Securing Patient Communications and Healthcare Data in an AI-Driven Ecosystem

How SER and DSPM can protect system-generated messages, patient data, and clinical workflows

Healthcare organizations send millions of system-generated communications daily for appointment reminders, lab results, patient portal notifications, and billing notices. The volume and velocity are only accelerating with rapid adoption of cloud platforms and AI-driven clinical applications that circulate sensitive structured and unstructured patient data.

Despite this move to modern tools, many organizations still rely on legacy email relay infrastructure that lacks visibility, authentication controls, and modern security protections, compounding risk for communication delivery, patient trust, and regulatory compliance. The path forward to removing such risks starts with understanding how secure email relay, cloud email services, and data security posture management can close gaps before they become breaches, headlines, or broken trust.

The risk of legacy email infrastructure

Every day, healthcare organizations dispatch millions of automated messages through platforms and patient portals like Epic's MyChart. As a result, patient trust has migrated to the inbox. Where a face-to-face consultation once anchored the care relationship, presumably secured digital communications now dominate.

"Healthcare is not only in the patient safety business or the patient care business; they're in the patient trust business," said Susan Biddle, Director of Healthcare Solutions for cybersecurity leader Proofpoint.

Compromised trust has real clinical consequences. Patients who doubt the legitimacy of digital outreach may delay or ignore care reminders. Exposed communications invite fraud.

According to the FBI's *2025 Internet Crime Report*, business email compromise generated more than $3 billion in losses, consistently ranking among the costliest cybercrime categories year after year precisely because it exploits trusted workflows rather than technical vulnerabilities.[1] Once credentials are compromised, a threat actor can operate inside an organization indefinitely, launching attacks that look entirely legitimate to recipients.

Despite the mission-critical nature of these messages, most system-generated email still flows through legacy, on-premises relays configured years before modern authentication became standard. These relays function openly; any source on the network can send email through them without credentials, scrutiny, or attribution.

When an EHR, billing system, or dozens of other applications, share the same unauthenticated relay, there is no isolated pipeline, meaning there are no credentials to trace and no way to investigate an incident without manual log mining. "We solved this problem for the general way that institutions used to communicate, yet this is no longer the general way communication exists, and we have to solve this problem again," Biddle said.

The authentication controls the industry fought for years to achieve — best known as DMARC, SPF, and DKIM — simply do not exist in most system-generated email environments. Biddle describes the situation as, effectively, a regression to pre-2018 security standards at a time when the rapidly expanding volume of AI-produced clinical communications greatly expands the attack surface and urgency to close such a gap.

Securing system-generated messages for the modern healthcare enterprise

The COVID-19 pandemic provided an early, painful stress test with a sudden uptick in electronic communications. Electronic health systems worldwide struggled to deliver test results and vaccination notifications that fixed on-premises relays could not handle volume-wise.

According to Ash Valeski, Senior Director, Product Management at Proofpoint, early customers saw critical patient communications simply fail to send. The problem was structural: fixed infrastructure cannot scale on demand, and unauthenticated relays offer no visibility into which source is causing a failure or a security incident.

The fix, he said, is architectural isolation: "Give your Epic email its own pipeline ... so that you have perfect visibility into that critical source of email, and you always know what it's doing."

A purpose-built secure email relay (SER) replaces fragmented legacy infrastructure with a dedicated, security-first pipeline. Think of it as a secure, inspected gateway that every system-generated message must pass through before reaching its destination. It requires authentication from every sending

"Healthcare is not only in the patient safety business or the patient care business; they're in the patient trust business."

SUSAN BIDDLE | Director of Healthcare Solutions | Proofpoint

"Are we just trusting that the developer or the third party is doing the right thing from a data sensitivity standpoint? That's a lot of trust."

ASH VALESKI | Senior Director, Product Management | Proofpoint

application — credentials tied to a specific originating address and authorized IP range — so that only messages from approved systems can relay through the channel.

Beyond authentication, a modern SER scans content for malware and sensitive data, enforces DKIM signing, and injects the one-click unsubscribe headers now required by Google and other major providers. These are deliverability requirements, not optional add-ons.

As health systems migrate workloads to cloud platforms, the challenge compounds. App developers whose tools live in AWS or Azure cloud environments often resort to mass-market relay services that are inexpensive but not designed with healthcare compliance in mind. A cloud-native SER resolves this by serving as a central, security-focused relay point regardless of where those applications are hosted, Valeski said.

Agentic AI applications, such as ambient clinical notetakers, billing agents, or care coordination tools, are given goals and use whatever data and tools are available to accomplish them. They do not discriminate between sensitive and non-sensitive information.

"Are we just trusting that the developer or the third party is doing the right thing from a data sensitivity standpoint? That's a lot of trust," Valeski noted.

The email relay is the last line of defense. It's the one control point through which all outbound communication must pass, regardless of which system generated it. Routing every application's email through a protection-focused email relay lets organizations scrutinize what agentic systems are sending and build an audit trail that supports compliance and incident response.

DSPM for the AI-driven healthcare enterprise

Data security posture management (DSPM) is the continuous practice of knowing where sensitive data lives, who or what can access it, how it is being used, and whether that posture is drifting.

In an AI-driven healthcare environment, this is now an operational imperative. Generative AI assistants embedded in everyday productivity tools are creating a forcing function, according to Derek Maki, Senior Vice President of Product, Data Security for Proofpoint. Organizations that have not done the foundational work of discovering, classifying, and labeling sensitive data are finding that these tools surface it regardless — and often to users whose access accumulated, unchecked, through years of role changes.

"AI is creating new risk for sure, but it's also perpetuating risk that's existed for many years," Maki said.

Roughly 80% of real risk exposure resides in unstructured data, where AI is generating new content faster than rules-based classification can keep up, according to Maki. Proofpoint's autonomous custom classifiers deploy within the customer's environment — sensitive data never leaves — and train on actual organizational data to achieve approximately 99% classification efficacy.

That level of speed and precision represents a significant departure from traditional approaches, which required extensive human intervention to build and tune classifiers over months. Maki pointed to one global healthcare customer that stood up more than 300 custom classifiers in 30 days — a deployment timeline that would have been unthinkable with legacy tools. When classification is reliable, enforcement becomes systematic across data loss prevention, insider threat, and outbound communication controls.

For health systems beginning this journey, the practical guidance is to start in a focused manner, he added. Pick a high-value platform like Microsoft's SharePoint or OneDrive, deploy discovery and classification, remediate over-permissioned privileges, and build momentum from early wins.

Track outcome-based metrics, such as stale data cleaned up, over-permissioned users remediated, and/or documents with unauthorized AI reach blocked. The goal is a unified, closed-loop program that connects discovery and data categorization all the way through to enforcement, linking DSPM to the secure email relay that governs what applications are transmitting. Knowing what protected data applications can access and controlling what they send form the complete security posture that AI-driven healthcare now requires.

> ***"AI is creating new risk for sure, but it's also perpetuating risk that's existed for many years."***

DEREK MAKI | Senior Vice President of Product, Data Security | Proofpoint

From vulnerable infrastructure to trusted communications

Security risks are playing out now in every health system that routes EHR notifications through an unauthenticated relay, in every AI scribe transmitting clinical conversations to a third-party vendor without governance in place, and in every SharePoint instance full of unclassified patient data that generative AI can surface with a single query. The attack surface is not emerging; it has already arrived.

What is emerging is industry recognition that this is an urgent issue. AI adoption is moving faster than security governance. Clinicians and developers are deploying tools that generate and transmit sensitive data without IT visibility. Legacy infrastructure was simply never built to carry the loads now being placed on it.

A modern SER directly addresses the communications gap. The technology gives health systems a dedicated, authenticated pipeline for every message that leaves a clinical platform, whether it originates from an EHR, a cloud-hosted application, or an agentic AI workflow. Every sending source is credentialed and traceable. Every message is scanned before it reaches a patient. The authentication standards the industry spent years establishing for traditional email are finally extended to the communications patients depend on most.

DSPM addresses what happens upstream of those communications, particularly continuously mapping where sensitive data lives, who and what can reach it, and how it moves across clinical systems, cloud platforms, and AI environments. When classification is reliable and enforcement is systematic, security leaders can say yes to new AI tools without flying blind.

Together, SER and DSPM close both ends of the loop: controlling what applications send and governing what data they should be able to access in the first place. As Biddle put it: "Healthcare has spent years trying to secure their system and has made a tremendous amount of progress. The next frontier, if you will, is about securing trust."

To learn more, visit proofpoint.com/healthcare.

References

1. Federal Bureau of Investigation, Internet Crime Complaint Center. 2026. *2025 Internet Crime Report*. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

proofpoint.

Proofpoint, Inc.

Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Produced by HIMSS