Compliance

Healthcare's email security certificate crisis

How expired and self-signed certificates break email encryption across the healthcare ecosystem

PAUBOX

Table of contents

Executive summary

Email is one of the primary ways healthcare organizations exchange information. It moves lab results, care instructions, billing data, referrals, imaging, and scheduling across an ecosystem of providers, payers, and vendors. Most IT leaders assume encryption is holding the line. They trust that Transport Layer Security (TLS) takes care of the transport-layer details.

TLS the technology that protects an email while it is traveling from one server to another, preventing outsiders from reading or altering it. However, the transport layer protecting it is far more fragile than most IT realize.

In practice, TLS often works as designed, but the certificate chain it depends on is breaking down. Across healthcare, certificate validation fails far more often than most organizations realize.

In a sample of outbound email traffic from Paubox, 803,378 unique relays were analyzed.[1] Roughly 4% of those connections went to servers with unverifiable certificates, including expired or self-signed.[1]

BY THE NUMBERS

803,378
relays

↓

30,744
certificate failures

↓

4%
unverifiable connections

↓

Up to 19 million

of PHI-bearing email addresses at risk

How TLS and certificates actually work

TLS is the protocol that encrypts data in transit. TLS doesn't work on its own. It depends on certificates to prove the identity of the server on the other end and to create a trusted, encrypted channel.

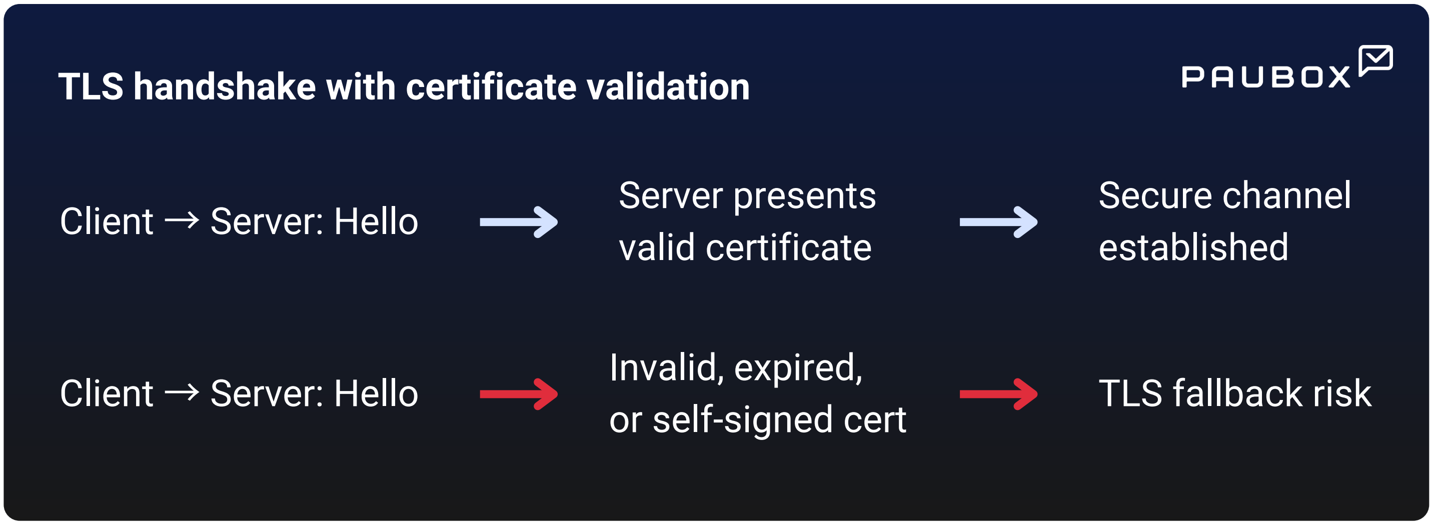
A digital certificate is a file used to prove the identity of a server on the internet. A valid certificate tells your system three things:

- you're connecting to the right server
- the server's identity has been verified by a trusted authority
- the encryption keys being exchanged can't be tampered with

If the certificate is expired or self-signed, trust collapses. Think of certificate validation like checking a passport. If it's expired or issued by the traveler themselves, the identity can't be trusted. TLS may still try to negotiate a connection, but the encryption can't be verified. That's the part most IT teams never see.

With a bad certificate, encryption can downgrade, fail, and get bypassed entirely. Cloud email platforms prioritize message delivery over security, creating a hidden structural weakness in healthcare email. Once certificate trust breaks, every assumption about secure transport collapses and most organizations never realize it happened.

> Up to **3 million healthcare email addresses** are aimed at servers with expired certificates.



TLS handshake with certificate validation

Client → Server: Hello → Server presents valid certificate → Secure channel established

Client → Server: Hello → Invalid, expired, or self-signed cert → TLS fallback risk

The certificate problem you can't see but attackers love

Healthcare depends on an aging supply chain of IT vendors, billing companies, EHR add-ons, imaging services, and managed service providers (MSPs). These vendors exchange email on behalf of healthcare organizations every day, often without direct oversight from the provider itself.

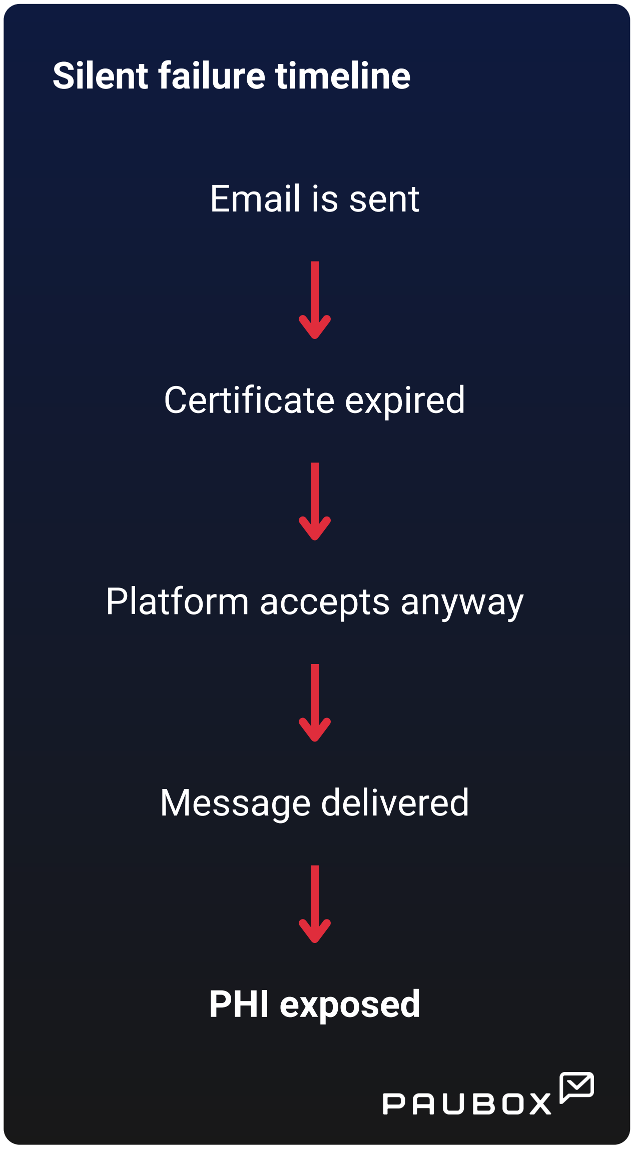
Many of these environments still run outdated or misconfigured mail servers.[3] When those servers present invalid certificates, cloud email platforms face a choice between security and deliverability. Deliverability often wins.

That means PHI can travel across an untrusted or unverifiable path without the sender knowing. It also means attackers can exploit these gaps by setting up infrastructure that intentionally mimics certificate failure conditions, making it easier to intercept or manipulate email traffic.

> **Millions** of healthcare emails each year are routed to servers whose identity cannot be fully verified.

For a sector that already faces rising phishing, credential compromise, and vendor-driven breaches, this is exactly the kind of weakness attackers look for.

A separate analysis presented at the USENIX Security Symposium showed that many SMTP servers fall back to plaintext or accept invalid certificates when TLS negotiation fails, exposing messages to active interception and downgrade attacks.[4] These real-world weaknesses align with the silent failure modes we observe in healthcare email: TLS appears to be working, but certificate validation quietly collapses in the background.[4]



Silent failure timeline

Email is sent

Certificate expired

Platform accepts anyway

Message delivered

PHI exposed

What we see across the healthcare ecosystem

Paubox processes email traffic across thousands of healthcare organizations, giving us a unique view into the real-world certificate hygiene of the industry.

Across the ecosystem we see servers:

- presenting expired certificates
- using self-signed certificates
- presenting incomplete or broken certificate chains

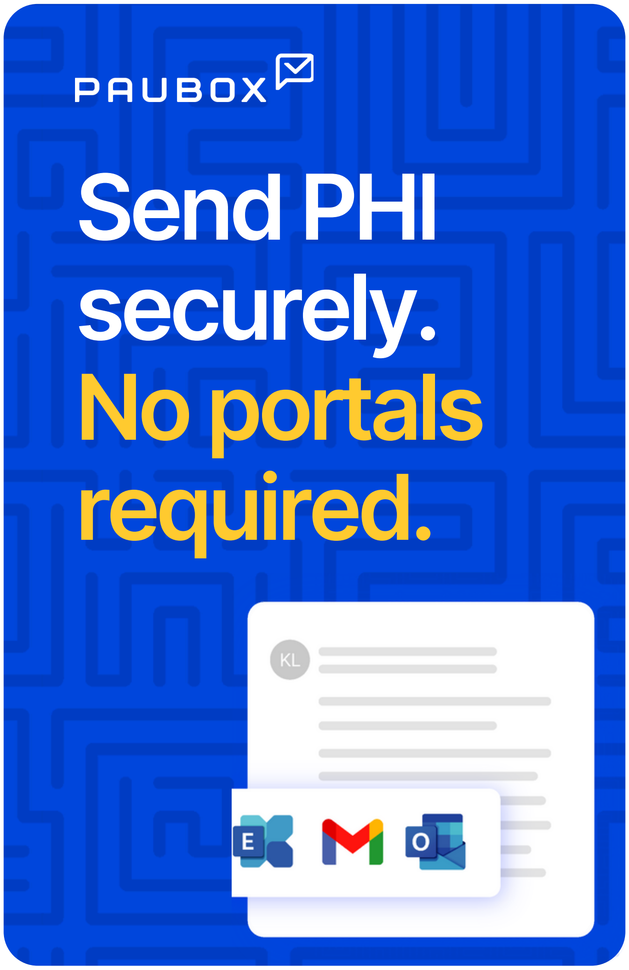
In a one-week sample of outbound traffic from Paubox customers, we observed 803,378 unique outbound relays. Of those, 0.48% presented expired certificates and 3.35% used self-signed certificates.

A self-signed certificate is created by the server itself, not verified by a trusted third party. That means there is no independent way to confirm the server's identity.

> **4% of outbound healthcare email connections** observed went to servers with unverifiable certificates.

In total, roughly 4% of outbound connections went to servers whose identity could not be fully verified because of certificate problems.

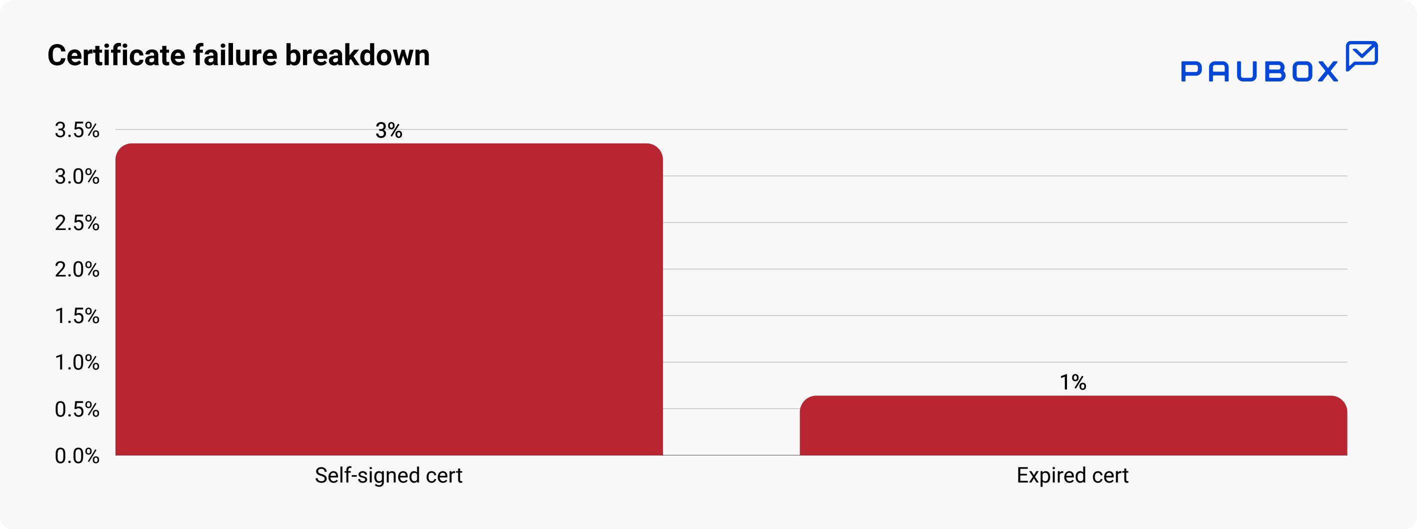
At Paubox scale, that translates into millions of PHI-bearing messages each year being directed at endpoints that cannot be trusted with high confidence.[1]



These issues show up across healthcare in hospitals, clinics, billing firms, revenue cycle vendors, imaging companies, and niche service providers. They show up in rural networks and enterprise environments.

Healthcare organizations rarely know when they rely on a downstream vendor with broken certificate infrastructure. Self-signed certificates are especially risky because they remove the third-party validation that HIPAA expects for authenticated transport security.

HIPAA doesn't spell out "no self-signed certs," but the Security Rule requires organizations to verify the integrity of the connection. A self-signed certificate cannot provide that verification, which means the encryption cannot be trusted or proven. In practice, this turns PHI transmission into an unverifiable risk.


Certificate failure breakdown

EMAIL SECURITY
Inbound Email Security
Protect yourself with AI-powered email security
Start for free
RYAN WINCHESTER, Paubox customer
CareM

Why cloud email platforms make this problem worse

Microsoft 365 and Google Workspace don't treat certificate failures in email the same way they treat them in browsers. Browsers are strict. Email transport is permissive.

When a certificate fails in a browser, the connection is blocked unless the user deliberately bypasses the warning. Most people recognize this as the security warning page that appears when a website cannot be trusted.

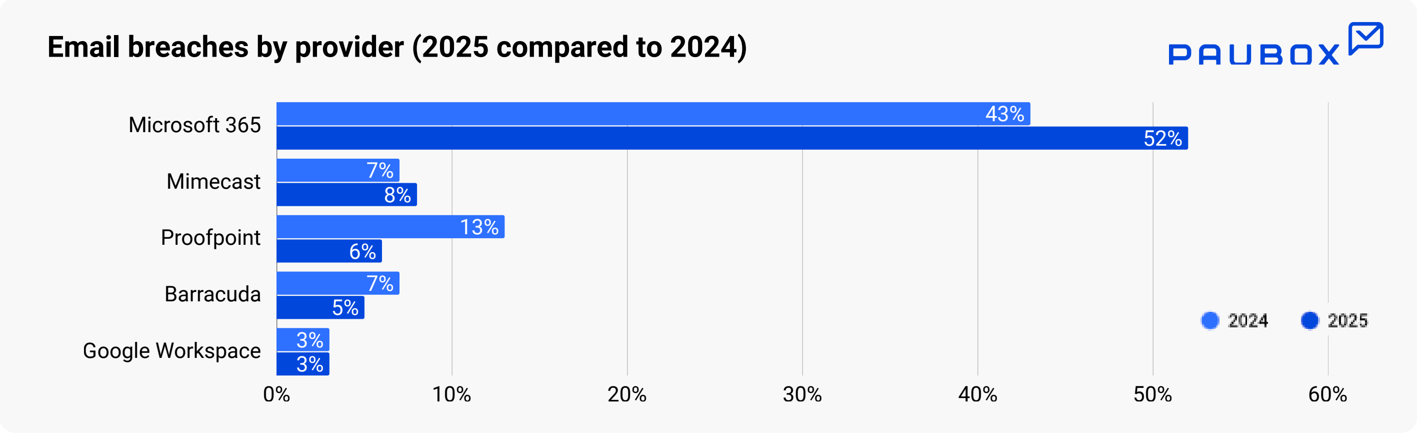
With email transport, platforms often make exceptions. They negotiate the strongest connection they can, and if they can't verify the certificate, they may deliver the message anyway.

Cloud email platforms routinely accept weak or unverifiable certificates because the alternative is message failure.

Deliverability wins over security, and that behavior silently propagates risk across every domain that depends on them.

Because a handful of providers like Google and Microsoft now handle a large share of global business email, their certificate-handling decisions impact millions of domains and amplify ecosystem-wide risk.[6]

The sender sees nothing unusual. Logs show nothing alarming. The recipient gets the message. But the encryption layer is weaker than expected, or in some cases, not guaranteed at all. This is exactly how encryption fails in healthcare.



The vendor problem hiding underneath

The certificate crisis gets worse when you factor in healthcare's vendor ecosystem. Every clinic, health system, and payer relies on dozens or hundreds of business associates. A business associate is any vendor or partner that handles protected health information on behalf of a healthcare organization.

Many of those business associates still use old, self-managed mail servers or legacy network appliances. Certificates expire. Renewal automation breaks. Chains go missing, and nobody notices.

Our outbound data shows that in a single week, roughly 5% of healthcare email connections went to servers with unverifiable certificates. The problem is baked into day-to-day communications between providers and their vendors.

Providers trust that their messages are being protected. Vendors trust that their certificate is "close enough." However, cloud platforms prioritize delivery over validation.

No one owns the full chain of responsibility. That's how a single broken certificate on a billing vendor's server can expose thousands of patient records.

Given that 16% of email-related breaches this year have involved business associates, certificate hygiene is more than a niche issue.[7]

How Paubox closes the gap

Paubox encrypts outbound email automatically and delivers it directly to the inbox without relying on certificate validation from the recipient's server. This eliminates the weakest point in the traditional model. There is no dependency on someone else's infrastructure behaving correctly.

Paubox Email Suite strengthens this even further by actively checking the certificates on the receiving server before sending PHI. It is a core part of the outbound security functionality included in all Paubox Email Suite tiers providing outbound email encryption. It looks for:

- expired certificates
- self-signed certificates
- incomplete or missing certificate chains
- revoked or malformed certificates

When Paubox detects any of these failures, it does not send the message over that connection. Instead, it automatically delivers the message as a Paubox secure message. No other email vendor currently offers this level of certificate validation and enforcement.

Healthcare organizations get encryption they can prove, not just encryption they hope is working.

Most healthcare providers assume their email is secure because TLS is enabled, but TLS only works when certificates hold the line. Across healthcare, that line is old and broken. Expired and self-signed certificates are everywhere, and fallback behavior from major platforms hides the problem.

The certificate crisis is real, and it's undermining the most widely used communication channel in healthcare. It's time to stop trusting what you can't verify and start using encryption that doesn't depend on someone else's infrastructure.

Paubox rated #1 on G2 for Email Encryption Software

BEST SOFTWARE
2025
Top 50
HEALTHCARE PRODUCTS

Sources

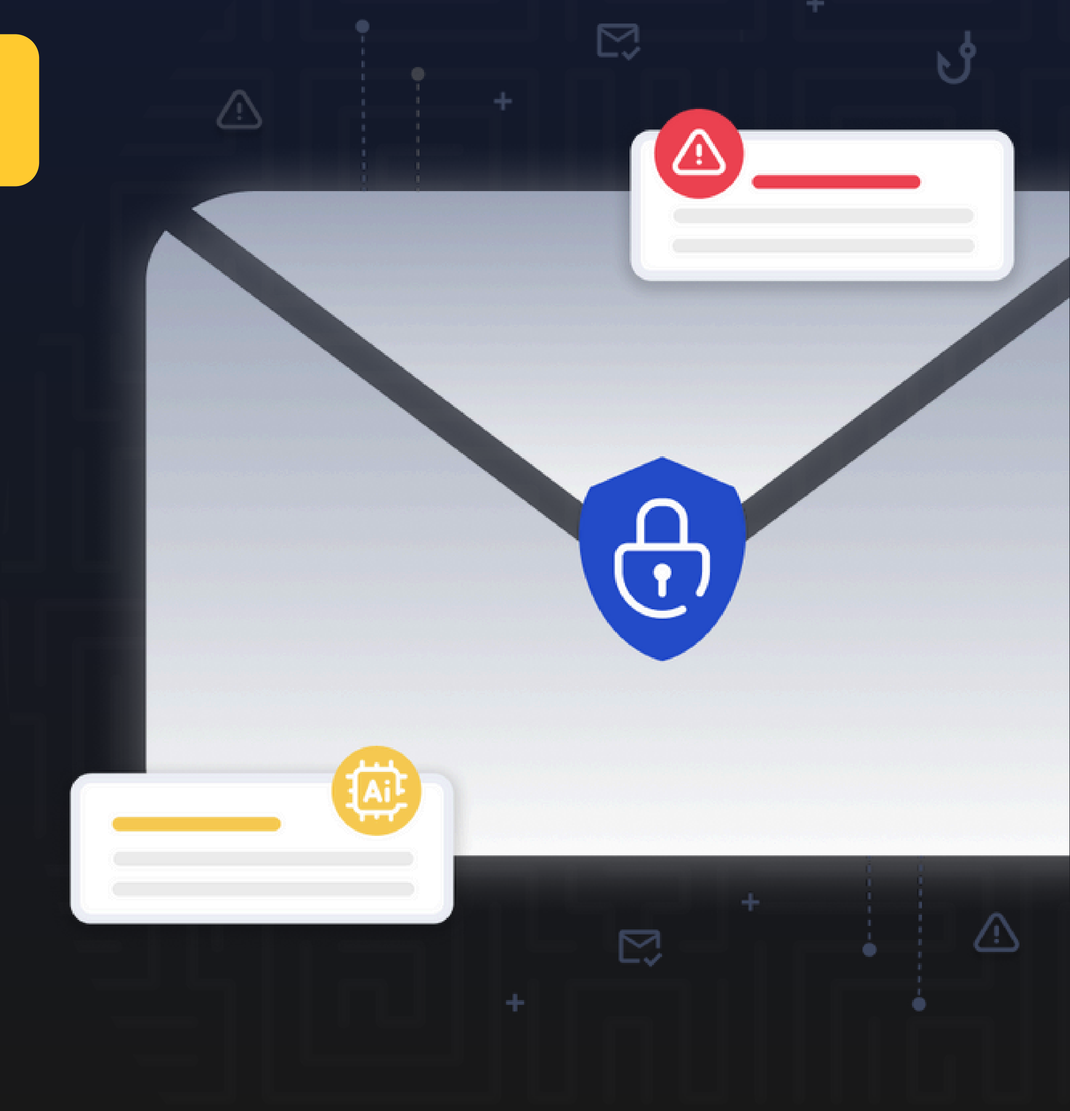
1. National Security Agency. “Eliminating Obsolete TLS Protocol Versions.” 2021.
2. U.S. Department of Health and Human Services. “45 CFR §164.312 – Technical Safeguards for Electronic Protected Health Information.”
3. Paubox. “2025 Healthcare Email Security Report.” 2025.
4. Paubox. “2025 Mid-Year Email Breach Recap.” 2025.
5. Paubox. “Outbound Cluster Certificate Analysis, Nov. 9–15, 2025.” Internal dataset.
6. ACM Internet Measurement Conference. “Who’s Got Your Mail? Characterizing Mail Service Provider Usage.” 2021.
7. Holz, T., et al. USENIX Security Symposium. “Why TLS Is Better Without STARTTLS: A Security Analysis of SMTP Opportunistic Encryption.” 2021.

PAUBOX

Stop email phishing attacks with AI security

Surface hidden threats with generative AI email security that learns and evolves.

Talk to an expert



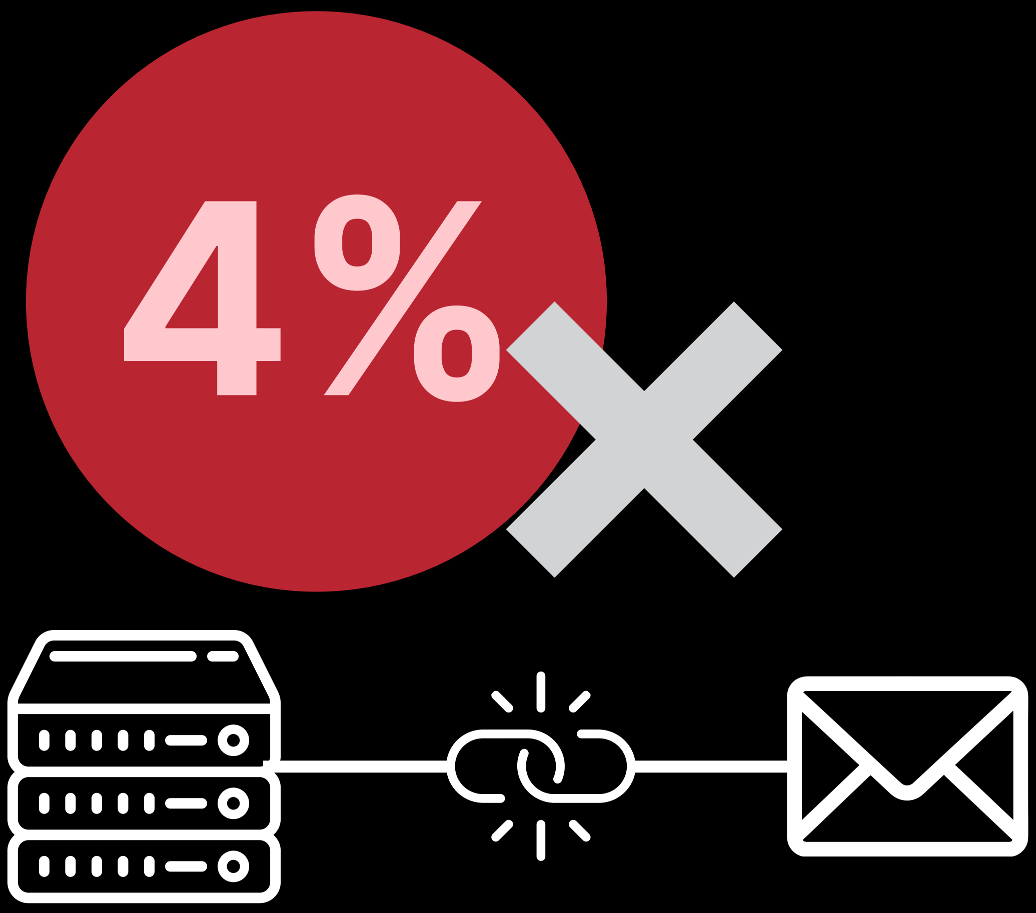
Healthcare’s hidden email threat

Standard email encryption is critically important flawed due to widespread, unseen certificate failures.

The foundation is broken

Encryption depends on trust

Transport Layer Security (TLS) relies on valid server certificates to verify identity and create a secure channel.



Widespread failure

4% of connections are unverifiable

In a Paubox sample, 4% of healthcare email connections went to servers with bad certificates (expire or self-signed).

Silent risk

Cloud platforms hide the problem

Major email platforms prioritize message delivery over security, often sending emails even when a recipient’s certificate fails validation.

Widespread failure

Millions of PHI records exposed

This silent failure means millions of emails with PHI can be sent over untrusted connections each year

PAUBOX