

Proofpoint Secure Email Relay

Protect patient data and improve email security and deliverability

Key highlights

- Secures transactional email sent from EHR platforms (such as Epic and Oracle Health), practice management systems, and patient portals
- Protects PHI in appointment reminders, lab results, and billing communications with optional encryption and DLP
- Simplifies HIPAA-aligned DKIM signing and DMARC compliance across every sending source
- Blocks compromised or spoofed senders from abusing your health system's trusted domains
- Helps ensure deliverability of critical patient communications to Gmail, Yahoo, Apple, and Outlook inboxes
- Simplifies migration to the cloud of on-premises relays used by clinical and administrative systems
- Supports unsubscribe header insertion and list management for patient communication programs

Healthcare organizations send large volumes of transactional email: appointment reminders, lab results, billing statements, and patient portal notifications. These messages originate from EHR systems such as Epic and Oracle Health (Cerner), practice management platforms, network-connected medical devices, telehealth tools, and payer or billing partners.

Much of this traffic carries protected health information (PHI) and must reliably reach the patient inbox. But not all sending systems and partners apply strong email security controls. This creates openings for account compromise, domain spoofing, and phishing campaigns that impersonate your health system.

Proofpoint Secure Email Relay (SER) consolidates and secures this transactional traffic. It adds DKIM signatures to every message to help meet DMARC requirements, blocks compromised senders from abusing your domains, and applies optional payload encryption and email DLP to protect sensitive data in transit.

SER also enforces application-level controls that give your health system precise oversight of every sending source. Each application connecting to SER authenticates with its own unique credentials, so every sending system is clearly identified and accountable. Once authenticated, SER applies application-specific authorization policies governing which sender identities an application can use and the volume it can transmit. SER can also enforce unsubscribe and suppression list management, helping ensure applications do not send to patients or members who have opted out.

Together, these controls protect trusted email channels, limit the potential impact of a compromised application, and give your health system the visibility to manage a diverse portfolio of clinical, operational, and patient engagement systems securely.

Secure Patient Communications from Risky Environments

Your health system likely has many applications and third-party partners that are authorized to send mail using your domains. This creates opportunities for attackers to compromise authorized sender accounts and send malicious email that appears legitimate and may pass authentication checks.

Proofpoint SER reduces this risk with a controlled, closed-loop relay system. Only verified business entities can send through the platform, eliminating the risks posed by open or free relay services. SER securely accepts email from authorized applications using SMTP authentication and TLS (STARTTLS) and applies Proofpoint antispam and antivirus protection to every message. It also blocks malicious attempts to send email as your organization.

SER consolidates legitimate application traffic, including EHR-generated messages, behind dedicated, reputable IP addresses. This helps protect your email reputation, your brand, and your patients from bad actors.

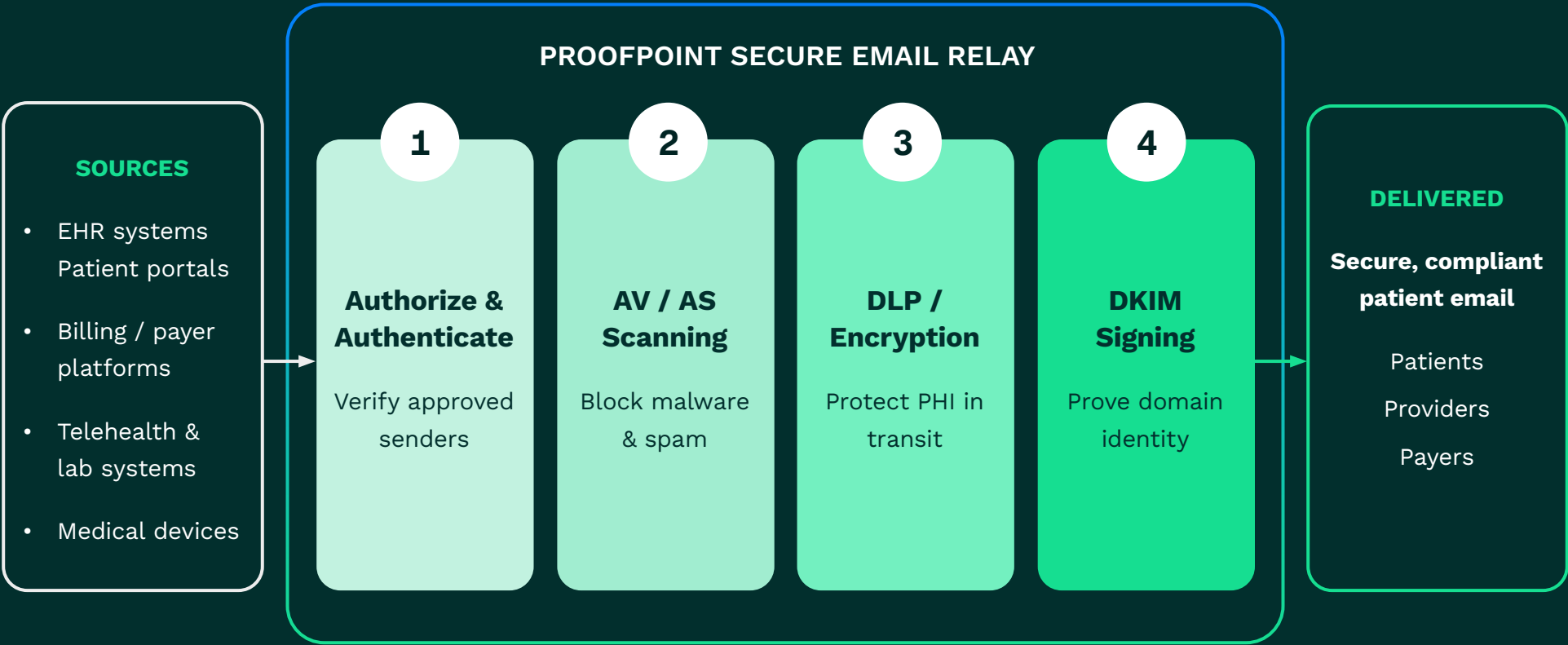


Figure 1. Ensure secure, clean, and HIPAA-aligned transactional patient email.

Accelerate DMARC Deployment Across Clinical and Administrative Systems

When your EHR, patient portal, billing vendor, and lab systems all send email on your behalf, achieving full DMARC compliance can be a challenge. Proofpoint SER simplifies this process.

SER automatically enables DKIM signing for outbound messages and ensures SPF alignment, so every sending source—including Epic and other clinical systems—meets DMARC authentication requirements. You don't have to make complex configuration changes or risk breaking critical patient communication flows to get there. With consistent authentication and visibility across all senders, your health system can move to an enforced DMARC policy faster.

Meet HIPAA and Regulatory Compliance Requirements

To stay compliant with HIPAA and other regulations, you need to protect PHI wherever it travels, including in appointment reminders, lab result notifications, and billing statements sent by automated systems.

Proofpoint SER helps ensure that transactional patient messages meet privacy and security mandates through optional encryption and DLP capabilities. These capabilities help support regulatory frameworks like HIPAA, as well as financial-sector requirements such as PCI DSS, SEC and FINRA for healthcare billing and payer communications.

Secure Clinical Applications Migrating to the Cloud

Healthcare organizations are moving clinical applications to the cloud, and industry research shows that most have either already made the move or plan to within the next two years.¹ Cloud and account compromise have also emerged as significant threats for healthcare organizations. When an EHR module, patient portal, or lab system moves off premises, its outbound email can move beyond the direct visibility of the security team that previously managed it on-site.

Proofpoint SER gives health systems a consistent, secure relay layer across cloud and on-premises clinical applications. SER provides consistent authorization, authentication, and security controls for cloud and on-premises senders, including antispam, antivirus, encryption, DLP, and DKIM signing.

This helps health systems migrate applications to the cloud without rebuilding their email security architecture or establishing sender reputation from scratch. It also helps reduce new deliverability and compromise risks associated with the transition. SER simplifies the migration process and helps protect patient communications throughout the transition.

Prevent PHI Data Loss from AI-Driven Patient Communications

EHR platforms represent one of the largest and most strategic technology investments for healthcare organizations. As these systems increasingly embed AI capabilities, healthcare providers are turning to agentic AI tools to automate clinical and administrative workflows, including patient communications.

As AI agents generate and send emails containing protected health information (PHI), healthcare organizations need to apply the same security and compliance controls used for communications sent by clinicians and staff. Without appropriate guardrails, AI-generated messages can expose sensitive patient data through misaddressed emails, excessive data sharing, or policy violations.

Proofpoint SER provides these guardrails through encryption and DLP for AI-generated outbound email. It applies PHI protection policies and helps prevent unauthorized disclosure before messages leave the organization. By extending these controls to AI-driven patient communications, healthcare organizations can enable AI innovation while helping maintain compliance and protect patient trust.

1. Ponemon. *Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care*. 2025.

Scale Security with AI Adoption

As healthcare organizations embed AI into more clinical and administrative workflows, the number of AI-driven senders and the volume of PHI-bearing email will grow. Agents may take on more patient-facing communications, including scheduling, follow-up, billing, and care coordination. Without a consistent relay point for these new sending sources, security teams can lose visibility into which agents are sending messages, who receives them, and whether appropriate policies are being applied.

Proofpoint SER provides a consistent control point as AI adoption grows, applying authorization, encryption, DLP, and DKIM signing to AI-generated email. This helps healthcare organizations expand their use of AI without allowing patient data protection to fall behind.

Ensure Deliverability of Critical Patient Communications

Bulk sender requirements from major providers such as Google, Yahoo, Apple, and Microsoft place greater emphasis on strong sender authentication and message integrity. Proofpoint SER helps your health system align with these requirements, so appointment reminders, lab results, and billing notices are more likely to reach patient inboxes instead of being filtered as spam.

SER applies DKIM signatures to outbound messages and helps support SPF and DMARC alignment. It also supports one-click unsubscribe capabilities for applicable bulk and subscription email. This can help health systems manage patient newsletters, wellness communications, and other optional communications separately from required clinical notifications.

Simplify SER Adoption and Ongoing Management

Proofpoint offers optional application owner support, migration planning and execution, and post-implementation deliverability services for SER. The solution is available as a standalone offering or as part of Proofpoint Collaboration Security Prime.

Health systems can deploy SER to address immediate sender authentication and deliverability needs or incorporate it into a broader strategy to protect email, messaging, and collaboration channels across the organization.

Contact your authorized Proofpoint representative for details.

About 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

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.