THE IMPORTANCE OF EMAIL ENCRYPTION IN THE HEALTHCARE INDUSTRY

EXECUTIVE SUMMARY

Email is a critical business communications tool for organizations of all sizes. In fact, a May 2009 Osterman Research survey[1] found that 97 percent of email users consider it to be important or extremely important in doing their work. By contrast, only 86 percent of users felt this strongly about the telephone.

The increasing complexity of email implementation options and government security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), create unique challenges for the effective use of email by healthcare providers. As patients, partners and healthcare vendors rely more on email, healthcare organizations must consistently use email in a way that will ensure government mandated compliance.

This white paper explores the email challenges facing healthcare providers and provides a brief overview of recommended hosted email and encryption services that will alleviate many of those challenges. The paper then discusses best practices for an integrated, secure hosted email infrastructure implementation that will provide the tools healthcare organizations need to achieve compliance.

EMAIL ADMINISTRATION CHALLENGES FACING HEALTHCARE PROVIDERS

While there are many large healthcare conglomerates with IT budgets and staff, there are just as many smaller healthcare organizations that rely on an office manager or even the practitioners themselves to manage their back-office IT systems. The staff at these physicians' offices, clinics, assisted living facilities, nursing homes, dentists, chiropractors and even pharmacies take on many different roles. As such, they may not have the time or technical expertise to grasp HIPAA's implications and requirements for secure email.

The challenging economic climate has also had a significant impact on small healthcare organizations. A recent study[2] from the Medical Group Management Association surveyed some 2,000 medical practice

[1] The Importance of Social Networking Tools Relative to Conventional Tools, May 2009, Osterman Research, Inc.

[2] Medical Practice of the Future: Competitively Position Your Products and Services.

managers regarding the economic downturn. According to the study's findings, the top three challenges associated with economy were identified as:

1. Dealing with operating costs that are rising more rapidly than revenues.
2. Maintaining physician compensation levels in an environment of declining reimbursement.
3. Selecting and implementing an electronic health records (EHR) system.

In light of these challenges, healthcare providers need to streamline the administration of their back-office IT systems, including email, wherever possible. The goal is to free up already stretched office staff from the burden of day-to-day administration of email servers, while keeping operating costs low.

HIPAA AND ITS IMPLICATIONS FOR EMAIL SECURITY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established ground-breaking national standards designed to make the healthcare system more efficient, accessible and most importantly, secure. There are three specific HIPAA regulations that pertain to the use of email within a healthcare organization:

1. The Electronic Data Interchange (EDI) Rule: Establishes standard health information terminology and electronic billing code sets to make the transition online for many healthcare organizations as seamless as possible.
2. The Privacy Rule: Mandates organizations maintain the confidentiality of Protected Health Information (PHI) – individually identifiable health information – and defines allowable uses and disclosures of this private information.
3. The Security Rule: Establishes standard safeguards so that all healthcare organizations know how to protect the confidentiality, integrity and availability of electronic PHI.

It's important to note that while these regulations apply to all healthcare organizations, they also apply to any business entity that works with healthcare organizations to handle patient information. Whether it's an accounting firm, lab consultants or even a temporary agency, HIPAA's influence on email communications is widespread.

WHY HEALTHCARE PROVIDERS MUST CARE

Organizations are responsible for developing, implementing and managing their HIPAA compliant security policies. If ignored and information breaches occur, there can be significant financial penalties. To emphasize how serious the government is about this, in 2009, The Health Information Technology for Economic and Clinical Health Act (HITECH) was passed, setting even stricter rules for disclosure reporting, privacy monitoring, the limited use of personal medical data for marketing, and patients' electronic access to their health information. HITECH also increased the maximum penalty for compliance violations ranging from $1,000 to $50,000 per violation, to as much as $1.5 million for repeated violations. These regulations are not to be taken lightly, because a single violation for a small healthcare provider could be a tremendous set back. In a time when many organizations are already feeling the weight of the economic recession, a HIPAA compliance issue and related fine could be the last straw.

Even when taking standard precautionary measures (e.g. staff training, courier delivery, etc.), email-based HIPAA violations can occur. These, for the most part, tend to be accidental, such as sending an unencrypted note that contains patient health information to an incorrect address. Under the new legislation however, the ramifications of these types of oversight are extreme. Organizations are required to report breaches to the individuals affected. If the breach affects more than 500 individuals, the breach must be reported to prominent media and the US Department of Health and Human Services.

For example, Walgreens had to publicly acknowledge and take full responsibility for a data breach in which the personal information of 28,000 retired Kentucky state employees was emailed without encryption. Birthdates, Social Security numbers, and health insurance claim numbers were among the information sent from Walgreens to an employee at the Kentucky Retirement Systems (KRS)[3].

There was no evidence of interception and the likelihood that the retirees would become identity theft victims as a result of the security violation was considered "minimal."

Nonetheless, Walgreens and KRS each issued notifications to retirees.

THE REQUIREMENTS FOR COMPLIANCE

With an understanding of why it is critical for healthcare organizations and their affiliates to meet HIPAA's requirements for email, it is just as important to discuss how they can achieve compliance.

The Security Rule is the most applicable to email as it requires organizations to protect the confidentiality, integrity and availability of the private patient information they create, receive, maintain and transmit.

The first technology requirement for Security Rule compliance specifies that all incoming and outgoing email messages are made available regardless of how long ago they were sent or received. This is achieved through the implementation of an archiving solution. The second requirement for the Security Rule addresses confidentiality and integrity of email messages. Specifically, HIPAA compliance requires multiple layers of encryption:

1. Domain-to-domain encryption (also known as "Boundary Encryption"): Creates a secure email network between an organization and nominated business partners with Transport Layer Security (TLS). All emails sent and received are encrypted.
2. Policy-based encryption: Establishes rules and parameters that will automatically encrypt emails based on words and phrases (i.e. "patient" or "ssn") found in the email.
3. User-based encryption: A user decides which emails should be encrypted.

[3] Kentucky government retirees victims of Walgreens' data breach http://www.blogiversity.org/blogs/identitytheft/archive/2009/03/23/kentucky-government-retirees-victims-of-walgreens-data-breach.aspx#ixzz17aOY8Emc

Compliance with this second requirement of the Security Rule is achieved through the implementation of an encryption solution. The most basic of these encryption layers is user-based encryption, but a policy-based encryption solution is most ideal since it reduces the chance of user error.

EMAIL SOLUTIONS

There are two basic types of email infrastructures. The first is on-site, also called in-house email management. The other is hosted email, where the healthcare organization outsources its email services to a third-party vendor.

The benefits of utilizing a hosted email service, instead of on-site management, are tremendous for healthcare providers of all sizes. Studies comparing both types of IT environments have repeatedly shown the overall cost of hosted email is significantly lower. Osterman Research estimates hosted Exchange can typically reduce management costs by more than 50 percent compared to an on-premises implementation. The fixed cost per email seat and flat monthly management fee – particularly when there are unforeseen issues – provides predictability and stability. In addition, hosted email vendors offer their customers a level of security not possible for most organizations that want to manage their own IT resources: from physically secure facilities, to robust data backup systems to the latest IT infrastructure certifications such as SAS Certification and PCI Compliance.

Hosted email providers also offer a team dedicated to customer support, even outside of normal business hours, to ensure email is available at all times. They have the expertise and bandwidth needed to manage email, freeing up those people once in charge of the communications systems, to work on projects that bring more direct value to the organization – like caring for patients.

BEST PRACTICES: A COMPREHENSIVE SOLUTION

While these security requirements may appear complex, there are secure hosted email solutions available, such as Pinnacle Consulting's hosted Exchange that make the implementation and management of these email systems seamless and affordable, even for the smallest of healthcare organizations. A secure hosted email solution incorporates both the archiving and encryption capabilities required for compliance into one integrated solution. As such, the end user is shielded from the complexities of these added layers of security, thereby making a hosted solution the easiest to use while still meeting HIPAA compliance requirements.

PINNACLE CONSULTING HOSTED EXCHANGE

Pinnacle Consulting is a premier provider of communications services, including hosted Microsoft Exchange. Currently used by 160 million people worldwide, Microsoft Exchange is the leading business-grade email messaging system employed in North America. Exchange offers a number of capabilities in addition to email; including calendaring, task management, address lists and access to shared document repositories and other functions.

By partnering with Pinnacle Consulting is for secure Exchange hosted email, healthcare providers can leverage four key differentiators to ensure they are prepared to meet HIPAA compliance:

Support – Pinnacle Consulting provides an experienced support team that handles the Exchange email infrastructure from implementation to ongoing management.

- True 24x7 support
- Microsoft-certified Exchange support staff
- Expert phone support in less than one minute

Infrastructure/Reliability – Pinnacle Consulting offers a level of reliability that ensures email is protected

- Only premium servers and network
- Multiple live and backup copies of your email and other critical business data, making it virtually indestructible
- Premium spam solution enhanced with Comtouch plug-in

Control – Pinnacle Consulting allows its customers to have the control they want to utilize email to its fullest potential.

- Proprietary control panel designed to give healthcare providers intuitive controls
- Online portal to add/delete users, provision all services including mailboxes, wireless email (BlackBerry, iPhone, Android), distribution lists
- Active Directory synchronization to run on-premise IT alongside Pinnacle Consulting services
- Advanced controls available, just like on-premise servers

Free Migration – Pinnacle Consulting makes it a seamless – and free – process for healthcare providers to scale and upgrade their Exchange environment.

- Dedicated Exchange migration team to guide new customers through migration process each step of the way
- Migration typically conducted over the telephone, with live one-on-one support
- Proprietary tools to automate migration
- Migration of Active Directory achieved in as little as 60 minutes

ENCRYPTED EMAIL

Encrypted Email from Pinnacle Consulting helps reduce the challenges and complexity of managing regulatory compliance and data loss protection of your Pinnacle Consulting hosted email. This is a policy-based managed encryption solution that provides healthcare organizations with an easy way to enforce email encryption without disrupting the day-to-day workflow of their staff. It puts the control back in the hands of the IT department by enabling them to manage the organization's entire email infrastructure.

- Comprehensive: Uses standards-based encryption in which encrypted messages are digitally signed and able to be validated for compliance purposes.
- Customizable: Enables rule association with outbound email content to protect organizations from liabilities associated with privacy and security; Reporting feature enables IT to audit employee usage and make changes.

- Easy to Use: Hides encryption complexities from the end user; policies can be easily added and updated through a centralized console.

Pinnacle Consulting's industry-leading partner offers an additional archiving product that works together to provide a full end-to-end solution for email security and compliance:

LiveOffice Mail Archiving: LiveOffice offers a complete and affordable software-as-a-service (SaaS) solution designed to seamlessly manage email archiving, as well as simplify mailbox management, shrink storage costs and reduce backup windows. It protects a healthcare organizations' most confidential information by developing and enforcing strict email policies.

- Total assurance. Covers all HIPAA compliance regulations.
- Secure environment. Messages are transmitted, stored off-site and backed up with the highest levels of security. Access is strictly controlled.
- Detailed management. Compliance officers and IT managers can set detailed parameters for the services using dedicated compliance management software.

CONCLUSION

There are many unique challenges facing small healthcare providers, but managing a secure, HIPAA-compliant email infrastructure need not be one. Armed with an understanding of HIPAA, its requirements for secure email and a trusted partner, any potential for violations or breaches could virtually be eliminated. As this whitepaper describes, comprehensive hosted secure email solutions are easy to implement, safely outsourced and most importantly, affordable. HIPAA compliance is not a choice or a nice-to-have – it's the law. Evaluate your communications infrastructure and make the right decision before it's too late.

HIPAA COMPLIANT EMAIL CHECKLIST

- Does your organization ever communicate by email with patients?
- Do you ever communicate by email with insurance companies, billing companies, laboratories or other external companies?
- Do you ever include a patient's name, address, phone number, condition, diagnosis code, drug or prescription information, Social Security Number, insurance ID number, billing information or any other confidential, proprietary patient data in any email communications?
- If you had to, could you prove that no Protected Health Information (PHI) had ever been sent by an unencrypted email?
- Could your organization withstand either the financial or reputational harm caused by an unintentional breach of confidential patient information?

WHAT TO ASK PROSPECTIVE PROVIDERS:

- How long have you been in the hosted Exchange business?
- What experience do you have supporting healthcare customers?
- What does your hosted Exchange service include, e.g. software versions, storage, etc.?
- How do your encryption and archiving capabilities address HIPAA compliance?
- How many data centers do you operate and what are their specifications and certifications?
- How secure are your data centers?
- What support do you offer?
- How long does it take to migrate our environment to your services?
- What Service Level Agreements do you offer?