zix | Google

A CASE FOR EMAIL ENCRYPTION

Improve Compliance, Secure PHI and Protect Relationships

Healthcare organizations face an ongoing compliance burden involving the protection of sensitive patient data. The task of safeguarding data grows increasingly complex as the organization's environment adapts to advancing threats and shifting technology trends. Once simply in record rooms and on desktops, now protected health information (PHI) is mostly electronic, on the move via email and, in email, is likely being viewed on smart phones and tablets. Securing PHI in email will not only meet a regulatory compliance need but will protect an organization's reputation.

The Final Rule

Achieving compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Health Information Technology for Economic and Clinical Health (HITECH) Act, while always important, became a top priority with the announcement of the Final Rule. Expanding obligations to even more organizations in the healthcare industry, the Final Rule provides federal protections for PHI held by covered entities, their business associates and sub-contractors and reaffirms the standard that PHI should be rendered "unusable, unreadable, or indecipherable to unauthorized users."[1]

If a breach of unsecured PHI occurs, covered entities and any related business associates and sub-contractors must provide notification of the breach to affected individuals and the HHS Secretary. If a breach affects 500 individuals or more, the breach is published on the OCR breach list and media outlets serving the affected individuals' state or jurisdiction must be notified.

Beyond the reputational costs associated with a breach, organizations face onerous resolution agreements or possibly fines of up to $1.5 million. They also bear the costs of notification, consumer protection and potential lawsuits. The result is a price tag of $3.8 million per data breach, or $154 per compromised record, according to a 2015 Ponemon Institute study.[2]

Top Source of Data Loss

So how does your healthcare organization protect its patient data, meet compliance standards and prevent breach costs? In assessing vulnerabilities, one potential threat rises to the top — email.

Employees exchange dozens of emails per day. With the convenience of email as a communication and file-transfer method and the perceived difficulty of encryption, it's easy to overlook the risks for the sake of productivity; however, IT security and compliance professionals cannot ignore the sheer volume of unsecured PHI exchanged regularly between covered entities, business associates, sub-contractors and patients.

Safe Harbor through Encryption

Email encryption delivers a safe harbor under HIPAA. As listed by the Federal Registrar, "While covered entities and business associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor."[4]

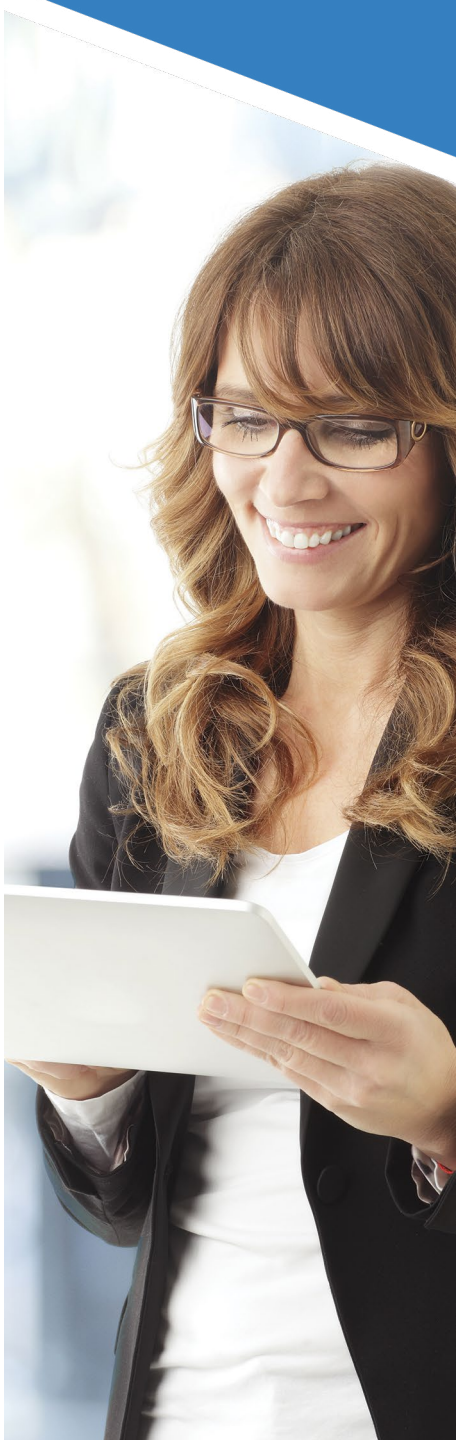
Combining encryption with other advances — automated, policy-based services, easy-to-use functionality and next generation mobility — addresses risks, concerns and compliance standards associated with email.

Outdated Technology Creates Risks

Business is no longer conducted behind a desk. Mobile devices have expanded the workplace and work hours, and more users spend time on email than any other mobile app.[3] Outdated email encryption solutions haven't kept pace with increasing dependence on mobile devices, forcing users to overcome distorted screen layouts and numerous complex steps. The results are stifled productivity, user frustration and security workarounds.

The Average Data Breach

costs $3.8 million per data breach, or $154 per compromised record.[2]



The inconvenience of outdated technology also creates an unnecessary burden on employees and recipients. Although compliance is critical, barriers to easy communication lead some employees and recipients to ignore policies and security practices simply to be efficient and move business forward. Even if employees and recipients are diligent, mistakes still happen if you rely on individuals to determine when encryption is needed.

These risks can be avoided with innovative email encryption.

Google Apps Message Encryption

Email encryption should not be difficult. Recognizing the evolving needs of your company, employees, patients and partners, Google Apps Message Encryption (GAME) provides innovative secure email for Google Apps users that is just as easy to use as regular email. Our top advancements include:

Automatic Scanning of Employee Emails

Powerful email encryption allows your employees to maintain their normal workflow and focus on their responsibilities. With automatic scanning and the use of proven and up-to-date policy filters, emails with sensitive content are encrypted without user action. Removing the hassle and taking the decision out of your employees' hands eliminates human error and better protects your email.

Convenient Delivery for Recipients

If your employees don't have to take any extra steps to encrypt email, why shouldn't your patients and partners be able skip the hassle too? GAME leverages the industry's only automatic decryption of secured emails if recipients use the same platform. Seventy-five percent of GAME encrypted emails are accessed without any extra steps or passwords.

For others who don't use the same platform, recipients can receive the message in less than two simple steps, removing any hassle and confusion.

75 percent
of encrypted messages are accessed without any extra steps or passwords.

Smooth Mobile Experience

Convenient mobile delivery of encrypted messages is a critical component to keeping business moving and making your patients and business partners secure and happy. For senders and recipients using GAME secure email is once again just as easy as regular email, because it is encrypted and decrypted automatically.

For other recipients, optimized layouts designed for the user's screen combined with an easy registration and login experience ensure mobile access is as seamless as the desktop experience.

Taking the Next Step

Healthcare organizations face a heavy compliance burden. Check one thing off your list. With the right solution, email encryption can be an easy way to protect a top source of vulnerability for your organization.

1. **The Health Information Technology for Economic and Clinical Health Act.** http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

2. **"The Cost of a Data Breach" by Ponemon Institute, 2015.** http://www.ponemon.org/blog/cost-of-data-breach-grows-as-does-frequency-of-attacks

3. **HHS 45 CFR Parts 160 and 164, Federal Register, April 27, 2009.** http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

4. **"BYOD and Mobile Security Report" by Holger Schulze, Information Security Community, 2014.** http://www.slideshare.net/informationsecurity/byod-mobile-security-report