

The experiment

Testing Google Workspace and Microsoft 365 under controlled conditions

To understand how force TLS actually performs in the real world, we ran a controlled experiment.

The goal: Simulate scenarios where encryption should be enforced, and see what Google Workspace and Microsoft 365 actually do under pressure.

Setup

We created business email accounts on both Google Workspace and M365. To simulate real-world vulnerabilities, we configured test recipient mail servers to only accept the deprecated protocols TLS 1.0 and TLS 1.1. These setups mimic legacy systems still found in smaller clinics, vendor environments, or rural networks.

This controlled environment allowed us to observe how each platform handles a handshake with an outdated recipient configuration. All message headers were

captured and analyzed to determine the actual encryption protocols used—or bypassed—during transmission.

Then, we set up recipient mail systems that only accept legacy TLS protocols—first TLS 1.0, then TLS 1.1. Any organization that exchanges email across a broad healthcare ecosystem is likely to encounter them. We sent emails from each platform to these recipient servers and captured the message headers to analyze the encryption protocols used during transmission.

Limitations:

These tests reflect platform behavior under specific conditions. Results may vary with different admin settings or policy configurations. However, the fallback behaviors we observed are consistent with known documentation and repeatable in similar controlled environments.

PAUBOX 

Peace of mind.
Stop worrying if your email is
HIPAA compliant.

Test 1: TLS 1.0

- Google Workspace: Delivered the message using TLS 1.0—an obsolete encryption protocol deprecated by the NSA, NIST, and every major security standards body.
- M365: Refused to use TLS 1.0, but still delivered the message—unencrypted, in cleartext.

Result:

Google violated security best practices to preserve delivery. Microsoft preserved delivery by bypassing encryption entirely. Neither behavior aligns with HIPAA expectations or regulatory guidance.

Test 2: TLS 1.1

- Google Workspace: Again, delivered the message using TLS 1.1, another protocol explicitly deprecated due to known weaknesses.
- M365: Again, refused the connection but defaulted to unencrypted delivery.

Result:

Same story. Legacy protocols were either used (Google) or ignored (Microsoft), but in both cases, encryption failed to meet modern standards.

GOOGLE WORKSPACE MESSAGE HEADER SNIPPET

```
Received: from mail-ed1-  
f48.google.com (mail-ed1-  
f48.google.com [209.85.208.48])  
(using TLSv1 with cipher ECDHE-  
RSA-AES256-SHA (256/256 bits))  
(No client certificate requested)  
by ****.paubox.com (Postfix) with  
ESMTPS id 4ZyyLQ3n7dz5nKM  
for <***@paubox.us>; Thu, 15 May  
2025 17:46:05 +0000 (UTC)
```

GOOGLE WORKSPACE MESSAGE HEADER SNIPPET

```
Received: from mail-ed1-  
f50.google.com (mail-ed1-  
f50.google.com [209.85.208.50])  
(using TLSv1.1 with cipher ECDHE-  
RSA-AES256-SHA (256/256 bits))  
(No client certificate requested)  
by ***.paubox.com (Postfix) with  
ESMTPS id 4ZyyH54ZgJz5nKM  
for <***@paubox.us>; Thu, 15 May  
2025 17:43:13 +0000 (UTC)
```

M365 MESSAGE HEADER SNIPPET

```
Received: from NAM12-BN8-  
obe.outbound.protection.outlook.c  
om (mail-bn8nam12on2132.  
outbound.protection.outlook.com  
[40.107.237.132])  
by ***.paubox.com (Postfix) with  
ESMTP id 4ZyxcR2V2xz5nKM  
for <***@paubox.us>; Thu, 15 May  
2025 17:13:10 +0000 (UTC)
```

M365 MESSAGE HEADER SNIPPET

```
Received: from NAM11-CO1-  
obe.outbound.protection.outlook.c  
om (mail-co1nam11on2090.  
outbound.protection.outlook.com  
[40.107.220.90])  
By ***.paubox.com (Postfix) with  
ESMTP id 4Zyy0R3Mz3z5nKM  
for <***@paubox.us>; Thu, 15 May  
2025 17:30:30 +0000 (UTC)
```

How common is this?

Misconfigurations like the ones shown in our experiment are not isolated events—they're disturbingly prevalent across healthcare organizations of all sizes.

- 31.1% of breached healthcare orgs had misconfigurations that exposed them to major email risks¹
- Microsoft 365 alone accounted for 43.3% of all healthcare email breaches in 2024¹
- Downgrade behaviors and weak encryption protocols remain systemic,

often due to legacy systems and intermediary devices. These configurations are common in under-resourced or decentralized healthcare environments—particularly in rural settings—where email remains a primary mode of communication but security investments lag behind.²

Many organizations treat force TLS as a budget workaround—using it to satisfy security checkboxes without allocating funds for dedicated, policy-based encryption. It lets teams claim email is 'secured' without the cost of proven solutions. But that illusion can lead to dangerous exposure.

WHY THIS MATTERS

Force TLS settings give IT teams the illusion of control. But what we found shows that platforms make their own decisions behind the scenes—favoring deliverability over security, without notifying the sender. Encryption doesn't just fail, it fails silently.

According to a 2023 ACM study, in many cases, devices silently downgrade or re-encrypt traffic

without preserving end-to-end security.² For healthcare organizations, this means even when TLS appears active, the contents of a message may be vulnerable. It reinforces a hard truth: relying on TLS alone, especially without enforcement or visibility, is no longer sufficient to protect PHI.

There's no audit trail showing encryption was bypassed. No bounce. No alert. Just exposure.