SECTION 02

Default SES sends PHI in plaintext

"Require TLS" is opt-in. By default, Amazon SES uses opportunistic TLS. When the receiving server offers no TLS, the message sends in plaintext anyway.

What SES delivers at every TLS state

SES attempts an encryption handshake on every outbound message. If that handshake fails for any reason, including the receiving server not offering TLS at all, the message sends anyway in plaintext.

RECEIVER TLS OFFERED	SES DELIVERY (DEFAULT CONFIGURATION)
TLS 1.3	✓ Delivered over TLS 1.3
TLS 1.2	✓ Delivered over TLS 1.2
TLS 1.1	⚠ Delivered over TLS 1.1 (deprecated)
TLS 1.0	⚠ Delivered over TLS 1.0 (deprecated)
None	⚠ Delivered in plaintext

Any healthcare organization or healthtech vendor running default SES is one misconfigured receiving server away from sending protected health information as plaintext across the open internet. The receiving server does not have to belong to a bad actor for that to happen. It could be a small clinic, a specialty lab, or a partner organization running an older mail server.

This is precisely the pattern that produces the breaches Paubox documented in last year's research. The 2026 Healthcare Email Security Report counted 170 email-related breach incidents reported to HHS in 2025,[5] and the configuration gaps behind them follow the same shape every time: a sender that does not require any encryption, paired with a receiver that has not kept its mail server up to date.

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