PAUBOX RESEARCH

PAUBOX

Amazon SES has three encryption gaps that expose PHI

Amazon documents a TLS 1.2 minimum. PHI still ships over retired protocols, to invalid certificates, and in plaintext.

What we found

Across 14 controlled tests, Amazon SES failed to enforce the encryption its documentation requires.

Amazon tells developers Simple Email Service requires TLS 1.2 and recommends TLS 1.3. The recorded behavior does the opposite. It delivers over protocols retired in 2021, accepts invalid certificates, and falls back to plaintext when a receiver offers no encryption.

What it means for buyers

Plaintext is the default fallback
When the receiving server offers no TLS, SES delivers PHI across the open internet unencrypted.

Retired protocols still go through
SES delivers over TLS 1.0 and 1.1, versions retired across the industry since 2021.

Invalid certificates are never blocked
SES blocked 0 of 4 invalid-certificate tests, delivering to self-signed and expired certificates.

Sources: Paubox 2026 research, How Amazon SES puts PHI at risk | Amazon SES Developer Guide (April 2026) | IETF RFC 8996, Deprecating TLS 1.0 and TLS 1.1 (March 2021).