Hewlett Packard Enterprise

Business white paper

Safeguarding Healthcare Information and Leveraging HPE SecureMail in Your HIPAA Compliance Program

Table of contents

Introduction

Healthcare institutions are faced with a daunting problem: safeguarding sensitive healthcare and personal information in internal and external email communications. By default, the content of email is unprotected. As an email message travels from sender to recipient, it passes through servers and across networks that may provide attackers with opportunities to eavesdrop or even to access the content of the email. This could potentially expose protected health information (PHI), personally identifiable information (PII), intellectual property and other sensitive information in the body of the email message and the attached files.

The general solution for safeguarding email is to use an email encryption technology. Unfortunately, most of these products have significant drawbacks. For example, some don't provide protection along all parts of the transit path from sender to recipient. Some can be hard to use and too time consuming. And some may actually increase the vulnerabilities of a healthcare organization by storing messages and keys in the cloud.

This white paper introduces you to the email encryption solution that contains none of these drawbacks, and which provides many additional advantages as well: HPE SecureMail. It explains why HPE SecureMail is a first-rate solution for stopping threats against email sent within your organization and to outside recipients. It also highlights how HPE SecureMail can be leveraged in your Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) compliance programs.

Stopping Threats Against Your Institution's Email

Until very recently, there was a widespread misperception that email communications were private and secure, but that is definitely not the case. Front-page incidents where the contents of entire email stores—thousands and thousands of messages—were accessed and published, such as the Sony Pictures breach and the incident during the 2016 Presidential campaign have finally brought an end to this misperception. These high-profile breaches have also brought to the forefront an awareness of the staggering costs that can be incurred by the impacted organizations as a result of such email breaches.

"There was a widespread misperception that email communications were private and secure, but that is definitely not the case."

Healthcare institutions face so many potential threats against their systems, networks and data that it's easy to overlook threats against email as well. But the fact is that healthcare records are significant targets for attackers because they typically contain all the information thieves need to perpetrate identity theft, including fraudulently opening lines of credit and filing phony tax refund requests with the Internal Revenue Service. Additionally, thieves can also use the information from medical records to purloin prescription drugs for consumption or resale, or even obtain medical care or surgery under a false name, leaving the real person who owns the account to pay for the fraudulent charges incurred. The Ponemon 2016 Cost of Data Breach report found that the average cost per stolen record in the healthcare industry is approximately $355.[1] Compare that to the estimated $6.00 or less for purchase of stolen credit and debit card information, and it is clear that healthcare information is highly valuable and likely to be targeted by attackers who are motivated by profit. It is also clear that, when multiplied by the tens or hundreds of thousands of records usually involved in a breach, an incident could result in considerable expense to the impacted institution.

[1] **healthcareitnews.com/news/cost-data-breaches-climbs-4-million-healthcare-events-most-expensive-ponemon-finds**

“Average cost per stolen record in the healthcare industry is approximately $355.”

On a smaller scale, each of your institution’s emails is individually at risk of unauthorized access. An attacker may want to access the contents of email in order to sell the sensitive information they contain, such as healthcare records; to commit identity theft by misusing personal information; or to gain access to confidential or proprietary information about your institution. The latter could be used in many ways, from planning targeted attacks against the Human Resources department to stealing or even altering research data. These threats can come from both external attackers and insiders, so emails could be at risk even if they never leave your institution’s networks.

All email encryption technologies are designed to prevent attackers from viewing the contents of emails while in transit. The details of this vary can significantly from product to product, but the fundamental principle is the same. The sender, or a server near the sender, uses a cryptographic key to encrypt the content of the email. The encrypted email is then routed to the recipient, or a server near the recipient, that uses a second cryptographic key to decrypt the content, enabling the recipient to view the email message. Anyone monitoring the networks over which the encrypted email is carried is unable to decrypt it and view the original contents.

Email encryption solutions have become widely used for many reasons, including:

- Preventing costly and damaging data breaches by protecting sensitive data in transit.
- Enabling institutions to use cloud-based email and collaboration services by providing a way of protecting those emails.
- Supporting compliance with a variety of security and privacy legislation and regulations, such as HIPAA and HITECH.

Choosing the Best Email Encryption Solution

It’s important to carefully evaluate potential email encryption solutions for your healthcare institution before selecting one. Putting the wrong solution in place can significantly increase your IT staffing costs for both administration and technical support. It can also frustrate and impede your users, who are likely to circumvent a cumbersome or time-consuming solution and, in doing so, actually make a serious security problem even worse.

To assist you in evaluating potential solutions, here are six differentiators you should be sure to consider when conducting your evaluation of potential email encryption products:

1. Emails should be protected all the way from sender to recipient.
2. Emails sent from cloud-based services should also be protected.
3. Email encryption and decryption should be easy for both senders and recipients to use.
4. Cloud solutions should offer privacy protection without storing either the email messages or the keys.
5. Key management should be worry-free for on-premise solutions.
6. Product should cover all most important customer use cases.

Let’s take a closer look at each of these.

"HPE SecureMail provides end-to-end encryption, from sender to recipient without air gaps."

Differentiator 1: Emails should be protected all the way from sender to recipient.
Most people don't realize how many steps can occur in the transit of an email from sender to recipient. To illustrate this, imagine you are a health professional at a clinic. You need to get some PHI to a colleague at another clinic in your healthcare system. You compose an email on your laptop and click "Send." The email goes over the clinic's wireless and wired networks, and is then routed over the Internet to your healthcare system's enterprise network. Once it reaches the enterprise network, it passes through additional network segments and security devices until it reaches an email server. When your colleague is notified of your email, the same steps basically happen in the reverse order to deliver the email to your colleague.

In this example, there are many opportunities for attackers to intercept the email. Any network segment or device along the way could potentially be compromised or controlled by an attacker. An email encryption solution that can protect email along the entire path from sender to recipient, through all the networks and devices, is said to provide end-to-end encryption. **HPE SecureMail** enables end-to-end encryption. HPE SecureMail provides client endpoint message encryption capabilities to secure messages from when the message is sent until the message is opened by the intended recipient. HPE SecureMail provides desktop email client plug-ins and native mobile device applications to encrypt and decrypt messages on the device, including all email replies. The encrypted email message and payload are sent and stored (i.e. "pushed") to the recipient's email system until the recipient is ready to read the message. Once the user is authenticated, the message is decrypted and presented to the user. This protects against TLS vulnerabilities and "man-in-the-middle" security threats as the email is encrypted as it traverses the network to the recipients email system.

In addition to end-to-end encryption, HPE SecureMail also performs other functions to protect email. One such function provided by HPE SecureMail is to keep email messages encrypted when they're stored on mail servers, in recipient mailboxes, and in other locations en route to the recipient. Another is to use message integrity techniques so that email messages aren't altered or otherwise tampered with. Finally, HPE SecureMail also offers auditing capabilities so that your institution has a detailed log of each time a user sends an encrypted email.

"HPE SecureMail encrypt emails and files before they reach the Office 365 servers in the cloud."

Differentiator 2: Emails sent from cloud-based services should also be protected.
Many institutions have been transitioning from traditional email services, based on mail servers located at the institution's facilities and completely controlled by the institution, to cloud-based email services such as those provided by Microsoft® Office 365. Cloud-based email services can be a significant improvement for institutions by reducing support and infrastructure costs, as well as enabling users to access email from virtually anywhere.

Institutions switching to cloud-based email services need to be aware that their responsibility for providing end-to-end encryption for their users does not change because of this transition. Control over encryption should remain in the hands of users and administrators to ensure accountability by keeping the encryption keys separate from the encrypted email in the cloud. This helps to prevent a third party from easily acquiring both the keys and the email messages, then using the keys to decrypt the messages. HPE SecureMail encrypt emails and files before they reach the Office 365 servers in the cloud. Thus, **HPE SecureMail enhances the features of Office 365**, encrypting content sent to Office 365.

Differentiator 3: Email encryption and decryption should be easy for both senders and recipients to use.
If email encryption is difficult or time consuming for senders to use, odds are they'll find a way to circumvent it. Likewise, if recipients find email decryption to be a burden, they're likely to complain to senders, who will circumvent encryption in the future.

"HPE SecureMail makes encryption and decryption incredibly simple on desktop, mobile or web."

Recognizing these concerns, HPE SecureMail makes encryption and decryption incredibly simple on desktop, mobile or web. On desktop and laptops, HPE SecureMail adds "Send Secure" buttons to the user interface in Microsoft Outlook. All a sender has to do to encrypt an email is click "Send Secure." That's it. HPE SecureMail also has the unique SecureFile feature, which adds an "encrypt" button to Microsoft Word, PowerPoint and Excel. SecureFile enables users to encrypt files independent if they are sent via email or not. Users define who can open or edit any sensitive file for full security on cloud collaboration.

HPE SecureMail also offers mobile apps for iOS and Android and full integration with mobile device management from Blackberry. The HPE SecureMail mobile apps work with existing email client applications without requiring an additional secure mobile inbox or webmail service.

Because these actions are so simple, they're likely to meet with little resistance. Also, HPE SecureMail's approach minimizes training and support costs related to adopting and using email encryption and decryption.

Differentiator 4: Cloud solutions should offer privacy protection without storing either the email messages or the keys.
Most email encryption products do a poor job of fully protecting the privacy of their customers' emails. Such products have architectures based on centralized message and key stores. Basically, a message store is when all the encrypted emails pending decryption by their recipients are held on a server controlled by the email encryption product vendor. A key store holds all the encryption and decryption keys on the product vendor's servers. Since the vendor has access to both the messages and the keys, the vendor could potentially decrypt customer emails at will.

"HPE stores no messages or keys, enhancing customers' privacy in the cloud."

This is particularly concerning for the following reasons:

1. A malicious insider working for the vendor or supporting the vendor (contractor, etc.) could decrypt customer emails in order to steal sensitive information.
2. The vendor could be directed by law enforcement, courts, or other legal bodies to decrypt and turn over a customer's emails as part of legal discovery processes.
3. Messages are usually only stored on the vendor's servers for a limited period of time. If a customer doesn't pay for longer-term storage, the messages may be unavailable to both customer and recipient.

To avoid these risks, HPE SecureMail uses a push-based architecture. In a push-based architecture, each encrypted email travels from sender to recipient just as a regular email does. There are no message stores or key stores; emails simply go to their recipients and are stored, still encrypted, in their recipients' mailboxes until the recipients access and decrypt them. HPE stores no messages or keys, providing customers complete privacy in the cloud.

HPE SecureMail's breakthrough **HPE Identity-Based Encryption** (IBE) and **HPE Stateless Key Management** (SST) enable encryption without message scanning or retention of messages or keys. This dramatically reduces the risk of email contents being decrypted by anyone other than the recipient. The architecture also provides a highly scalable and flexible solution for email encryption because there are no message or key stores. HPE SecureMail can be used on-premise, **in the cloud**, or with a hybrid on-premise/cloud approach, all with the same privacy protections.

Differentiator 5: Key management should be worry-free for on-premise solutions.
A major drawback of many on-premise email encryption products is that they introduce a major burden: key management. Keys are needed to encrypt emails for each sender and to decrypt emails for each recipient. Each key must be managed throughout its lifecycle, including key generation, distribution, storage, replacement, recovery, and revocation. For most institutions, this requires hiring administrators dedicated to key management. The other option is to use a cloud-based provider that manages keys on behalf of your organization. But that option, as already discussed, comes with the drawback that the cloud provider has all of your keys and messages stored in their servers.

HPE SecureMail takes a different approach, one that completely eliminates the key management burden, including any need for email key management administrators. HPE SecureMail uses HPE Identity-Based Encryption and HPE Stateless Key Management together. That means that HPE SecureMail generates encryption and decryption keys on the fly for each email based on the recipient's email address. With this approach, there are no user keys stored with HPE or anywhere else. This is important because it dramatically reduces potential security and privacy risks associated with keeping all of the keys in a centralized key store.

It's important to note that HPE SecureMail also uses the latest industry standards for HPE IBE, including those listed below. This provides strong protection and avoids the use of proprietary, unproven encryption schemes, which are more likely to contain exploitable weaknesses.

- Institute of Electrical and Electronics Engineers (IEEE) 1363.3-2013, IEEE Standard for Identity-Based Cryptographic Techniques Using Pairings
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-5:2015, Information technology—Security techniques—Encryption algorithms—Part 5: Identity-based ciphers
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 5091, Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems
- IETF RFC 5408, Identity-Based Encryption Architecture and Supporting Data Structures
- IETF RFC 5409, Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)

Differentiator 6: Product should cover all most important customer use cases.
A final distinction between HPE SecureMail and other products is that HPE SecureMail offers a great deal of flexibility for expanding its capabilities. Institutions that don't need additional capabilities can save considerable money by adopting HPE SecureMail instead of a cumbersome competing product that includes many unnecessary or unwanted features. Institutions that do want additional capabilities can choose the best-of-breed products they want from HPE or others, then easily integrate those products with HPE SecureMail to build a complete solution tailored to the specific needs of the institution.

> "The SecureFile feature adds an "encrypt" button to Microsoft Word, PowerPoint and Excel for additional security in cloud collaboration."

HPE offers several **add-ons for HPE SecureMail**, including the following:

- **SecureFile** adds an "encrypt" button to Microsoft Word, PowerPoint and Excel. SecureFile enables users to encrypt files independent if they are sent via email or not. Users define who can open or edit any sensitive file for full security on cloud collaboration
- **Mobile** add-on provides iOS and Android apps for mobile use of HPE SecureMail
- **Application Edition** add-on, which provides a web services application programming interface (API) for integrating other applications with HPE SecureMail
- eDiscovery add-on, which offers supervisory capabilities for performing eDiscovery of emails (e.g., decrypting .pst files of employees who have left the institution)
- **Good Dynamics** add-on, which integrates the Good Dynamics mobile device management (MDM) product with HPE SecureMail to provide easy-to-use email encryption capabilities for Good Dynamics users

HPE also partners with other security product vendors to extend HPE SecureMail's capabilities. HPE SecureMail can be paired with the Digital Guardian data leak prevention (DLP) product to add DLP capabilities to HPE SecureMail. This enables an institution to detect attempts to send certain types of sensitive information such as PHI or PII via email and to automatically encrypt the content of the email message. DLP is invaluable for preventing data breaches whether the information is sent intentionally or accidentally.

Leveraging HPE SecureMail for HIPAA and HITECH Compliance

Institutions are often challenged to meet and maintain compliance with the requirements in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). This is largely due to how vague most of the requirements are. Figuring out which security controls need to be used can prove frustrating.

Because emails can carry PHI over unsecured networks and onto unknown mail servers, this information must be protected, and the only security control capable of doing this today is an email encryption product. HPE SecureMail provides strong standards-based end-to-end encryption that protects PHI across networks and on email servers. HPE SecureMail also performs detailed auditing, which supports compliance with HIPAA and HITECH. HPE SecureMail is used by multiple customers in the **healthcare and life-sciences industries** as part of their HIPAA and HITECH compliance programs.

HPE SecureMail is used by multiple customers in the healthcare and life-sciences industries as part of their HIPAA and HITECH compliance programs.

In addition, because HPE SecureMail doesn't use message scanning to encrypt messages, nor does it store messages or keys, an institution maintains control over the content of its email and HPE does not access the contents of sensitive messages. According to Federal government guidance on the HIPAA regulations, "...a Business Associate Contract Is NOT Required... with a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents." In most cases, this lessens the need for an institution using HPE SecureMail to sign a Business Associate Agreement (BAA) because HPE does not have access to unprotected information from the institution's emails.

Conclusion

Unauthorized access to the contents of a single email from your institution—let alone thousands of emails—can lead to a data breach and potentially a HIPAA violation as well. This could cause serious harm to your institution and its reputation, as well as embarrassment, or more serious impacts to the individuals whose information was accessed. Institutions need to have a robust, flexible and scalable email encryption technology in place to prevent such consequences.

HPE SecureMail provides an outstanding solution for your institution's email encryption needs. It provides end-to-end encryption for emails, from senders to recipients, regardless of whether your institution uses traditional email servers or cloud-based email services. HPE SecureMail is easy and quick for both senders and recipients to use. Because it uses Identity-Based Encryption and stateless key management, it greatly enhances privacy by avoiding the use of key and message stores, and it reduces additional administrative burden on your technical staff. Additionally, it is significantly more cost efficient than other, older email encryption products. Finally, HPE SecureMail offers many options for expanding its capabilities through HPE add-ons and partner products, allowing your institution to tailor your email encryption solution so that it perfectly meet the needs of your institution.

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

[2] **hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf**

Sign up for updates

Hewlett Packard
Enterprise