Compliance

What healthcare gets wrong about HIPAA and email security

From misconfigurations to flawed assumptions: A look at the hidden risks in everyday communication systems.

PAUBOX

PAUBOX

Table of contents

Executive summary

Email remains the #1 source of HIPAA breaches in healthcare. In the first half of 2025, 107 email-related incidents were reported to HHS — on track to surpass the 180 breaches in 2024.[1]

For many healthcare organizations, HIPAA compliance starts and ends with enabling encryption. If a business associate agreement is signed, it feels compliant. HIPAA's Security Rule requires more: encryption in transit and at rest, access controls, and proof that those safeguards worked.

Common platforms like Microsoft 365 and Google Workspace prioritize message delivery over security. Others, like portals, create so much friction that providers and patients bypass them. And systems that rely on staff to manually trigger encryption expose organizations to frequent preventable errors.

Outbound email encryption is the foundation of HIPAA compliance. Without automation and verification, even well-meaning organizations risk failing the Security Rule.

This report explains what HIPAA requires for email, clarifies where common practices fall short, and outlines what IT and compliance teams can do to ensure encryption is automatic, verifiable, and consistently applied.

BY THE NUMBERS

107

email-related breaches occurred in the first half of 2025 out of the 302 breaches reported to HHS

52%

of breaches reported this year so far occurred on Microsoft 365, up from 43% in 2024

82%

of healthcare IT leaders worry that their staff will miss a critical alert or skip a security step

65%

of portal users stop engaging after day one

What HIPAA requires for email compliance

HIPAA's Security Rule outlines the technical safeguards that every covered entity and business associate must implement to protect electronic protected health information (ePHI). For email, that responsibility focuses on one critical point of failure: the moment data leaves your system.

The Security Rule requires "appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information".[2]

- **Encryption in transit and at rest:** Email must be encrypted using secure, modern protocols such as TLS 1.2 or higher, ensuring that PHI remains unreadable as it moves between servers.

- **Access controls:** Only authorized users should be able to send or receive messages containing ePHI. This includes authentication, role-based permissions, and multi-factor verification where appropriate.

- **Integrity verification:** The organization must have a way to confirm that a message was not altered or intercepted during transmission.

- **Audit and verification:** HIPAA expects not only that encryption is active but that it can be proven. Logs and audit trails should demonstrate that safeguards were applied for every outbound message containing PHI.

- **A signed Business Associate Agreement (BAA)** with any vendor that handles ePHI is also mandatory. Without it, the service cannot be considered HIPAA compliant, regardless of technical setup.

> "Too many vendors still treat HIPAA as optional. If you're handling PHI without encryption or a BAA in place, you're creating liability."
>
> **Hoala Greevy**
> CEO, Paubox

Where compliance breaks down

Most healthcare organizations have policies and tools that appear to check every HIPAA box. Encryption is enabled, staff are trained, and BAAs are signed. Yet, email remains one of the most common sources of HIPAA violations. The issue is a disconnect between configuration and verification.

Delivery-first platforms

Cloud email systems like Microsoft 365 and Google Workspace are designed to prioritize message delivery. When encryption fails or an outdated TLS protocol is encountered, those platforms often send the message anyway rather than risk a bounce.[3]

That silent fallback results in unsecured PHI being transmitted, with no alert to the sender and no audit trail showing that encryption failed. From a compliance standpoint, that's a breakdown the organization can't detect until it's too late.

Paubox's 2025 Mid-Year Report found that 52% of email-related breaches involved Microsoft 365.1 Most occurred despite 'encryption settings' being enabled because fallback delivery occurred when the recipient didn't support TLS 1.2 or higher.[3]

52%

of healthcare email breaches involved Microsoft 365

65%

of portal users stop engaging after day one

82%

of healthcare IT leaders worry their staff will miss a critical alert or skip a security step

Portal fatigue

To compensate for encryption uncertainty, some organizations turn to secure portals. Portals meet the security requirement but fail the usability test. They force patients and partners through multiple steps — creating logins, entering codes, or downloading attachments — just to read a message.

Engagement drops, communication delays increase, and staff often bypass the portal to get information where it needs to go faster. Studies from the National Library of Medicine shows that portals reduce patient communication: 65% of portal users stop engaging after day one, and 22% cite difficulty navigating basic portal functions.[12]

Those studies further show that the roadblocks portal cause, have the "potential to generate more work, confuse patients, alienate non-users, and increase health disparities".[12]

Human-dependent encryption

The third common failure point is manual encryption. Many systems rely on users to type a keyword into the subject line or click an "encrypt" button. It works, until someone forgets. Every single unencrypted message containing PHI can trigger a reportable HIPAA breach.

In one enforcement action, a clinic was fined $25,000 simply for sending PHI to the wrong recipient via unencrypted email.8 The more human action required, the higher the chance of inconsistency, and the greater the compliance exposure.

Email encryption cannot depend on default settings, portals, or user behavior. HIPAA compliance requires encryption that's enforced by design, proven through logs, and applied to every message automatically.

What's changed in 2025, and what's next

For the first time in more than a decade, the U.S. Department of Health and Human Services (HHS) is moving to strengthen the HIPAA Security Rule. In early 2025, the Office for Civil Rights (OCR) proposed updates that would make encryption of all ePHI, at rest and in transit, a required safeguard, not an addressable one.[9]

The proposed rule also calls for mandatory annual compliance audits, configuration hardening, and verified security controls for business associates. It's a shift from policy-driven compliance to proof-driven accountability.

This change closes one of the biggest loopholes in healthcare security. Under the original 2013 Security Rule, "addressable" safeguards allowed organizations flexibility in how they implemented certain controls.

> In 2025, OCR issued fines ranging from **$80,000 to over $9 million for orgs** whose email systems lacked enforced encryption or adequate risk analysis.

Many interpreted that flexibility as optional, relying on policies or limited TLS configurations to meet the standard. The proposed rule makes clear that encryption is now a baseline expectation. In 2025 alone, OCR issued fines ranging from $80,000 to over $9 million for organizations whose email systems lacked enforced encryption or adequate risk analysis.[5]

OCR's proposed updates also emphasize the need for technical controls that can verify encryption and prevent unauthorized access to ePHI in transit. They have explicitly called out email as a persistent risk vector, noting that most breaches still involve unencrypted or misconfigured communication systems.

What this means for healthcare IT and compliance teams

The practical impact of these changes is straightforward: organizations must be able to prove that every outbound message containing PHI was encrypted using secure, modern protocols (TLS 1.2 or higher) and that those protections are upheld through delivery.

While still essential, policies, staff training, and signed BAAs are still essential, but they are no longer enough. Proof of encryption will become a compliance requirement, not a best practice. OCR Director Melanie Fontes Rainer stated, "HIPAA-regulated entities need to be proactive... not wait for OCR to reveal long-standing HIPAA deficiencies."[10]

Systems that rely on users to encrypt manually, that send without encryption when TLS negotiation fails, or that cannot generate audit logs will not meet this new standard.

What's next

Even before the proposed rule is finalized, the message from regulators is clear: encryption-by-default should be the norm across all healthcare email. IT and compliance leaders should begin auditing outbound encryption behavior now, confirm that legacy TLS versions are disabled, and ensure their email provider can produce verifiable proof of encryption for every message.

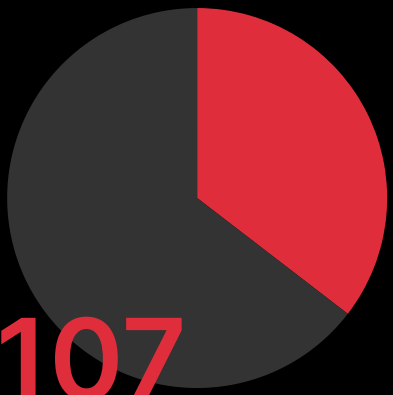
Organizations that adopt automatic, provable encryption ahead of these updates will reduce the risk of reputational and financial damage from a HIPAA breach.

Sources

1. Paubox. (2025, August). Mid-year healthcare breach recap 2025. https://www.paubox.com/resources
2. U.S. Department of Health & Human Services. (n.d.). The HIPAA Security Rule. Health Information Privacy. https://www.hhs.gov/hipaa/for-professionals/security/index.html
3. Paubox. (2025, March). State of email security in healthcare 2025. https://www.paubox.com/resources
4. Paubox. (2025, March). How Microsoft and Google put PHI at risk. https://www.paubox.com/resources
5. Paubox. (2025, March 14). HIPAA compliant email: The definitive guide. Paubox Blog. https://www.paubox.com/blog/hipaa-compliant-email
6. Paubox. (2025, March). The hidden cost of inaction: How inaction fuels rising breach costs in healthcare (in partnership with Osterman Research). https://www.paubox.com/resources
7. IBM. (2025). Cost of a data breach report 2025. IBM Security. https://www.ibm.com/reports/data-breach
8. Office for Civil Rights (OCR). (2025, January). OCR settles potential HIPAA violations with Massachusetts medical records provider. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
9. Office for Civil Rights (OCR). (2024, December 27). HIPAA Security Rule to strengthen the cybersecurity of electronic protected health information. U.S. Department of Health and Human Services. https://www.federalregister.gov/documents/2024/12/27/2024-27961/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
10. Paubox. (2025). Healthcare IT is dangerously overconfident about email security. https://www.paubox.com/resources
11. U.S. Department of Health and Human Services. (2024–2025). Press releases and public statements by OCR Director Melanie Fontes Rainer. https://www.hhs.gov/about/news
12. Paubox. (2023). Why patient portals are inconvenient: An evidence-based perspective. Paubox Blog. https://www.paubox.com/blog/why-patient-portals-are-inconvenient-an-evidence-based-perspective

PAUBOX

Inside the HIPAA compliance gap



107

email-related breaches occurred in the first half of 2025 out of the 302 breaches reported to HHS

52%

of breaches reported this year so far occurred on Microsoft 365, up from 43% in 2024

82%

of healthcare IT leaders worry that their staff will miss a critical alert or skip a security step

> "Too many vendors still treat HIPAA as optional. If you're handling PHI without encryption or a BAA in place, you're creating liability."
>
> **Hoala Greevy**
> CEO, Paubox

65%

of portal users stop engaging after day one

PAUBOX

Stop email phishing attacks with AI security

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

Talk to an expert