PAUBOX

2025 REPORT

The Healthcare Email Security Report

Key insights from 180 email-related healthcare breaches

Executive summary

Between January 1, 2024, and January 31, 2025, 180 healthcare organizations reported email-related security breaches to the HHS Office for Civil Rights (OCR). Despite increased spending on email security solutions, these organizations still fell victim to cyberattacks—many due to limited security.

This report uncovers the root causes of these breaches and provides actionable recommendations to improve email security posture in the healthcare industry. Many organizations operate under a false sense of security, assuming that investing in premium solutions is enough. However, without proper implementation and enforcement of security protocols, they remain vulnerable.

OCR Director Melanie Fontes Rainer warns, "HIPAA-regulated entities need to be proactive in ensuring their compliance with the HIPAA Rules, and not wait for OCR to reveal long-standing HIPAA deficiencies."[1] The prevalence of breaches in 2024 underscores this warning: many healthcare organizations only realize their security gaps after a serious incident occurs.

The financial impact of these breaches extends beyond reputational damage. A Paubox survey found that nearly 70% of IT healthcare leaders estimate the consequence of a HIPAA violation would cost over $250,000, but according to IBM, the true average cost of a data breach in healthcare is $9.8 million[2]. Cases like Solara Medical Supplies' $9.76 million class action settlement[3] highlight how regulatory enforcement is escalating, putting organizations at greater financial risk.

> According to IBM, the true average cost of a data breach in healthcare is $9.8 million.

Methodology

This report is based on data collected from the HHS Office for Civil Rights (OCR) Breach Portal[4], commonly referred to as the Wall of Shame. It includes breaches reported between January 1, 2024, and January 31, 2025 that were categorized as email-related incidents. The analysis also incorporates:

MX record analysis: Reviewing mail exchanger records of breached organizations to determine their email security provider.

SPF and DMARC: Assessing whether the breached organizations had properly configured email authentication mechanisms.

Risk classification framework: Assigning organizations to High, Medium, or Low risk based on their security configurations.

Comparative analysis: Evaluating security postures across different email security providers, such as Microsoft 365, Proofpoint, and Google Workspace.

Email security by the numbers

180

healthcare organizations fell victim to email-related breaches in 2024

43.3%

of healthcare breaches were Microsoft 365

5%

of known phishing attacks are reported by employees

264%

increased surge of ransomware attacks on healthcare organizations