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.

Table of contents

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- Microsoft refuses those outdated protocols, but sends the message anyway, completely unencrypted.

Healthcare organizations depend on email to share everything from lab results to care instructions. So when platforms like Microsoft 365 and Google Workspace promise encryption, most IT teams take that promise at face value.

That trust may be misplaced. Despite appearances, these platforms can deliver messages using deprecated encryption protocols—or none at all—without warning the sender. It's a built-in failure mode that leaves sensitive data exposed and compliance assumptions shattered.

This report exposes a security failure: email platforms that claim to encrypt by default often don't—at least, not in the ways IT leaders expect. Through testing and real-world examples, we reveal how encryption breaks down inside Microsoft 365 and Google Workspace, and the dangerous assumptions this creates in healthcare environments.

If your HIPAA compliance strategy depends on TLS settings you haven't tested, this is your warning.

We also unpack what's at stake: a false sense of compliance and security, 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.

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.

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.

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)
```

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)
```

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-
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 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 risks[1]
- Microsoft 365 alone accounted for 43.3% of all healthcare email breaches in 2024[1]
- 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.

Why the NSA deprecated TLS 1.0 and 1.1

Outdated protocols are unsafe by design

In 2021, the National Security Agency (NSA) issued formal guidance on encryption standards. It was unambiguous:

"NSA recommends that only TLS 1.2 or TLS 1.3 be used; and that SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 not be used."[5]

This was a direct response to known vulnerabilities that attackers routinely exploit.

Here's why the NSA—and nearly every other standards body—has moved to deprecate earlier versions of TLS.

> "NSA recommends that only TLS 1.2 or 1.3 be used..."[5]
>
> NSA Guidance on Eliminating Obsolete TLS Protocols

What's wrong with TLS 1.0 and 1.1?

1. Weak cipher suites
These protocols support encryption methods that can be cracked with modern computing power—exposing email contents to interception.

2. No protection against downgrade attacks
An attacker can trick a system into accepting a weaker connection, then eavesdrop or alter the data in transit.

3. Lacking modern cryptographic protections
TLS 1.2 and 1.3 introduced stronger authentication, forward secrecy, and resistance to known exploits.

4. Out of compliance with federal and industry standards
NIST, DHS, and multiple industry frameworks no longer consider TLS 1.0 or 1.1 acceptable for protecting sensitive or regulated data—including PHI.

If federal agencies can't use them, why can your email provider?

RFC 8996, published by the Internet Engineering Task Force (IETF) in 2021, formalized what security experts had already concluded: TLS 1.0 and 1.1 are insecure by design. The RFC explicitly states that these protocols 'MUST NOT be used,' citing their lack of support for modern cipher suites and vulnerability to downgrade attacks. It also notes that TLS 1.2 is now widely deployed, eliminating the need for backward compatibility.[6] Continued use in modern systems—especially by cloud email providers—is no longer justifiable, even for legacy interoperability.

There is broad consensus that these versions should not be used under any circumstances, yet leading email providers continue to allow or silently fall back to them.

> "Using obsolete encryption provides a false sense of security because it seems as though sensitive data is protected, even though it really is not."[5]
>
> NSA Guidance on Eliminating Obsolete TLS Protocols

That's the uncomfortable truth. Google Workspace still allows transmission using TLS 1.0 and 1.1. Microsoft 365 won't use them—but instead of rejecting the message entirely, it delivers it in cleartext.

Neither approach would be permitted in federal systems. But they're happening every day in healthcare.

For organizations that handle PHI, that gap is indefensible.

TLS PROTOCOLS: SECURE VS. DEPRECATED

Acceptable	Deprecated
TLS 1.2	TLS 1.0
TLS 1.3	TLS 1.1

CLOUD PLATFORMS' TLS DOUBLE STANDARD

Google Workspace:
Allows delivery over TLS 1.0 and 1.1, despite browser-level deprecation in Chrome

Microsoft 365:
Rejects TLS 1.0/1.1 but silently delivers in cleartext with no bounce

How bad actors exploit TLS gaps

Weak transport encryption invites attack

As noted by the Journal of Computing and Information Technology, "Downgrade attacks thrive on backward compatibility… attackers can force communication to fall back to SSL 3.0 or TLS 1.0, exposing sensitive data."[3] This reinforces the urgency of enforcing modern TLS protocols and eliminating outdated versions from your infrastructure.

TLS downgrade is more than a compliance issue. Attackers know exactly how to exploit this vulnerability.

When a message is transmitted over outdated encryption—or none at all—it becomes easy to intercept, manipulate, or impersonate. Threat actors just need to sit between sender and recipient and wait for a platform to fall back to an insecure connection.

Common attacks tied to weak TLS enforcement

1. Man-in-the-middle (MITM) attacks
If a message is downgraded to TLS 1.0 or 1.1, attackers can intercept it in transit. These older protocols lack protections against modern MITM tactics, allowing attackers to view, modify, or reroute sensitive data.

2. Downgrade attacks
Even when higher versions of TLS are available, attackers can interfere with the handshake to force a downgrade to a weaker protocol—one they can decrypt.

3. Spoofing and impersonation
Messages sent in cleartext (as we saw with M365) can be intercepted, copied, and used to craft nearly identical phishing emails. Combined with display name spoofing, attackers can convincingly pose as care providers, finance teams, or even patients.

4. Credential theft
Unsecured login prompts, password reset links, or shared URLs sent in plaintext can be intercepted and reused. In healthcare, this can mean unauthorized access to billing portals, patient portals, or even EHR systems.

5. Ransomware delivery
Once inside the network, attackers often deploy ransomware via email attachments or malicious links. An intercepted message gives them a clean entry point—one the sender thinks was secure.

Weak encryption = weak perimeter

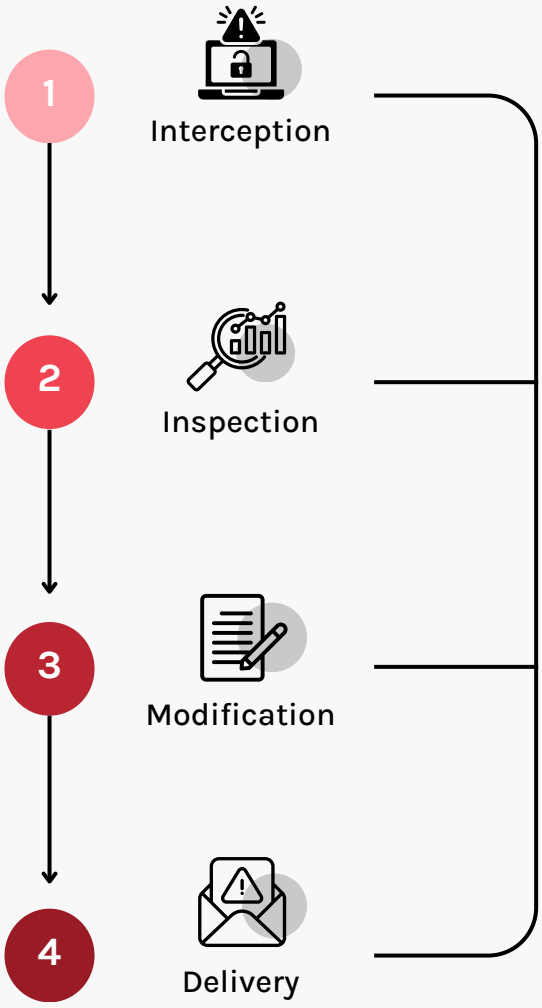
Most IT teams assume that once an email leaves their infrastructure, it's protected by TLS. But the minute it downgrades—or skips encryption entirely—the attack surface shifts from “unlikely” to “active opportunity.”

Attackers don’t need to guess where to look. They target healthcare specifically because they know:

- It’s heavily reliant on email
- It’s underfunded in cybersecurity
- And it’s full of false confidence in legacy tools (link to report)

Without enforced modern encryption, sending an email can become an open invitation for attackers.

HOW MALWARE EXPLOITS WEAK TLS



"Downgrade attacks thrive on backward compatibility... attackers can force communication to fall back to SSL 3.0 or TLS 1.0, exposing sensitive data."[3]

Journal of Computing and Information Technology

What about inbound threats?

While this report focuses on outbound encryption, inbound email threats represent a significant and often overlooked risk. Spoofed email headers, display name impersonation, and phishing emails targeting providers and staff are still among the most common—and effective—entry points for attackers.

Solutions like Paubox ExecProtect+ are designed to neutralize these risks by blocking spoofed and impersonated emails before they ever reach the inbox. There are no plugins to manage and no behavior to retrain—just automatic protection built for healthcare environments.

A complete email security strategy requires both outbound encryption and inbound protection. Without both, gaps remain.

Why this matters for healthcare

This risk plays out in healthcare systems every single day

Healthcare organizations use email to communicate everything from care coordination and lab results to discharge instructions, referrals, billing, and insurance claims. Unlike portal-based systems, email goes beyond internal networks—it reaches patients, partners, and vendors who may not have modern security infrastructure.

That makes the transport layer—the invisible layer between send and receive—critical. If encryption fails there, it fails everywhere.

When platforms like Google Workspace and Microsoft 365 fall back to obsolete protocols or skip encryption entirely, the implications are immediate:

- Protected Health Information (PHI) is exposed in transit
- Senders never know the message wasn't protected
- No logs, no alerts, no way to prove if the message was encrypted or not
- HIPAA violations become inevitable, even if intent was compliance

> "While email remains the main communication tool in healthcare, it still poses as the weakest form of security."[8]
>
> **Briana Contreras**
> Managed Healthcare Executive

KEY TAKEAWAY

Outdated TLS configurations and certificate mismanagement are consistently listed among the top security risks—even in API environments. [3]

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.

WHAT YOU DON'T SEE

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.

ONLY 5% of known phishing attacks are reported by staff

Fallout from a successful breach

A single failure in email encryption can trigger a cascade of consequences—technical, operational, and reputational

When PHI is exposed due to weak or missing encryption, the consequences don't stop at a compliance violation. Breaches disrupt operations, drain resources, damage reputations, and erode trust with the people healthcare organizations are meant to serve.

And they're not rare.

In 2024 alone, 180 healthcare organizations reported email-related breaches to the HHS Office for Civil Rights (OCR). Many were caused by preventable misconfigurations or gaps in transport security.[1]

Legal and regulatory action

- Mandatory breach notifications to HHS, media, and affected patients
- Investigations by OCR into HIPAA Security Rule violations
- Fines and settlements, often in the millions. The average cost of a healthcare data breach? $9.8 million, according to IBM.[1]

Case in point

Solara Medical Supplies paid a $3 million OCR settlement and a $9.76 million class action settlement after an email breach exposed over 114,000 patient records.[1]

HIPAA BREACHES ARE ON THE RISE

Cybercriminals are targeting healthcare

Paubox Email Suite Plus keeps your organization secure and patient data safe

Operational and clinical disruption

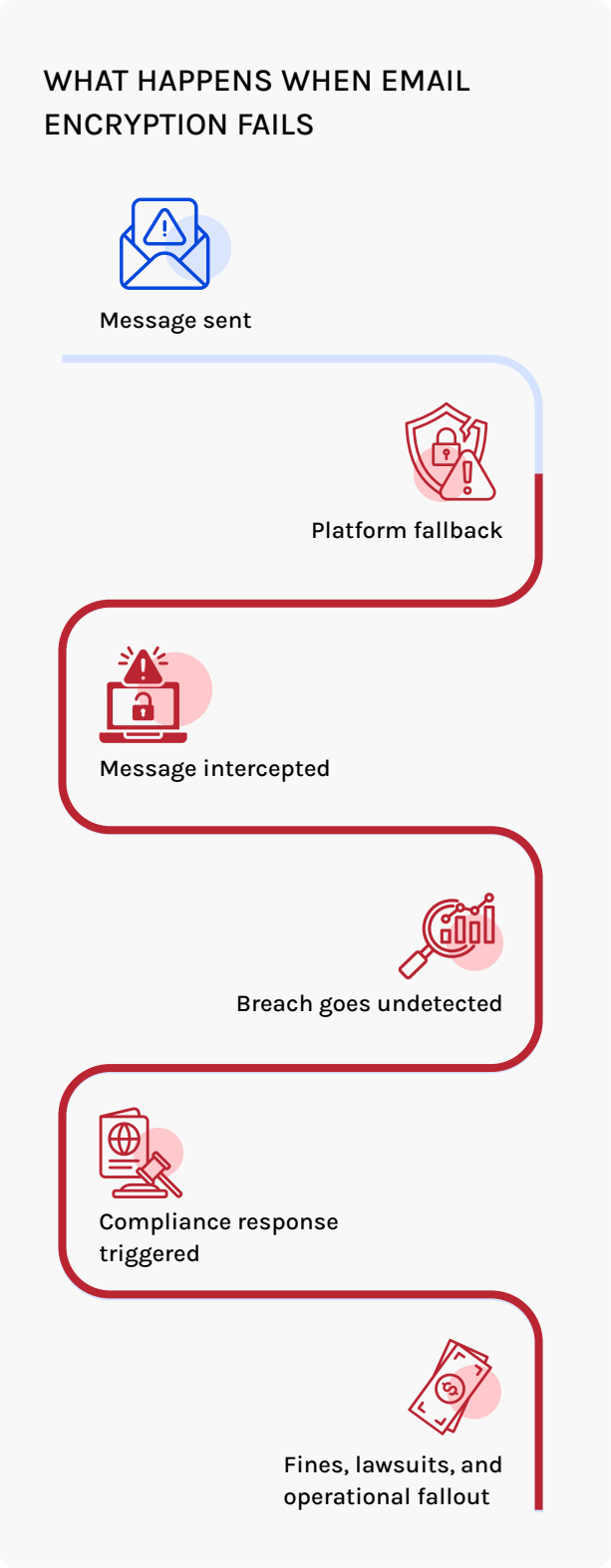
- IT teams diverted from core work to handle audits, response, and recovery
- Communication breakdowns with staff, partners, and patients
- Care delays due to system shutdowns or mistrust of digital communication
- Manual workarounds increase the chance of further human error

> “These attacks endanger patients by exposing vulnerabilities in our health care system, degrading trust, disrupting patient care, and delaying medical procedures.”[7]
>
> **Andrea Palm, Deputy Secretary**
> HHS

Loss of trust–internally and externally

- Patients lose confidence in care providers who can’t protect their data
- Funders and partners question risk posture and compliance maturity
- Employees fall back on unsafe habits when tools fail to protect them

Trust is hard to earn and easy to lose. Especially when the breach could have been prevented.



What IT leaders should do now

If your email encryption relies on assumptions, it's time to re-evaluate.

Force TLS sounds like a safeguard, but as this report shows, it silently introduces risk—especially in complex healthcare environments where compliance, interoperability, and care continuity all hinge on secure communication.

The good news? You can fix this. But it requires moving beyond checkbox compliance and adopting a more rigorous, policy-driven approach to email security.

Five steps to take now

1. Audit your real-world encryption behavior
Make sure encryption isn't just turned on, it's actually working. If you can't confirm the protocol version used, you're flying blind.

2. Eliminate TLS 1.0 and 1.1 as acceptable encryption options
Modern systems allow you to disable legacy protocol support. Do it. There is no valid reason to transmit PHI using encryption deprecated by every standards body.

3. Configure fallback rules that prioritize security over deliverability
If a recipient's server doesn't meet your encryption standards, the email should bounce. Silent delivery in cleartext, like we saw with M365, is not an acceptable risk posture.

4. Replace opportunistic TLS with enforced, policy-based encryption
Look for solutions that guarantee encryption regardless of the recipient's configuration. Blanket protection shouldn't depend on what someone else's server supports.

5. Train your compliance and risk teams to stop treating email as "solved"
Just because it's been working doesn't mean it's secure. Make secure email part of your ongoing audit and risk assessment processes instead of a one-time setup.

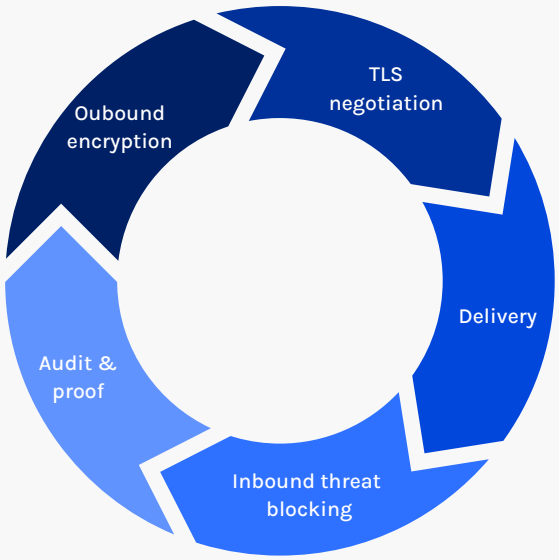
True compliance means preventing breaches

The goal is provable protection. You should be able to demonstrate, for every message containing PHI, that encryption was applied using secure, standards-compliant methods.

Force TLS can't do that. Paubox can.

Unlike traditional secure email portals or S/MIME plugins, Paubox delivers blanket encryption without adding friction to the user experience. There are no passwords to share, portals to log into, or keys to exchange. Every message is encrypted by default and delivered directly to the recipient's inbox—just like any other email. That means no workflow disruption, no training overhead, and no excuses for insecure delivery.

LIFECYCLE OF EMAIL SECURITY



KEY TAKEAWAY

Securing email is not just about encryption at send—it's also about preventing impersonation and phishing at receive. Layering outbound and inbound protection is the only way to ensure full lifecycle security.

Encryption only counts if you can verify it

Healthcare IT leaders are under more pressure than ever to secure patient data, avoid regulatory penalties, and maintain operational uptime. But if your email platform silently downgrades encryption—or skips it entirely—then even the best policies won't protect you.

You need encryption that holds up under real-world conditions–every message, every time..

It's time to stop trusting cloud platforms to get it right by default, and start demanding encryption that's built for healthcare.

> "Confidence without clarity is what gets organizations breached. We don't just need encryption—we need evidence."
>
> **Rick Kuwahara**
> Chief Compliance Officer, Paubox

PAUBOX EMAIL SUITE

Talk to us about secure email that doesn't depend on wishful thinking

- Setup in 15 minutes
- HITRUST certified since 2019
- No portals, no passwords
- Top rated U.S. support

Let's chat!

PAUBOX

Sources

1. Paubox (2025). 2025 Healthcare Email Security Report. https://www.paubox.com/2025-healthcare-email-security-report
2. ACM (2023). A Survey and Analysis of TLS Interception Mechanisms and Motivations. https://dl.acm.org/doi/abs/10.1145/3580522
3. JCIT (2024). The Role of SSL/TLS in Securing API Communications: Strategies for Effective Implementation. https://universe-publisher.com/index.php/jcit/article/view/20/20
4. U.S. Department of Health & Human Services. (2023). 45 CFR §164.312 – Technical safeguards for electronic protected health information (ePHI). Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312
5. NSA (2021). Eliminating Obsolete Transport Layer Security (TLS) Protocol Versions. Cybersecurity Information Sheet, UOO197443-20. National Security Agency. https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF
6. RFC 8996 (2021). Deprecating TLS 1.0 and TLS 1.1. https://www.rfc-editor.org/rfc/rfc8996
7. U.S. Department of Health & Human Services. (2023). HIPAA Security Rule – Proposed Modifications to the Standards for the Security of Electronic Protected Health Information (ePHI). https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html
8. Managed Healthcare Executive. (2023). Email remains a leading security risk in healthcare. https://www.managedhealthcareexecutive.com/view/email-remains-a-leading-security-risk-in-healthcare