PAUBOX

2025 REPORT

2025 mid-year email breach data reveals there’s no slowing down

Insights from 107 email-related healthcare breaches

Table of contents

Executive summary

The first half of 2025 made one thing clear: healthcare's email security problem isn't going away. From January through July, HHS recorded 107 healthcare breaches involving email—on track with last year's pace, but with a notable shift in severity.[1] The average breach exposed nearly 16,000 records, and the largest topped half a million.

Organizations face a tough combination: limited staff and budget, a growing attack surface, and increasing pressure to stay compliant. Too often, email security is dependent on outdated tools and human vigilance. This report examines where the risks are showing up most and where blind spots persist.

BY THE NUMBERS

107
email-related breaches so far in 2025, compared to 180 overall last year

52%
of healthcare breaches were on Microsoft 365, up from 43% in 2024

41%
of orgs were assessed as high risk, up from 31% last year

79%
of breached domains had ineffective DMARC protection, a major jump from 65% in 2024.

PAUBOX

The first half of 2025 by the numbers

107

email-related breaches so far in 2025, compared to 180 overall last year

1,653,512

individuals affected across all incidents

52%

of healthcare breaches were on Microsoft 365, up from 43% in 2024

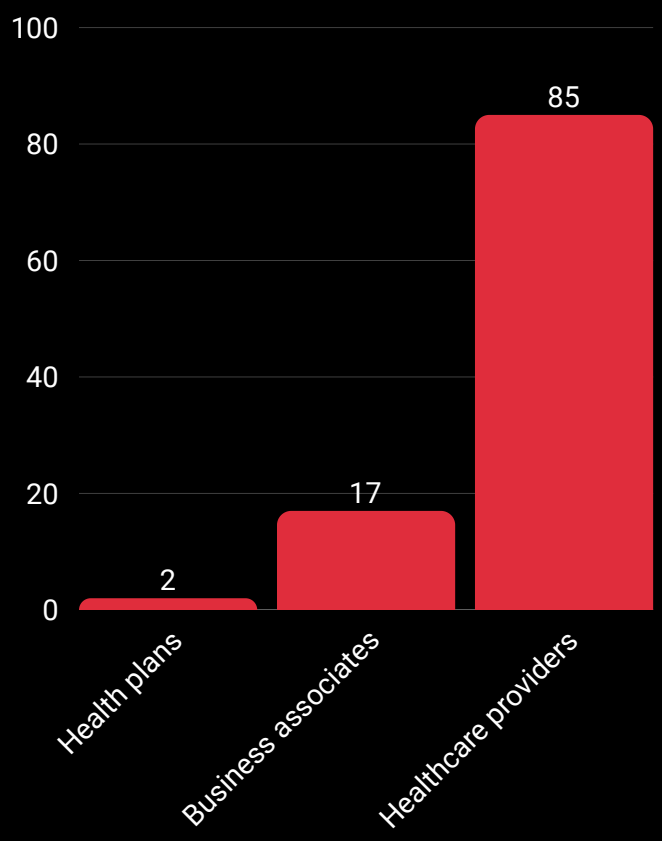
41%

of orgs were assessed as high risk, up from 31% last year

79%

of breached domains had ineffective DMARC protection, a major jump from 65% in 2024.

Breaches by type of organization



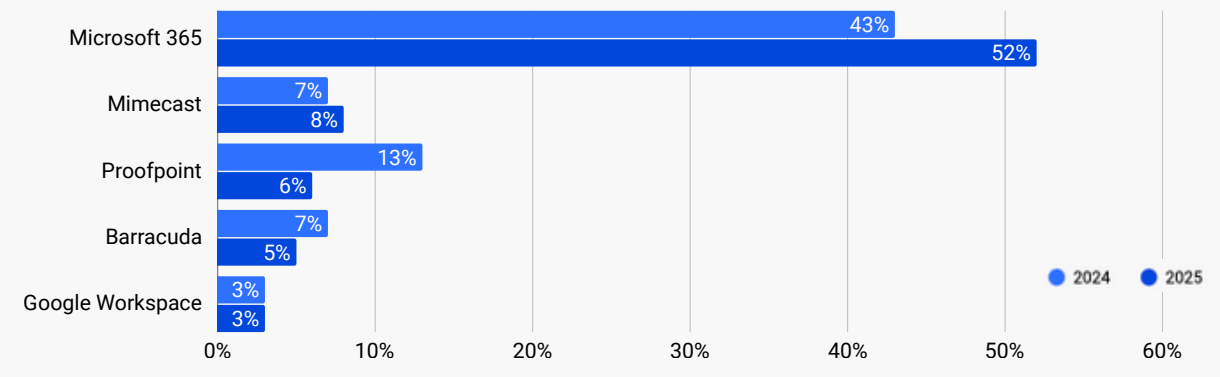
Understanding the breach landscape

Email remains the dominant communication method in healthcare—and still the most common source of breaches. In the first half of 2025 alone, 107 healthcare organizations reported email-related incidents to HHS, putting the year on track to match or exceed the 180 breaches reported in 2024. While the volume may be consistent, the security posture appears to be slipping. More organizations are falling into high-risk categories (41% compared to 31% in 2024), and fewer are meeting even the most basic security configuration standards.

Microsoft 365 continues to top the list of breached email environments, accounting for 52% of incidents so far in 2025—up sharply from 43% last year. Other premium providers such as Mimecast (8%), Proofpoint (6%), and Barracuda (5%) also appear, indicating that brand-name solutions alone aren't preventing breaches. Even Google Workspace showed up in a small number of incidents (3%). The inclusion of email security platforms in this year's breaches suggests that setup, maintenance, and enforcement are more important than the brand name you buy.

According to the 2025 IBM Cost of a Data Breach report, the average cost of a healthcare breach is now $11 million—the highest of any industry for the 14th consecutive year.[2] Across the board, these breaches often come down to misconfiguration, lack of continuous enforcement, and overreliance on staff to spot threats in real time.

Email breaches by provider (2025 compared to 2024)



Where breakdowns happen

Of the 104 email breaches reported to HHS so far in 2025, 81% were categorized as hacking or IT incidents. Credential compromise and phishing continue to dominate, but the routes attackers take reveal operational cracks: unmonitored inbox rules, ineffective display name protection, or mismanaged configurations. It all adds up to IT teams feeling overwhelmed. Tools like Paubox Email Suite Plus automatically block suspicious emails and display name spoofing reduce the burden on staff without IT intervention.

> According to IBM, the average cost of a breach is now $11 million, up from $9.8 million in 2024

Strained IT teams often lack the time to continually test configurations, monitor delivery logs, or train every staff member on subtle indicators of risk. Without automation that enforces security by default, they're left hoping staff make the right choice under pressure. This aligns with broader concerns across the industry—82% of IT and cybersecurity leaders say they worry about missing threats due to the overwhelming volume of alerts and data they face, and 86% simultaneously worry about HIPAA compliance, often due to gaps in resourcing and skills.[4]

IT teams aren't the only ones feeling the pressure. When staff aren't confident in what to trust—or when security features get in the way of getting work done—they find workarounds. Those workarounds introduce risk. In a recent Paubox survey, 41% of healthcare providers said their teams have bypassed secure messaging at least once in the past year, prioritizing productivity over security.[5] What staff fail to realize is that those security protocols keep larger disruptions at bay. 50% of organizations cite cyberattacks as the leading cause of critical workflow disruptions.[3] These decisions often stem from frustration with portals, quarantines, or confusing alerts.

KEY TAKEAWAY

Misconfigurations, alert fatigue, and staff workarounds continue to fuel avoidable security incidents. 82% of IT leaders say they worry about missing threats.

How email breaches happen

To better understand the nature of email breaches in healthcare, it is crucial to examine the attack vectors used by cybercriminals. Below are the most common attack methods:

- **Phishing attacks:** Cybercriminals send deceptive emails impersonating legitimate sources to trick employees into revealing credentials or downloading malware. According to a Paubox survey, IT leaders estimate only 5% of known phishing attacks are reported by employees to their security teams.

- **Spoofing & impersonation:** Attackers impersonate or spoof executive email accounts to authorize fraudulent transactions or request sensitive data. Threat actors forge email headers to make messages appear as though they originate from trusted sources, bypassing weak security configurations.

- **Credential theft:** Hackers use leaked or stolen login credentials to gain unauthorized access to email systems, often due to weak or reused passwords.

- **Malware & ransomware:** Attackers distribute malicious software through email attachments or links, encrypting files and demanding ransom for decryption keys.

- **Insider fraud:** More than half of insider fraud incidents within the healthcare sector involve the theft of customer data, according to Carnegie Mellon University Software Engineering Institute (CMU SEI). Employees with access to patient information remain a significant risk factor in breaches.

Each of these attack vectors exploits poor security configurations and user vulnerabilities, highlighting the need for robust authentication and threat detection mechanisms.

Why SMB and mid-market orgs are so vulnerable

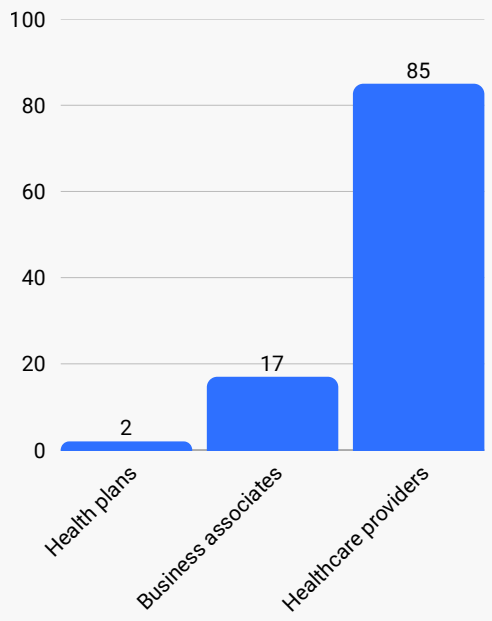
SMB and Mid-market providers, typically having anywhere from 10 to 1,000 employees, rely heavily on third-party support for email security. Business associates—billing vendors, imaging firms, outsourced IT providers—were involved in 17 of the 107 email-related breaches so far this year. That's 16% of all incidents, including several of the largest.

In many cases, providers may not even be aware of all the third-party vendors touching their data. The recent Episource breach, which has now reportedly affected 192.7 Americans (over half the U.S. population) as of the beginning of August, is an example of how deeply embedded business associates can be, and how invisible that risk often is until it's too late.[8]

> 16% of email-related breaches in 2025 have involved business associates

Onsite Mammography and Restorix Health both experienced breaches tied to email mismanagement, exposing hundreds of thousands of patient records. Even the best

Breaches by type of organization



KEY TAKEAWAY

Third-party vendors often introduce invisible risk, and smaller orgs rarely have the oversight or leverage to enforce security best practices.

internal practices can't cover gaps introduced by vendors.

System and process failures rarely surface until a breach exposes them, and by then, the damage is already done. For many healthcare organizations, the assumption that email security is merely a checkbox crossed off by purchasing software is a blind spot that can carry steep financial and operational consequences.

A single attack on a hospital in Georgia in 2024 resulted in a terabyte of stolen data, a total system shutdown, and weeks of paper-based operations.[9] Appointments were canceled, care was delayed, and patient records were leaked online—all traced back to a compromised email account.

Adding even more pressure, enforcement agencies are paying closer attention. In late 2024, OCR fined a Pennsylvania clinic for transmitting PHI over unencrypted email—despite staff believing their email system was compliant. The corrective action plan required a full risk analysis and updates to encryption policies. Across OCR investigations, faulty risk analysis is a repeated finding. Even small providers are now expected to validate how their systems behave, not just how they're configured.

> "Healthcare IT leaders are confident in their systems… until a breach happens."
>
> **Rick Kuwahara**
> Chief Compliance Officer, Paubox

Enterprise-level healthcare creates breach risks at scale

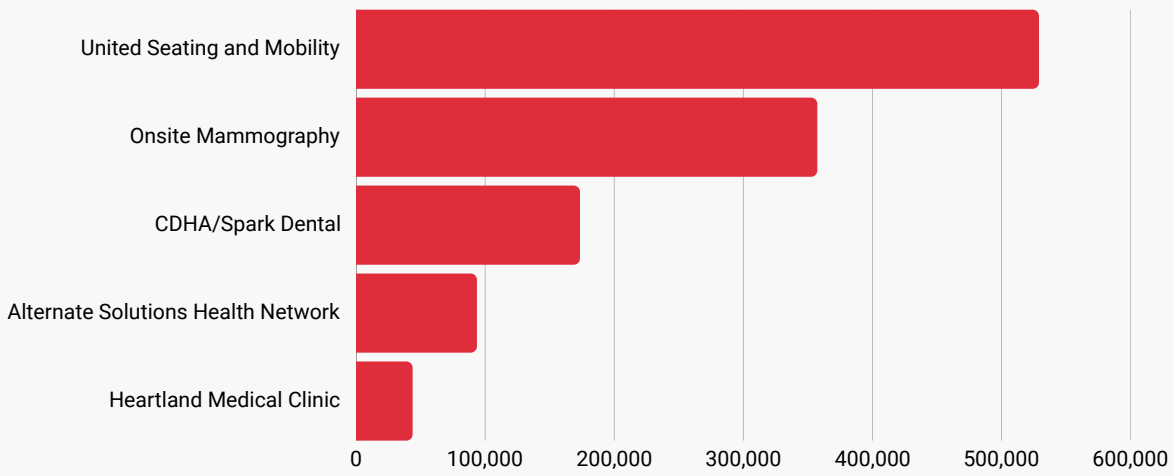
For large health systems, complexity is a liability. Enterprise-level organizations often operate with hundreds of applications, thousands of users, and sprawling third-party ecosystems. Email security incidents in these settings can expose hundreds of thousands—or even millions—of records in a single breach.

With scale comes more fragmentation. It's common for different departments, locations, or acquisitions to run separate systems, use different email protections, or follow varied security policies. This decentralization increases the odds of misconfiguration, incomplete risk analysis, and inconsistent enforcement. According to OCR enforcement data, failure to conduct an adequate enterprise-wide risk analysis has been cited in more than 75% of HIPAA resolution agreements involving security incidents from 2020 to 2024.[7]

Due diligence during mergers and acquisitions is another area of concern. Episource, acquired by Optum (a UnitedHealth Group subsidiary), reported a breach in 2025 that affected 5.4 million individuals. The incident drew congressional scrutiny, as lawmakers questioned whether UHG had upgraded Episource's legacy systems and implemented MFA.

While these organizations typically have more security resources than their smaller counterparts, they also face greater internal friction. Security alerts may go untriaged, compliance controls might be bypassed for convenience, and frontline staff can become desensitized to phishing simulations and warning banners. The key challenge for enterprise IT leaders is not just protection, but coordination: ensuring that every team, tool, and process works

Largest breaches by organization (Top 5)



together to detect, block, and respond to email-based threats. Paubox's integration with Microsoft 365 and Google Workspace offers a standardized, automated layer of protection—regardless of which system a team uses.

Email security remains one of the highest-risk, lowest-visibility areas for healthcare organizations. The 2025 breach numbers show that threat volume hasn't slowed—and user-dependent security strategies are still failing.

The takeaway for IT leaders is to audit assumptions. It's time to revisit what your system is doing when you're not looking. You don't need to choose between security and usability. A thorough risk analysis and proactive security updates cost a lot less than a breach. Silent failure modes, misaligned tools, and user workarounds aren't going away.

PAUBOX EMAIL SUITE

Email security and compliance for healthcare

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

Let’s chat!

PAUBOX

Sources

1. U.S. Department of Health and Human Services. (2025). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
2. IBM Security. (2025). Cost of a Data Breach Report. https://www.ibm.com/reports/data-breach
3. Mattermost. (2025). State of Mission-Critical Work. https://mattermost.com/exclusive-report-the-state-of-mission-critical-work
4. Forrester Consulting. (2025). The State of Threat Intelligence. https://services.google.com/fh/files/misc/forrester_state_of_threat_intel_2025.pdf
5. Paubox. (2025). State of Email Security Report. https://www.paubox.com/resources/email-security-report-2025
6. Paubox. (2025). The Hidden Cost of Inaction. https://www.paubox.com/resources/hidden-cost-of-inaction-report-2025
7. U.S. Department of Health and Human Services. (2024). Enforcement Results: Resolution Agreements and CMPs. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results/index.html
8. McGee, M. (2025, August 7). UnitedHealth Group's Latest Health Data Breach Woes. Healthcare Info Security. https://www.healthcareinfosecurity.com/blogs/unitedhealth-groups-latest-health-data-breach-woes-p-3926
9. State of Maine Office of the Attorney General. (2024). Cartersville Medical Center Breach Notification. https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b5d2ed34-3d1c-449e-915a-1683af30ba6a.html
10. Bitsight. (2025). The State of Cyber Risk and Exposure. https://www.bitsight.com/resources/state-of-cyber-risk-and-exposure-2025
11. Cobalt. (2025). CISO Perspectives Report. https://resource.cobalt.io/ciso-perspectives-report