Executive summary

Amazon Simple Email Service (SES) puts protected health information (PHI) at risk by default. SES documentation tells developers the service "requires TLS 1.2 and recommends TLS 1.3."[1] Our testing results, however, contradict this claim.

Three problems surfaced in testing. SES sometimes sends PHI in plaintext. Other times, it encrypts using outdated protocols that standards bodies retired in 2021.[2] SES also accepts invalid security certificates from the receiving server, which means it could deliver an email to an impersonator instead of the intended recipient.

AWS offers a setting called "Require TLS" that sounds like it would fix all of this. It only fixes one of the three problems: the plaintext case. The outdated-protocol and bad-certificate gaps stay open.

This matters for healthcare because HIPAA's encryption rules are about to tighten.[4]

BY THE NUMBERS

14

controlled tests run by Paubox against Amazon SES sending infrastructure.

0 of 4

invalid security certificates were blocked by Amazon SES.

2021

was the year IETF retired TLS 1.0 and 1.1. SES still delivers over both.

Only 1 of 3

gaps closed by Amazon SES's "Require TLS" setting. The other two stay open.

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