Global Information Assurance Certification Paper

E-mail Communication with Patients in the Wake of the HIPAA Final Security Rule

Dennis A. Schmidt
GSEC Version 1.4b
April 4, 2003

Abstract

Over the last decade, the popularity of e-mail communication between doctors and patients has risen steadily. The asynchronous nature of e-mail provides convenience and more effective use of time for both parties. Patients can now make appointments or get prescriptions renewed without spending idle time waiting in lines at the doctor's office or on the phone. Physicians and their staffs can provide lab results or patient follow up more efficiently. E-mail also provides an electronic "paper trail" of such transactions that can be maintained in the patient's medical record.

The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, introduced sweeping rules governing the privacy and security of all forms of patient information. On February 20, 2003, the Department of Health and Human Services (HHS), responsible for the implementation of HIPAA, released the HIPAA Final Security Rule which focuses on the protection and privacy of electronic patient information. The Final Security Rule places broad restrictions on how electronic data containing patient information, including e-mail, is stored and transmitted. The final rule could have a profound effect on doctor/patient e-mail communications. This paper will explore the issues that the HIPAA regulations raise with doctor/patient e-mail communications and will discuss some possible solutions.

Background

The popularity of e-mail as a means of communication has been growing exponentially in the last ten years. People of all ages and social and economic backgrounds have discovered the speed and convenience of sending e-mail to friends and family. A natural progression of this new communications revolution is a rising desire for patients to communicate with their doctors via e-mail.

Physicians are not as enthusiastic about communicating with patients, but they are gradually changing their minds. Dr. Daniel Z. Sands, a leading proponent of patient/physician e-mail communication, writes that while almost 50% of the general population communicates with e-mail, a survey in 1999 reported that only 3% of physicians admit that they routinely trade e-mail messages with their patients. Doctors have several concerns about e-mail, including reimbursement for time, legal liability, security and the risk of patients improperly using e-mail during medical emergencies. [22]

In spite of those concerns, doctors appear to be increasing their use of e-mail. It was recently reported that in 2003, 15% of physicians now use e-mail in their practice. "It is becoming more difficult for clinical practitioners to avoid adopting a communications tool preferred by so many of their patients." [6, p. 3] The most common tasks that patients prefer to accomplish via e-mail include asking basic questions that do not require a visit, scheduling appointments, refilling prescriptions, and getting lab results.

Early guidelines from the American Medical Association (AMA) on patient e-mail seemed to focus more on ethical and business concerns than on electronic security of the information. Doctors were advised to warn the patients that e-mail should only be used for non-emergency situations. Doctors were also concerned that time spent dealing with e-mail was difficult to bill. Security of patient e-mail focused more on errors in delivery (wrong address in the To line) than on protection of the information. Encryption of e-mail was only addressed for wireless networks. [2]

More recent guidelines from the AMA still focus more on ethical and administrative concern, but have also added guidance on informing patients of the insecurities of unencrypted e-mail transmissions. Still, little additional guidance is given toward encryption and electronic security. [3]

HIPAA Essentials

Just as doctor/patient e-mail communication is starting to pick up steam, restrictions introduced by the Health Insurance Portability and Accountability Act (HIPAA) could have a chilling effect on it. HIPAA, as originally passed by Congress in 1996, was designed to ensure that workers could maintain health insurance coverage while transitioning between jobs. However, HIPAA has been expanded into a much larger set of regulations covering the privacy and protection of individually identifiable health information also known as Protected Health Information or PHI.

HIPAA consists of three major parts: the Codes and Transaction Sets Final Rule; the HIPAA Final Privacy Rule; and the HIPAA Final Security Rule.

Before discussing the content of the HIPAA rules, it is necessary to briefly discuss the rules development process. The developmental flow for each rule is independent from the development flow of other rules. The process for each rule begins with the release of a "proposed rule" where HHS describes what they intend to do. Following the release by HHS, interested parties are given a comment period to voice concerns (or support) for any part of the proposed rule. HHS then develops the final rule. When a final rule is released, it contains two sections: a preamble, which provides commentary and rationale for the development of some provisions and the actual rules. The final rule becomes effective or enforceable two years and 60 days from its release date.

The Codes and Transaction Sets Final Rule was released in August, 2000 and becomes effective in October, 2003 for most covered entities after a one year extension granted by Congress. It governs the standardization of codes used in communications between healthcare providers and insurance companies and does not have a direct effect on e-mail communication.

The HIPAA Final Privacy Rule was released in December, 2000 and becomes effective on April 14, 2003. It deals primarily with safeguarding the privacy of patient information in all forms, with a focus on forms other than electronic. However, section 164.530 of the Privacy Rule contains a sentence (affectionately known as the "mini-security rule" [17]) that provides vague guidance for protecting electronic health information: "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information". [15, p. 82827]

The mini-security rule generated significant consternation and confusion among healthcare institutions. It was apparently written with the anticipation that the Final Security Rule would be released soon after the release of the Privacy Rule. A coinciding Security Rule would have eliminated the ambiguity of the mini-security rule. Instead, the Final Security Rule was delayed repeatedly and was not released for over two years. It was published less than two months prior to the effective date of the Privacy Rule.

Hence, healthcare institutions were unclear as to what planning they needed to do to satisfy the vague requirements of the mini-security rule. Should they be forming plans based on the proposed Security Rule? Or, should they delay making plans until the Final Security Rule was released? If IT planners tried to start planning early, they could needlessly waste valuable resources if the Final Security Rule turned out to be significantly different from the proposed rule. An item that was a major concern was a provision of the proposed Security Rule which required encryption of all health information "transmitted over the internet (wide-open)". [14, p. 43245] This provision, combined with the requirements of the mini-security rule, could have put a complete stop to unencrypted e-mail communication with patients on April 14, 2003. Since many organizations were not able to implement enterprise-wide encrypted e-mail systems in time to meet the deadline, some were preparing to prohibit all e-mail communication with patients beginning on April 14th.

The HIPAA Final Security Rule was released on February 20, 2003 after many lengthy delays. It has an effective date of April 21, 2005. During the long months that healthcare organizations were anxiously waiting for its release, HHS made repeated assurances that the final rule would look very much like the proposed rule. As it turned out, the final rule is significantly different from the proposed rule. The most significant change was that encryption of transmitted PHI was now listed as an "addressable" item.

Addressability was a new concept not seen in the proposed rule. When a standard "includes addressable implementation specifications, a covered entity must assess whether each implementation specification is a reasonable and appropriate safeguard in its environment". [13, p. 8377] If the covered entity determines that the specification is not reasonable and appropriate, it must document the reasons and implement an appropriate alternative.

So, what does all of that mean? Basically, since encryption of transmitted PHI is now addressable, covered entities should encrypt if possible, but, if encryption is not feasible, they now have alternatives. This is a significant change from the proposed rule which said that covered entities must encrypt – no options allowed. According to the preamble of the Final Security Rule, HHS made encryption addressable because they realized that there is no universal solution to the encryption of e-mail and they did not want to have a chilling effect on doctor to patient communication or doctor to doctor communication about a patient.

Why is Encryption of E-mail Such an Issue?

There are many products and solutions available for encrypting e-mail messages, most of which would individually be more than sufficient for protecting patient information. However, most of these solutions do not interoperate with each other well and are too difficult for many users to grasp. In a healthcare environment, doctors can expect to have contact with the full spectrum of ages, technical skills, ethnic groups, intelligence levels, and financial backgrounds. A doctor might get e-mail from a teenager who has worked with computers his whole life or from an 85 year old grandmother who has just learned how to use e-mail. The teenager may not have a problem understanding public and private key concepts including key generation and key exchanges. Expecting the 85 year old grandmother to do the same may be a bit unreasonable. To be accepted by the general patient population, any encryption solution for e-mail must be simple to use and as transparent to the user as possible. The need for strong technical skills to send encrypted e-mail is a significant barrier for adoption. Following is a summary of available encryption models.

PGP and PKI

"PGP (Pretty Good Privacy) is a popular program used to encrypt and decrypt e-mail over the Internet". [4] It uses the RSA (Rivest-Shamir-Adleman) algorithm which is the same security paradigm used in Netscape and Microsoft secure web browsers and a variety of other well know secure interfaces. PGP provides end-to-end security. The entire message is encrypted before transmission and decrypted by the receiver. If the message is intercepted by an unauthorized party, it is virtually impossible to decrypt without the proper keys. PGP is available in both a commercial version (currently marketed by Network Associates) and a free open source version. The open source version can be

used freely by anybody, except for commercial enterprises. The major problem with PGP is ease of use. Using PGP within an enterprise, public and private keys are exchanged through a public key infrastructure (PKI). PKI requires both the sender and receiver to know how to generate and exchange public and private keys. PGP is very popular with "techies", but doctors and the 85 year old grandmother described earlier may find PGP to be overwhelming. In its current form, it would not be an acceptable solution for encrypted Patient to Doctor e-mail communication.

Encrypted Attachments

Another possible solution for encrypted e-mail involves encrypting the desired information on the sender's machine into a single file and then sending it as a standard e-mail attachment. The intended receiver can decrypt the message on any machine that has a secure browser installed. He simply needs to have a password to decrypt it. Several commercial products are available that provide variations of this technology. Postx (www.postx.com) and Pkware (www.pkzip.com) both offers products that fit into this category. The advantages of using encrypted attachments include:

- No special client or additional software is needed by the recipient.
- The recipient only needs a password to decrypt the message.
- Any type of file can be encrypted – text, graphics, spreadsheets, etc.
- Relatively inexpensive, less than $50 per client.

Unfortunately, there are some significant disadvantages to this technology when used for doctor to patient communications:

- The technology is essentially one-way. A doctor could send an encrypted message to a patient, but the patient cannot easily answer with an encrypted message. To do so, the patient would have to purchase the encryption software and install it on his machine. Postx has some limited "answering" capability, but the patient would still not be able to initiate an encrypted message without installing the software.
- Administering passwords presents a management challenge. Doctors and patients would have to have some prearranged password scheme. Requiring a doctor to remember different passwords for hundreds of patients is impractical. Basing passwords on a unique user property such as Social Security Number or medical record number would be easier to manage, but less secure, since passwords could be figured out.
- The encrypted attachment is more vulnerable to brute force hacking algorithms. If an attacker can capture a copy of the attachment, he can crack the password if given enough time.

The encrypted attachment technology seems suitable for specific small scale applications, but would not work well in an enterprise sized patient communications system.

Web Based Encryption

Web based encryption systems have grown in popularity recently. There are a variety of products on the market that provide web-based encryption solutions. Among others, some of these are: Tumbleweed (www.tumbleweed.com), CertifiedMail (www.certifiedmail.com), and Authentica (www.authentica.com). The basic operation of all of these is relatively simple. E-mail containing sensitive information is never sent directly to the recipient. Instead, the sensitive message is sent to and stored on a secure server through a secure web connection. An unencrypted "you've got mail" message is then sent to the recipient with a link to the message on the secure server. The recipient clicks on the link and reads his message through a secure web connection. The message is never actually delivered to the recipient; it is only viewed through a secure web browser. There are several significant advantages to a web based encryption system. These include:

- No special client is required; only a secure browser is necessary.
- Message delivery is encrypted end to end.
- Customizable lexicon or "dirty word" search capability which scans outgoing mail for words or phrases that could be related to PHI.
- Scalable. Will work in large enterprises.
- Hooks available to allow an electronic copy of messages to be automatically put in the patient's medical record.
- Some versions also have other desirable features including encrypted attachment capability and built-in virus and spam filtering.

There are also some disadvantages to a web based encryption system. These include:

- Expensive to buy and to maintain. Since most of these systems are designed for large scale environments, the basic software costs can be rather large. The systems typically require additional robust secure servers to support them as well as the technical staff needed to administer the servers.
- Password management is an issue. In a basic system, it is possible to send an unencrypted message to the recipient that contains a link that points to the secure message. However, if an unauthorized user gains access to the unencrypted message, he has also obtained the keys to the secure message. To prevent this, the central system would need to provide some sort of authentication system. That would require additional resources to manage user accounts for a pool of thousands of patients who "may" access the system. Several of the commercial systems

provide an automated registration system which could offload much of the administrative overhead.
- Message management and archival is an issue. Healthcare providers must determine how long they want to retain messages on the system before they are deleted. They must also decide what type of backup and retention policies are necessary for their business needs.

Of all the encryption options reviewed so far, the web based encryption system seems to be the best suited for an enterprise hospital environment. An informal review of hospital systems shows that many hospitals are either incorporating commercial off the shelf systems or building their own internal systems.

Do We Really Have to Encrypt?

Now that we have examined various encryption techniques and solutions, we will explore one other possibility which raises the question: To be HIPAA compliant, do we really have to encrypt e-mail messages containing PHI? The simple answer is: Not necessarily. Remember, the Final Security Rule leaves encryption as an addressable item. Covered entities should encrypt where practical, but, if encryption is not practical, entities must use an alternative method to protect health information.

Throughout the HIPAA rules, the themes of reasonableness, due diligence, and practicality are repeated over and over again. The drafters of the HIPAA rules did not intend for the rules to unduly impede healthcare operations nor did they intend for healthcare providers to go broke implementing HIPAA compliant systems. The preamble to the Final Security Rule contains some extensive discussion about encryption of transmitted health information:

> We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. [. . .] It became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet. As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption. [. . .] We include as an addressable implementation specification the requirement that transmissions be

encrypted when appropriate based on the entity's risk analysis. [13, p. 8357]

Interpreting this discussion, healthcare organizations are given the flexibility to analyze the risk of transmitting health information in an unencrypted form. If the risk is acceptable, then they might elect to accept that risk. When doing a risk analysis, organizations should consider the following points:

- It is accepted knowledge in security circles that the transmission of data over a network is the least vulnerable portion of the e-mail process. If a hacker wishes to capture sensitive information in e-mail, he is more likely to go after the servers at either end of the transmission where the data is stored than to try catching it during a network transmission.
- Implementing a web based encryption system can be very expensive, likely exceeding $100K. In times of tight budgets, this money might be better spent on server security than on encryption tools.
- The risks involved with transmitting patient information should be fully examined. The risk that the patient might sue an organization if his health information is accidentally disclosed could be reduced if the organization gets the patient to share some of that risk by authorizing the unencrypted transmission of their patient information.

The bottom line is that, although the Final Security Rule encourages organizations to encrypt transmissions wherever practical, it also allows them to transmit unencrypted heath information if they are willing to assume the risks involved.

Other Needs for Transmitting Health Information

This paper has focused primarily on doctor to patient e-mail communication. However, there are other models for electronic communication of PHI that will be affected by HIPAA. Below is a brief review of some of them.

Doctor to Doctor Communication. It is frequently necessary for doctors to communicate with other doctors about a patient. If the doctors are from the same institution, they are more likely to be communicating on the same internal protected network and unencrypted PHI may not be a major concern. If the doctors are from different organizations, then they are more likely to be communicating over external networks. In this case, the risks of transmitting unencrypted PHI are similar to those in the doctor to patient communication model, except that, when two doctors are communicating, it is less practical for them to get the patient's permission in advance to send his data over an unencrypted line.

Healthcare Provider to Healthcare Payer Communication. This model involves communications between hospitals and insurance companies. These

communications will most likely be filled with PHI. This model has encryption issues similar to the Doctor to Doctor Communication model except that *all* communications are likely to be over external lines and the volume of traffic is likely to be much greater. The risks and vulnerabilities involved with this process might mandate that a dedicated hardware encryption line be installed between the two organizations

Public to Patient Communication. This model is a bit unusual. An internet search on the term "patient e-mail" yields dozens of links to hospitals that provide a service where the general public can send e-mail messages to inpatients. The messages are sent to a common e-mail address and the hospital then delivers them to the patient. Since the persons sending this type of message are generally not healthcare providers, they are not covered by HIPAA rules. However, a message from a friend saying: "*Hi John. Hope the gall bladder surgery went well.*" certainly contains PHI. In this case, the person initiating the message is not required by HIPAA to encrypt or protect it. However, once the healthcare facility receives the message, it is then obligated to protect the privacy and security of the message under HIPAA rules.

Conclusions

As we have seen, e-mail communications between doctors and patients is only going to continue to increase over time. Patients definitely want it and doctors are gradually coming on board. The recent introduction of federal HIPAA regulations mandates that healthcare providers take additional steps to ensure the protection and privacy of electronic Protected Health Information. Fortunately, the final HIPAA Security Rule allows some flexibility on how healthcare providers may provide those protections. The ultimate implementation chosen by each healthcare provider will be driven by the business needs and resources available to that particular institution.

References

[1] American Health Lawyers Association. "Preliminary Comments on the Final HIPAA Security Rule: The Curtain Rises on the Next Act". 20 Feb. 2003. URL: http://www.healthlawyers.org/ofnotes/ofnote_hipaa_030220.cfm (30 Mar. 2003)

[2] American Medical Association. "H-478.997 Guidelines for Patient-Physician Electronic Mail". URL: http://www.ama-assn.org/apps/pf_online/pf_online?f_n=browse&doc=policyfiles/HOD/H-478.997.HTM (30 Mar. 2003)

[3] American Medical Association. "Guidelines for Physician-Patient Electronic Communications". URL: http://www.ama-assn.org/ama/pub/category/2386.html (30 Mar. 2003)

[4] AT&T PKI Center Glossary. URL: http://www.aces.att.com/glossary/pgp.htm (2 Apr. 2003)

[5] Best, Jason. "New Guidelines Remove Risk From Doctor-Patient E-mail". 4 Dec. 2002. URL: http://www.medem.com/corporate/xl_corporate_medeminthenews_detail.cfm?ExtranetPressNewsKey=135 (30 Mar. 2003)

[6] Braithwaite, William, et al. "Email and the Clinical Practice". Feb. 2003. URL: http://www.healthyemail.org/docs/PhysicianEmailGuide.pdf (30 Mar. 2003)

[7] Brewin, Bob. "New HIPAA security rules could open door to litigation". Computer World. 20 Feb. 2003. URL: http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,78684,00.html?nas=PM-78684 (30 Mar. 2003)

[8] Brewin, Bob. "HIPAA Data Rules Leave Choices to IT". Computer World. 24 Feb. 2003. URL: http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,78740,00.html?SKC=policy-78740 (30 Mar. 2003)

[9] Cowert, Richard G. "Digital Disconnect: The Need for Patient E-mail Consent Forms". Dec. 2001. URL: http://www.bakerdonelson.com/healthlaw/dickCowartNov2001.cfm (30 Mar. 2003)

[10] Gavin, Kara. "First large doctor-patient e-mail study finds positive attitudes on both sides". 4 May 2002. URL: http://www.eurekalert.org/pub_releases/2002-05/uomh-fld042902.php (30 Mar. 2003)

[11] Grove, Tom. "Summary Analysis: The Final HIPAA Security Rule". HIPAAdvisory. Feb. 2003. URL: http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm (30 Mar. 2003)

[12] "Guidelines for E-mail Communication with Patients". Safe Practice. Vol. 8 No. 2. May 2002. URL: http://www.medem.com/corporate/scpie.pdf (30 Mar. 2003)

[13] Health and Human Services, Dept. of. "Health Insurance Reform: Security Standards; Final Rule." Federal Register. Vol. 68, No. 34. 20 Feb. 2003. URL: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf (30 Mar. 2003)

[14] Health and Human Services, Dept. of. “Security and Electronic Signature Standards; Proposed Rule.” Federal Register. Vol. 63, No. 155. 12 Aug. 1998. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1998_register&docid=98-21601-filed.pdf (30 Mar. 2003)

[15] Health and Human Services, Dept. of. “Standards for the Privacy of Individually Identifiable Health Information; Final Rule” Federal Register. Vol. 65, No. 250. 28 Dec. 2000. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2000_register&docid=page+82461-82510.pdf (31 Mar. 2003)

[16] Lewers, Ted D. “Guidelines for Patient-Physician Electronic Mail”. URL: http://www.ama-assn.org/meetings/public/annual00/reports/bot/bot2a00.rtf (30 Mar. 2003)

[17] Marks, Richard D., et al. “DWT Releases Analysis & Comments On HHS’s Just-Released HIPAA Security Rules”. Feb 2003. URL: http://www.dwt.com/practc/hc_ecom/bulletins/02-03_HIPAASecRules.htm (30 Mar. 2003)

[18] Murphy, Gretchen. “Patient-centered E-mail: Developing the Right Policies”. Journal of AHIMA. URL: http://134.174.100.34/AHIMA/JAHIMA_Murphy.htm (30 Mar. 2003)

[19] Roberts, Paul. “Government publishes final HIPAA security standards”. Bio-IT World News. 21 Feb. 2003. URL: http://www.bio-itworld.com/news/022103_report2045.html (30 Mar. 2003)

[20] Sands, Daniel Z. “Electronic Patient-Centered Communication: Managing Risks, Managing Opportunities, Managing Care ”. American Journal of Managed Care. URL: http://www.ajmc.com/sands_editorial.html (30 Mar. 2003)

[21] Sands, Daniel Z. “Guidelines for the Use of Patient-Centered E-Mail”. URL: http://www.mahealthdata.org/mhdc/mhdc2.nsf/e214ac63ff65c87e852564580073a9fd/4a7c6d3989621597852567590006a1113?OpenDocument (30 Mar. 2003)

[22] Sands, Daniel Z. “How to Communicate with Your Doctor Using Email”. URL: http://www.healthology.com/focus_article.asp?f=healthcare&c=healthcare_emaildoctor (30 Mar. 2003)