PAUBOX

2025 REPORT

How Microsoft and Google put PHI at risk

We tested their encryption claims. What we found shows just how often patient data is left unprotected.

Executive summary

In a recent experiment, Paubox tested what actually happens when Google Workspace and Microsoft 365 are forced into encryption edge cases.

What we found was alarming:

- Google will still deliver messages using TLS 1.0 and 1.1, encryption protocols deprecated years ago.
- Microsoft refuses those outdated protocols, but sends the message anyway, completely unencrypted.

Forcing TLS sounds like a safeguard. Configure your email platform to require encryption for outbound messages, and if the recipient's server doesn't support it, the email bounces. Nothing gets through unless it's protected. That's the assumption.

In healthcare, where email routinely carries sensitive patient data, the illusion of security is especially dangerous because when encryption silently fails, there's no second chance to catch the mistake.

No error. No alert. Just delivery that looks successful, but isn't secure.

This report walks through our testing process, explains why force TLS creates a false sense of security, and outlines the technical, regulatory, and human consequences when encryption fails silently. If your HIPAA compliance strategy depends on TLS settings you haven't tested, this is your warning.

We also unpack what's at stake: lawsuits, OCR investigations, patient disruption, and operational chaos. Most importantly, we outline what IT leaders should do to get out of this gray zone—and into an email infrastructure that delivers provable encryption, every time.