

The myth of “force TLS”

“If it bounces, it must be secure” —right?

In theory, enabling “force TLS” in cloud email platforms sounds OK. It ensures that messages are only delivered if the recipient’s mail server supports encryption. If it doesn’t, the message bounces. No delivery, no risk. Simple. But this approach is built on assumptions that don’t hold up. The biggest problem? Force TLS doesn’t guarantee that the encryption used is strong, current, or even acceptable by today’s regulatory standards.

Let’s break it down.

Force TLS relies on the sending server to try to establish a secure connection. However, it doesn’t control which version of TLS is used. If the recipient only supports TLS 1.0 or 1.1, platforms like Google Workspace will use those protocols. Both TLS 1.0 and 1.1 are outdated, vulnerable to downgrade attacks, and explicitly flagged by the NSA as unsafe for any use in federal systems.

Microsoft 365 takes a different path. If secure transmission isn’t possible—because the recipient doesn’t support a modern TLS version—it still sends the message, but unencrypted as cleartext. No fallback, no failure notice, no indication to the sender that anything went wrong. The message gets delivered, just not securely.

The myth here is thinking that force TLS is a hard barrier. In reality, it’s a handshake that tolerates unsafe conditions behind the scenes. It’s encryption by best effort, not by guarantee. That’s not good enough for PHI.

Healthcare regulations require more than checkbox compliance. They need clarity, enforcement, and verifiable encryption. Force TLS doesn’t deliver any of that.

“Force TLS gives you just enough confidence to stop asking questions—until something breaks.”

Hoala Greevy
CEO, Paubox

HIPAA IMPLICATIONS

Force TLS failures directly intersect with HIPAA Security Rule §164.312(e)(1), which requires covered entities to implement technical safeguards to protect ePHI during transmission.⁴

If email is sent over deprecated TLS protocols—or worse, without any encryption—it can trigger breach notification requirements under the HIPAA Breach Notification Rule.

OCR has repeatedly cited transport encryption failures in major enforcement actions.

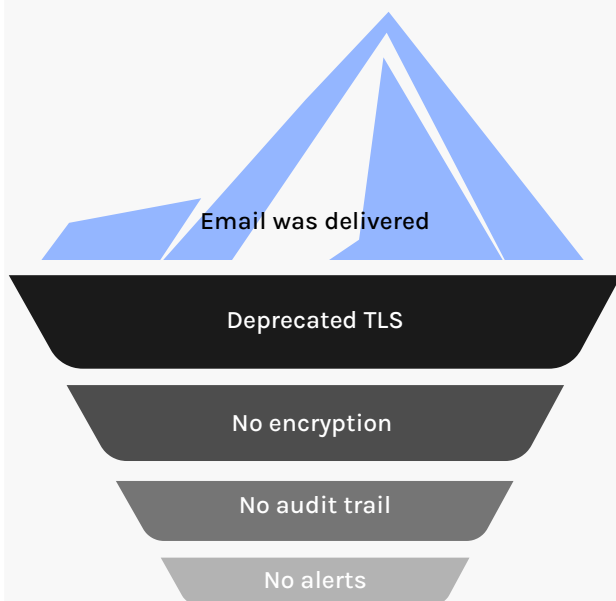
When encryption fails, people pay the price

This goes beyond data security. These failures ripple through care delivery, operations, and patient trust.

- **Delayed care:** Messages with lab results, medication changes, or discharge instructions may not arrive—or arrive unsecured, prompting workflow disruptions.
- **Lost trust:** Patients lose confidence when their information is exposed or their care is impacted by a breach.
- **Operational strain:** IT and compliance teams get pulled into audits, investigations, and breach notification cycles.
- **Legal and financial consequences:** HIPAA-related breaches cost healthcare organizations an average of \$9.8 million per incident, factoring in class action lawsuits, fines, and recovery costs.¹

In a sector where every message could carry sensitive information, every encryption failure is a potential breach.

WHAT YOU DON'T SEE



ONLY 5% of known phishing attacks are reported by staff