TLS 1.3." [1] The observed behavior does not match.

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