Personally Identifiable Information (PII) and Personal Health Information (PHI)

Ensuring Privacy in Regulated Industries

Email is firmly entrenched as a primary mode of business communication across desktops, gateways, applications, and mobile devices within and beyond enterprises. However, because email is a highly insecure channel for sharing information outside firewalls, regulated industries have had to resort to paper-intensive processes to share information.

Today, companies are transitioning to encrypted email for greater efficiency and cost-savings. As businesses share an increasing amount of sensitive, unstructured data via email, hackers will continue to attack. In response, government, industry, and consumers all demand improved privacy and security in email. especially in healthcare and financial services.

In the financial services industry, the combination of new state privacy regulations with customers' requirements for faster, more convenient services has driven the need for companies to implement end-to-end secure email systems.

In the healthcare industry, HIPAA and HITECH require and enforce the encryption of all Personally Identifiable Information (PII) and Personal Health Information (PHI). With the threat of public notifications and financial penalties for security breaches now more likely to be enforced, healthcare organizations can no longer afford to expose sensitive, personal information.

HPE SecureMail: Compliance Made Easy, Eliminate Paper-Driven Processes

HPE SecureMail simplifies compliance to privacy regulations, including PCI, HIPAA, HITECH, MA, UK FSA, and EU Data privacy directives and mitigates the risk of email security breaches. HPE SecureMail provides end-to-end security for email and attachments inside the enterprise to the desktop, at the enterprise gateway, and across leading mobile smartphones and tablets. Sensitive data is protected in transit and in storage. This turns email into a secure channel for communicating while eliminating time sensitive expensive paper processes.

HPE SecureMail accomplishes this by using the proven HPE Identity-Based Encryption (IBE) technology, a stateless architecture which avoids the scale bottlenecks associated with cumbersome webmail systems, traditional PKI or symmetric key approaches. Senders and receivers benefit from a simple user interface that makes secure messaging as easy and familiar as standard email communication.

Financial Services Use Cases

- Secure exchange of documentation between banks, partners and clients
- Protection of sensitive internal and external HR communications
- Secure strategic board and executive communications

Healthcare Use Cases

- Secure patient health care communications between hospitals, doctors, patients, labs, and insurance providers
- Secure payroll, accounting statement and billing attachments

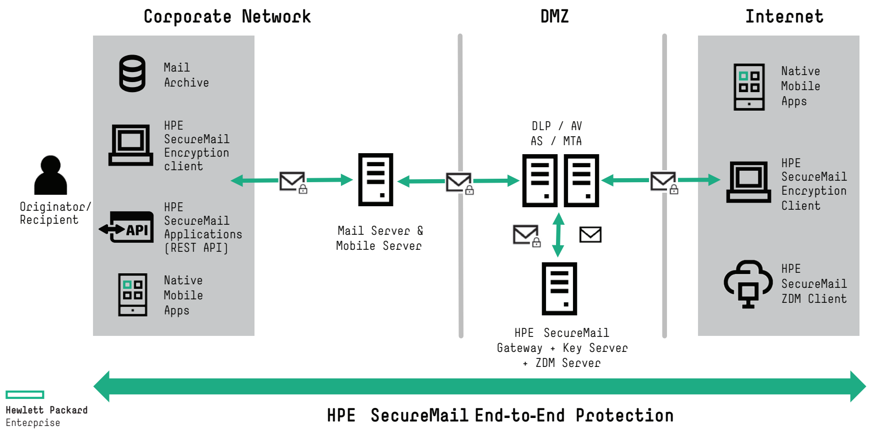
> "Competing encryption offerings we looked at would have required us to hire three or four dedicated administrators to keep everything running smoothly. HPE SecureMail can be managed with our regular email administrative staff, saving us a lot of time and money."
>
> – Project Manager,
> Major University Medical Center

Key Considerations

CONSIDERATIONS	HPE SECUREMAIL SOLUTION
Does the solution meet the compliance requirements of your industry such as PII, HIPAA, HITECH, and state privacy laws in one solution?	**End-to-end Standards-Based Encryption—**HPE SecureMail protects email data in storage, transit and in use and ensures compliance with the most stringent regulations.
Do you have a solution that easily integrates with your existing data loss prevention, anti-virus, anti-spam and e-discovery systems?	**Seamless Integration—**HPE SecureMail integrates with anti-virus, anti-spam, content filtering, data leak prevention (DLP), content hygiene services, archiving and eDiscovery, as well as with Outlook, Exchange, Active Directory and identity management systems.
Does the solution support mobile devices from one solution? Is the mobile experience native?	**Mobile email app for iOS BlackBerry Android smartphones—**HPE SecureMail Mobile Edition delivers secure mail into the user's existing mobile inbox for local reading.
Is the solution easy enough to use that employees will actually adopt it in compliance with industry regulations?	**Ease of Use—**native user experience across all platforms and devices, access to existing contact lists in all email systems, Send Secure button directly from inbox.
Can the solution grow with your organization's needs?	**Flexible and Scalable—**HPE SecureMail operates successfully in small companies and multinational organizations in the cloud, on premise, hybrid, or with cloud email services such as Office 365.
How do you ensure there are no breaks in the chain of security?	**Reduce the Risk of Security Breaches—**HPE SecureMail's data-centric security means that emails and attachments remain secure in transit, in use, and in storage.

HPE SecureMail Architecture

One Solution for Desktop, Web, Mobile, Cloud, Applications, and Automation


Corporate Network
DMZ
Internet
Mail Archive
HPE SecureMail Encryption client
Originator/ Recipient
API
HPE SecureMail Applications (REST API)
Native Mobile Apps
Mail Server & Mobile Server
DLP / AV AS / MTA
HPE SecureMail Gateway + Key Server + ZDM Server
Native Mobile Apps
HPE SecureMail Encryption Client
HPE SecureMail ZDM Client
Originator/ Recipient
Hewlett Packard Enterprise
HPE SecureMail End-to-End Protection

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA5-9776ENW, April 2016, Rev. 1