

Healthcare Industry Best Practices for Securing Email

E-mail has become an essential business tool in the healthcare industry, as a communications mechanism universally available to all healthcare participants. However, healthcare organizations are challenged with maintaining the ubiquity and usefulness of e-mail in the face of HIPAA privacy and security regulations requiring varying levels of control, tracking, and encryption of PHI disclosures. This paper lays out a set of best practices to help healthcare organizations create and manage a secure e-mail infrastructure that continues to support open communications with all healthcare participants, while ensuring the security of PHI and compliance with HIPAA regulations.

E-mail is Mission-Critical in Healthcare

There is no doubt that e-mail has become a vital tool for business and personal communication. E-mail provides a highly efficient and cost-effective way to deliver person-to-person messages, files and documents across organizational boundaries. Today most companies have put their faith in email, depending on it for time-sensitive, business-critical information, and email messages are now widely considered business records, rather than transitory communication. According to the Radicati group, there are over 400 million corporate mailboxes worldwide, and more than 45 billion e-mail messages are transmitted each day within enterprises. As a result of this growing use, businesses are increasingly dependent on e-mail to operate their businesses.

In the healthcare industry in particular, e-mail has become a well-entrenched communications tool, as health plans and health care providers struggle to improve the efficiency of their operations in a fragmented and highly regulated operating environment. Increasingly, healthcare organizations (HCOs) are leveraging e-mail to reduce costs and streamline communications with trading partners, peer organizations, governing bodies, business associates, physician groups, patients, and members. Health plans regularly use e-mail to support core business processes such as sales, enrollments, claims processing, billing, and payment processing. Health care providers are aggressively expanding their use of e-mail to help streamline communications and cut costs in both administrative and clinical domains. This includes using e-mail to communicate lab results, for physician-to-physician

“In our surveys, we’ve found that some of the largest e-mail users in healthcare organizations are business offices, risk management, case management, provider enrollment, and some of the patient care areas.”

Ann Geyer, Tunitas Group

consults, or as a supplement to traditional doctor/patient communication channels for scheduling appointments, requesting medication refills, asking follow-up questions, or providing patient education.

E-mail Communication of PHI is Pervasive

The difficult challenge facing healthcare organizations is what to do about communications of Protected Health Information (PHI) in e-mail. PHI generally includes any individually identifiable health information created or acquired by health organizations subject to HIPAA. The results of several HIPAA Privacy Rule compliance studies recently conducted by a number of healthcare organizations have reported that as much as 40% of all email emanating from HCOs contains some PHI, and that such use of email is pervasive across all types of business units.

What is notable about the emergence of email as an important mechanism to communicate PHI is that its use has often grown organically, and without a supporting business infrastructure to address security concerns. In fact, in some cases

'No PHI' Policies Don't Work

"In today's world, particularly with the compliance issues now facing us on both the privacy and security sides, a 'no PHI' e-mail policy is guaranteed to place your organization in jeopardy. You'll be lucky if its followed, and the expectation is that it won't be followed. If you are so lucky as to have users that are well behaved and follow this rule, you'll find that you're obviating a lot of the investment value of your e-mail system."

Ann Geyer, Tunitas Group

e-mail continues to be used to communicate PHI despite specific HCO policy sanctions against it. Some HCOs, uncomfortable with the enterprise level policy and procedure requirements for secure Internet messages, have chosen instead to prohibit the use of email and the Internet for transmission of confidential patient information. However, the value of email is so compelling in supporting task completion that many groups within the HCO continued to use it against policy. The practical effect of a 'no PHI in email' policy has been to allow a critical piece of the organization's business

infrastructure to evolve without appropriate attention to security concerns. But whether by inattention or explicit policy, many healthcare organizations are left to play catch up and supply an e-mail security infrastructure to an existing communication channel.

The Challenge – Protect PHI Without Diminishing the Value of E-mail

The increasing use of e-mail communications provides huge cost and productivity benefits to healthcare organizations by supporting the efficient exchange of clinical and administrative data, and transfers of bills and money. On the other hand, this very ease of access and use can threaten patient privacy, and expose the organization's computing infrastructure to spam and virus attacks. The challenge that HCOs face is to implement security controls to protect PHI in a way that does not significantly diminish the business utility of e-mail.

For example, HCO operations have come to depend upon the routine processing of its messages by trading partners and business associates. In some provider organizations, the business office heavily uses email to resolve claim adjudication and authorization questions. If a new security implementation places cumbersome or inefficient e-mail security requirements on payers who receive these messages, the consequence of the provider's security implementation could actually be to slow reimbursement. Obviously, such an outcome, from the provider perspective,

is very undesirable. In addition, security processes that are inefficient from either an internal and external user perspective could have the effect of actually *reducing* security, as workforce members will seek alternate electronic communication channels to exchange the messages needed to complete their work tasks.

Best Practices for Securing E-mail

In the healthcare industry, a set of best practices for securing e-mail are starting to emerge as leading payer and provider organizations finish deploying their HIPAA privacy solutions, and begin to examine how these implementations need to be modified for the impending security regulations deadline. In general, HCOs have focused their deployments on three core requirements:

- Identify and securely deliver messages containing PHI for HIPAA compliance
- Track and document compliance with HIPAA regulations for regulatory and legal risk mitigation
- Protect the network from e-mail-based threats including spam, viruses, worms and hackers

This paper brings together a set of lessons learned from these implementations to provide guidance for HCOs seeking to improve their e-mail security. Specifically, the paper describes a set of technology-neutral best practices that HCOs should consider in developing their email security infrastructures.

Healthcare Industry Best Practices for Securing E-mail	
1.	Audit e-mail use
2.	Recognize disclosure limitations
3.	Leverage trading partner encryption capabilities
4.	Don't overlook inbound messaging
5.	Seek encryption transparency
6.	Use structured messaging with patients/members
7.	Develop appropriate patient/member account provisioning
8.	Automate exception handling
9.	Establish a continuous improvement process
10.	Secure the infrastructure

1. Audit e-mail use

IT management is typically unaware of how email is used to support healthcare business functions, and e-mail is rarely (if ever) monitored for compliance with content and authorized-recipient policies. Relevant questions include:

- Are email disclosures of PHI typically ad hoc or part of a recurring business process?

- What workflows within the organization are dependent on routine processing of email by external recipients, and how critical is the timing of that processing?
- Who in the organization is regularly using email for communications with members / patients?

Without knowing the answers to these kinds of questions, it is unlikely that the HCO will be able to develop a security infrastructure that preserves the business value of email.

Unfortunately, to figure out the answers to these questions it may not be enough to ‘poll’ enterprise users regarding their e-mail practices. In some circumstances, these practices may actually be contrary to the organization’s Internet use policy, so users may not be forthcoming with respect to actual use. In other situations, profiling e-mail use practices across different parts of the organization can be extremely difficult due to the breadth of recipients and business functions.

Ultimately, a good understanding of the organization’s use of Internet e-mail must involve inspection of the message content and identities of senders and recipients. Such inspection would reveal whether or not the message requires some special treatment, as is the case where the message contains PHI. The source and target identities provide additional information about the context for such transmissions, from which business requirements of the security solution can be further investigated.

Given the very large number of messages sent and received by healthcare organizations, manual selection and inspection of messages is undoubtedly not possible. As a practical matter, investigators should use some sort of a ‘content filter’ to identify e-mail messages with the sensitive content. Such a filter can be used to create a log of these sensitive messages including both their source and destination. This log provides the basic data for analysis and requisite understanding of the organization’s messaging use. Note that this type of automated audit capability can be incorporated as an ongoing part of a HIPAA compliance process.

Recommendations:

- *Apply content filters to identify messages with PHI*
- *Identify common sources and destinations of messages containing PHI*
 - *Use audit information to identify domains of high PHI volume*
 - *Identify likely and unlikely departments sending or receiving PHI e-mail*
 - *Pay special attention to e-mail from your Business Associates*
- *Involve your HIPAA privacy and security teams to establish administrative and auditing policies*

2. Recognize disclosure limitations

The HIPAA Privacy Rule requires that HCOs ensure the confidentiality of electronic PHI, and in addition, sets explicit conditions for disclosure of private health information. Privacy Rule compliance also requires that the HCO create a Privacy Officer function, and implement policy and standard procedures to ensure that its disclosures of PHI are appropriate. Because of this, the Privacy Rule essentially puts in place an operational structure that should be consulted in the administration of the HCO's messaging infrastructure. To the extent that disclosure policies can be automated and enforced, HIPAA compliance will be less costly and risky.

Disclosures of PHI are generally permitted to other healthcare covered entities for purposes of 'treatment, payment, and health operations' (TPO). Disclosures can be made to the organization's suppliers or contractors only after the execution of a 'business associate agreement' wherein the contractor agrees to limit its disclosure of PHI and to implement security protections equivalent to that of the HCO. Other disclosures can be made only as required by state law or as are specifically authorized by the subject of the PHI (i.e. the patient).

Under HIPAA, disclosure of PHI should generally only occur in the context of a formal process. For example, contractors can only receive PHI after the execution of the business associate agreement. Before any disclosure is permitted, the organization's Privacy Officer should have put in place an agreement that spells out security obligations and (potentially) security parameters. IT administrators should use such knowledge to configure the HCO's secure e-mail system to allow confidential messages to routinely pass to the domains of these pre-approved business associates.

In addition to business associates, disclosure is also allowed to domains of other HIPAA covered entities (CEs). Disclosure to other covered entities is more problematic because there are quite a lot of them. Identification of CEs to whom the HCO routinely discloses PHI is provided by the previous audit of email use.

In addition to the above disclosures, which occur in the context of a formal process, HCO's also need to provide support for ad hoc disclosures on an exception basis. For example, any disclosure is permissible when specifically requested by the subject of the disclosed information. But that permission is limited to records of a single patient and therefore not replicable. Similarly, records may be released when required by a court order.

In theory and practice then, the HCO should construct and maintain a "master address book" of domains to which transmission of PHI is appropriate. Furthermore, the source of information about these domains is contained within privacy related business processes that Federal regulation requires the HCO to implement.

Recommendations:

- *Construct and maintain a “master address book” of domains to which transmission of PHI is appropriate*
 - *Business associates with agreements in place*
 - *Other HIPAA covered entities*
 - *Provide a mechanism for ad hoc disclosure of PHI on an exception basis*
-

3. Leverage trading partner encryption capabilities

The healthcare community includes many different participants, and each has their own HIPAA compliance and secure communications requirements to support. In this environment, unilateral secure e-mail solutions that don't take into account the capabilities of and costs to your partners will risk slow adoption (or even rejection), and may reduce the business value of e-mail.

Although it may sometimes be trivialized, communications security involves a ‘negotiation’ between sender and recipient. Whatever encryption technology is used, at some point sender and receiver must agree on how to communicate with each other and exchange cryptographic material. It is important to recognize that, with few exceptions, trading partners and business associates (the likely targets of PHI disclosure) have their own security obligations under HIPAA. They have their own independent responsibility to protect the PHI that they transmit over electronic networks from unauthorized interception or modification, and as a practical matter, they often have an encryption solution in place.

Given the above, there are two basic approaches to the choice of encryption solutions:

1. **A ‘unilateral’ or non-cooperative approach** – with this strategy, the HCO will analyze and chooses an encryption solution based on internal costs. To the extent that this solution raises the costs of trading partner costs, it will experience slow adoption and resistance. Because a unilateral approach is currently typical, it is not surprising that a relatively small portion of the industry’s business communication is currently encrypted.
2. **An ‘agnostic’ or cooperative approach** – with this strategy, the HCO can put in place a set of standard encryption capabilities can be leveraged by different trading partners to support secure communications. At a low level, this is exactly what occurs when using SSL encryption. As part of the SSL handshake the client lists the encryption ciphers that it supports and the server chooses among those the one’s best meeting its requirements. The HCO should develop efficient support for a variety of encryption procedures such as SSL,

S/MIME, DOM-SEC, STARTTLS and the like, and then negotiate with trading partners the solution that works best for communication with them.

Historically, HCOs have not been very good at negotiating cooperative agreements. Health plans tend to dictate solutions to their providers, as do larger delivery systems to their affiliates and smaller business associates. Large vendor business associates and EDI clearinghouses similarly tend to be inflexible with respect to their customers.

HIPAA should make these negotiations easier. With respect to business associates, such negotiation must occur as a matter of Federal law; the business associate agreement must have provisions for implementation of adequate safeguards, which almost certainly should include some sort of transmission security. And HIPAA mandates that each covered party designate privacy and security officers who have direct responsibility to ensure transmission security. So with HIPAA, the HCO can easily determine specifically the points of contact with whom it must negotiate, and since all parties will have similar responsibility for the security of 'transactions'; there is a basis for equitable negotiation.

Sometimes disclosures of PHI are not related to ongoing 'transactions' but are 'one time' events. For example, the disclosure may be to an out-of-the-area provider of continuing care, or be the result of a patient's request or court order. With such disclosures, the benefits of implementing a reciprocally 'efficient' encryption methodology are minimal. In these cases, the HCO should probably consider a unilateral security solution for 'one-time' disclosure.

Also, the HCO can safely assume that some recipients will have little in the way of established encryption policy and procedure. Consumers typically deal with only one or a few providers and plans at any given time, so the consumer can easily adapt to the HCO's secure communications procedures, if only on 'an exception' basis.

Recommendations:

- *Be easy to do business with electronically*
 - *Considering only your administrative cost may be counterproductive if your e-mail security solution increases trading partners costs*
 - *Unilateral solutions may preclude your ability to use e-mail from incompatible security approaches*
 - *Implement a variety of security solutions:*
 - *S/MIME, PGP, STARTTLS, HTTPS*
- *Recognize that a number of healthcare trading partners will not have much encryption infrastructure*
 - *This is one of the main benefits of secure e-mail*

4. Don't overlook inbound messaging

Many of the secure e-mail products on the market today offer authentication and encryption capabilities for outbound e-mail. The value of such a solution is that it satisfies the compliance needs of the HCO by ensuring that outbound messages are properly authenticated and encrypted, and blocks communications that are not.

However, many of these products provide only limited support for secure receipt of inbound e-mail. In many cases, the only way to support inbound encryption and authentication of e-mail messages is via a reply to a previous outbound message.

This creates the problematic “teeter totter” situation in which each trading partner implements its own outbound secure e-mail solution. Note that in this unilateral approach, the number of secure communications solutions starts to proliferate, as each trading partner deploys its own proprietary solution. Support costs will also be very high under this approach, because of the need to exchange unique and/or proprietary decryption keys or authentication credentials with each trading partner.

While individual vendor products are all generally capable of supporting encryption, interoperability between products from different vendors has proved difficult to achieve. Note that this situation is starting to change as a number of secure e-mail products are being released that supports the STARTTLS protocol, that ensures confidentiality of messages as they are transmitted between trading partner domains. In addition, leading healthcare technology consortia like the Massachusetts Health Data Consortium and the Open Group are investing in projects like the S/MIME Gateway (SMG) project to drive interoperability of S/MIME gateway products. In the meantime, cooperation is the best solution.

Recommendations:

- *Be prepared to negotiate a mutually acceptable secure e-mail solution*
 - *Based on one of the security solutions you support:*
 - *S/MIME, PGP, STARTTLS, HTTPS*
 - *Select vendor solutions that support industry standards and interoperability*
-

5. Seek encryption transparency

Desktop encryption initiated by end user e-mail senders has been proven to be too complex and expensive for most organizations to support. HCOs should implement secure e-mail solutions that are transparent to end users, to minimize user mistakes and support costs, and to maximize end-user productivity.

It is a simple fact that it is costly to support the use of encryption by the typical end user. While the software capability may currently exist on the enterprise desktop (e.g. with Outlook, Netscape Messenger or other common mail applications), end users will not be able to properly configure those applications or manage encryption keys without extensive training. Message encryption is an order of magnitude more difficult than ordinary file encryption, as message keys must be securely communicated to recipients. Therefore, at some level, desktop encryption has end users performing critical, technical security functions.

Fortunately, there appears to be little requirement for the enterprise desktop to be the point of encryption. The single justification for assigning encryption / decryption responsibility to end-users is to ensure confidentiality of the exchange between the sender and recipient. However such confidentiality is not required by regulation, and may actually be contrary to the fulfillment of other HCO obligations. When PHI is disclosed, the HCO needs to ensure that the disclosure is appropriate and, in some circumstance, record aspects of that disclosure. Encryption at the desktop makes it impossible to satisfying these obligations, as the application of enterprise policy generally requires some inspection of the contents of the e-mail message.

Even more problematic is inbound PHI. Since the incoming PHI should probably be considered part of the HCO's 'system of record', it needs to be available to other members of the HCO workforce as well as its record keeping system. It is difficult to identify a workflow to ensure this availability when decryption depends upon action of the end user. Since the content of both inbound and outbound disclosures must generally be available to enterprise resources, there is little justification to perform disclosure related encryption tasks at the end user's desktop.

The preferred approach is encrypt / decrypt at the enterprise e-mail gateway. This ensures the availability of the message in unencrypted form for fulfillment of enterprise's TPO obligations as well as application of enterprise disclosure policy. Furthermore, this approach ensures that enterprise security personnel can directly manage protection of the enterprise's confidential cryptographic material and thereby provide greater security at lower cost.

Recommendations:

- *Don't do e-mail encryption at the desktop – make the process transparent to end-users*
- *Do e-mail encryption and disclosure policy enforcement at the e-mail gateway*
 - *This approach is less error-prone, less support-intensive, and more productive for end-users*
- *Look for vendor solutions that can provide transparency for both outbound and inbound secure e-mail*

6. Use structured messaging with patients/members

Messages sent to and received from patients or health plan members require special handling - the HCO has significant obligations to respond in an appropriate way to information submitted by the consumer. Many HCOs are turning to Web-based patient and member portals to provide a secure mechanism for consumer communications that can be integrated into business processes to reduce errors and ensure that appropriate action is taken.

In general, patient and member email should be included in the patient record to the extent it contains relevant information such as complaints, reports on reactions to a drug, and so forth. To the extent that the HCO does not respond appropriately to the patients query or complaint, there is potential for increased liability. And although consumers cannot be expected to direct their message to appropriate HCO staff members, once messages have been received, the HCO is obligated to respond appropriately.

The significant issue with respect to consumer email then is one of workflow. The HCO must ensure that information in the consumer's email is processed appropriately. Reliance on human actors to correctly and consistently route and process e-mail messages from patients is, at best, a costly proposition. For example, a human recipient of the patient's email must recognize the need to include it in the patient record, copy relevant portions, and forward it to a medical records department for inclusion in a patient record system. These tasks take time and training, and where the recipient is a physician, successful completion of this kind of task will be neither timely nor reliable.

Allowing patients to submit email only through submission of a web form on a patient / member portal at the HCO's Internet site has several advantage:

- message purpose can be classified and categorized based on Web form selections
- message content can be easily parsed from the Web form
- messages can be routed to appropriate HCO staff or systems based on this content
- message copies can be routed and saved in the patient record system
- messages can be tracked, audited, and billed for
- patient/member expectations can be set in terms of response policies and response times

In addition to the above, a structured email approach has the additional advantage of allowing the HCO to manage the subject of patient email, and to not accept messages for which no workflow has been created.

Recommendations:

- *Automate the acceptance of patient/member e-mail messages through a Web portal*
- *Ensure that workflow/business processes exist for all patient e-mail that is to be accepted*
- *Restrict acceptance of e-mail messages for which no workflow exists*
- *Use message content to trigger policy-based message routing*

7. Develop appropriate patient/member account provisioning

Many of today's secure delivery solutions available for communications with consumers provide some type of Web-based account for message retrieval, and require the user to authenticate via a username and password. These consumer accounts should not be provisioned with authentication credentials using standard e-mail, because of the lack of security. In addition, because of the unilateral nature of these accounts, using them with trading partners may lead to maintainability problems.

One of the more popular secure message delivery mechanisms for consumer recipients is to redirect outbound e-mail messages to a secure Web-based delivery service. This "staging server" solution uses a Web link embedded in an e-mail notification to bring the recipient back to a secure server to read the message using his or her Web browser over HTTPS. This approach allows recipients to receive, read, reply to, and locally save secure messages without any additional software plug-in or client-side software to install beyond their normal e-mail client and browser. Clearly, this approach provides no confidentiality assurance unless the recipient is properly authenticated prior to downloading the message.

The HCO must create and distribute authentication credentials such as usernames and passwords to recipients of the PHI. But the manner of credential distribution is a significant concern. Clearly, email distribution is not appropriate, as the Internet email system itself does not ensure confidentiality. If the authentication credentials were distributed via plaintext email, then the confidential PHI could just as well be distributed via plaintext email. To ensure the security of e-mail messages, it is important that these authentication credentials be delivered via a 'secure' channel. Most likely the credentials need to be either sent via U.S. mail, or transmitted directly to the recipient via voice communication.

From a security perspective, this 'redirect to HTTP' approach has different vulnerabilities than conventional email, which places additional obligations on the HCO disclosing the PHI. Since web messages can be downloaded from any location, all that is required to access messages is Internet connectivity, a browser and the recipient's authentication

credential. Such 'ubiquity' increases vulnerability to unauthorized or inappropriate disclosure of PHI. For example, consider the case where the recipient has left employment with the trading partner after the HCO issued the recipient an account and password. The recipient should not be allowed to access secure e-mail - but how does the HCO know about the change in the recipient's workforce status? Without engaging trading partners to ensure the recipient's current status, HCOs should be very cautious in the use of web redirect methods for business to business transactions. Of particular concern, should be their use for the distribution regularly occurring reports or for distributions of PHI to lists.

Recommendations:

- *Accounts should not be provisioned through e-mail*
- *Security of Web mail approaches depend on the assignment and maintenance of end-user credentials, and so should not generally be used with trading partners*
- *Patient/member credentials should be delivered in person, via phone, or via U.S. mail to the consumer's "address of record"*

8. Automate exception handling

PHI disclosures to unfamiliar domains may not be supported by prior authorization and secure communications agreements. In such cases, some HCOs may opt to "hold" the message for review by an administrator, but this is the worst thing to do. Instead, the HCO should analyze scenarios under which messages need to be delayed, and develop workflows to overcome the difficulty.

Given the complexity of the HCO business relationships and large user communities, it is likely that a significant portion of the HCO's PHI disclosures will not be handled by a simple set of business rules. For example, initial disclosures of PHI to new or unfamiliar domains may not have 'prior authorization'. Such messages should most likely be held for further action by HIPAA administrators, Privacy Officers or message originators.

Perhaps the worst possible action to take in circumstances where message delivery is delayed, is to hold or quarantine the message for further unspecified action by an IT administrator. Non-delivery of e-mail messages interferes with the business processes and (possibly) patient treatment of both sender and receiver. Without timely resolution of the message delivery problem, senders will likely seek an alternative way to get messages through. The value of the messaging system is thereby diminished, while the use of alternative channels may bypass the security controls that the HCO seeks to rely upon.

Ideally, the HCO would analyze scenarios under which messages are delayed, and develop the workflow to overcome the difficulty. Such workflow could be at least partially implemented by automating messages to relevant participants in the email exchange, including senders and recipients, Privacy and Security Officers, and other administrators. At a minimum, senders need feedback regarding the delay in message delivery. Also, senders should be informed of actions that they may take to facilitate delivery, because they may be able to provide information that would speed up the authorization and negotiation of security parameters.

Recommendations:

- *Organizations should expect messages to violate security parameters – for example:*
 - *PHI e-mail sent to external recipients without an encryption key*
 - *PHI sent to unfamiliar domains where patient authorization may be required*
- *Implement business rules to determine appropriate course of action - for example:*
 - *logging / quarantine for Privacy Officer review*
 - *automate request for encryption keys*
- *Establish conditions where PHI e-mail merits expedited delivery*

9. Establish a continuous improvement process

The value of email derives, in part, from enabling end users to create and send messages to whomever they desire without involving the IT organization. The disclosure and security requirements imposed by the HIPAA rules, however, restrict this ‘anything goes’ mentality. The challenge of messaging security, then, is to ensure appropriate disclosure of PHI while minimizing the disruption to e-mail-based business processes. To meet this challenge, security personnel should seek feedback on the potential business disruption created as end users encounter the limitations imposed by the secure e-mail solution. Meaningful security logs will indicate what confidential messages were delivered in non-routine fashion, and security personnel can follow-up with senders of such messages to better understand the business consequence of such delays. Such feedback will be useful in improving the design of the security controls and supporting business process.

Almost certainly, the optimal set of security controls and supporting business processes will take time to develop. Without stronger regulatory requirements and common industry infrastructure and interoperability, the security of the HCO’s messaging systems will depend upon the slow evolution and learning of recipients. The learning is slow because the community to which the HCO discloses PHI is dynamic and because the HCO learns of the changing requirements of trading partners after the fact. Implementers should accept this circumstance as the nature of things, and implement a security system that can easily be updated

Recommendations:

- *Enterprise value derives from end user enablement - e-mail is simple, universal, and quick*
 - *this must be balanced by restrictions placed through security controls*
 - *not all messages will or should be permitted*
- *Challenge to balance security with business needs*
 - *policies predicated on the presence of PHI content will only be heuristic*
 - *need to guard against being overly restrictive*
- *Establish and manage periodic audit, policy review & revision, TP negotiation, and security controls administration*

10. Secure the infrastructure

As e-mail has become more and more of a mission-critical resource for healthcare organizations, there has been an increasing need to protect and secure e-mail applications and infrastructure. External threats include:

Spam – at Memorial Medical Center in Las Cruces, New Mexico, over 60% of inbound e-mail was spam, causing significant problems in terms of network utilization and bandwidth. While words like “Viagra” and “penis” seem like obvious triggers for spam filters, it's not so simple in the healthcare industry where communications about pharmaceuticals and anatomy are critical to the business. These e-mail filtering challenges highlight the balancing act that IT professionals in the healthcare industry must perform as they attempt to deal with the onslaught of spam. They have to thwart the tremendous amount of annoying—and often offensive—junk e-mail that's infiltrating their companies and simultaneously ensure that critical business information gets through.¹

Viruses and worms – Yorkhill Hospital in Glasgow was hit by a computer virus that made medical records unusable for over 16 hours, forcing the staff to resort to paper records. But even more of a threat to patient privacy are worms like Sobig, that send out e-mail from infected systems. It's quite conceivable that future worms and viruses could randomly attach files from the infected system to outbound emails, disclosing PHI.²

Hackers – A 25-year-old Dutch hacker downloaded medical records, health information, and social security numbers of more than 5,000 patients at the University of Washington Medical Center. The hacker claimed to be motivated by a desire to expose the vulnerability of electronic medical records.³

¹ Kym Gilhooly, “Spam Battle Plans”, *Computerworld*, July 28, 2003.

² “Virus hits hospital systems”, *BBC News*, August 22, 2003

³ R. O'Harrow, “Hacker Accesses Patients Records,” *The Washington Post*, December 9, 2000, p. E1

Unquestionably, the messaging systems of HCOs will be subject to external attack from Internet sources, and every HCO has learned painful lessons about the need to protect against email borne virus and spam.

However, it is important to further recognize the vulnerability of e-mail and other messaging related services themselves. Since these services open ports to the Internet, weaknesses in software or security administration can introduce points of vulnerability to the organization's perimeter defense. It is important that security staff apply rigor to hardening servers and services, and use good security practice in their administration in order to minimize their exposure and risk.

At this level, protection of e-mail and messaging infrastructure has a 'Security 101' character to it: "Harden the servers and their underlying OS by disabling or eliminating unneeded services ... apply relevant vendor security patches" ... and so forth. These steps should be applied across the e-mail infrastructure, including SMTP relays, POP servers, DNS and routers, as well as underlying server operating systems.

Beyond configuration changes, it is also important that good security practice be utilized in the administration of these systems. Individual administrators should be given the least privilege needed to perform their functions, role separation should be employed to the extent possible in order to separate configuration, ongoing user administration and audit functions. Default administrator accounts should be renamed and good password discipline applied.

Excellent guidance for the securing of networks and systems is provided by the NIST Special Publication series. Of particular interest is SP 800-45, "NIST Guidelines on Electronic Mail Security" (<http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf>)

Recommendations:

- *Minimize e-mail risks by appropriate configuration, hardening, and administration of e-mail infrastructure.*
- *Keep patches current on SMTP relays, POP and DNS servers, routers, and underlying operating systems.*
- *Establish good security practice through privilege minimization and role separation.*
- *Deploy perimeter security to protect users and networks from threats such as spam, viruses and worms*

About Tunitas Group

Tunitas Group is an health and technology consulting firm that specializes in the application of information technology to improve healthcare operations. By ensuring our client understand the benefits and business justification for technology improvement projects, we deliver positive ROI projects. Tunitas Group consulting services are used by leading health care organizations and their significant business partners.

For more information, please call 209-754-9130.

Tunitas Group
PO Box 278
Sierra Vista Lookout
Mt. Ranch, CA 95246
www.tunitas.com