HIPAA's Role in E-Mail Communications Between Doctors and Patients: Privacy, Security, and Implications of the Bill

James H. Stephens and Anthony V. Parrillo

Abstract

The confidentiality of a patient's information has been sacred since the days of Hippocrates, the Father of Medicine. Today, however, merely taking an oath to respect a patient's privacy has been overshadowed by regulations governing how certain healthcare establishments handle an individual's health information on the web. Consequently, if a healthcare organization employs electronic mail as a means of communicating medical and/or health data to consumers, providers, and other appropriate parties, it must ensure such information is safeguarded, since using the Web poses concerns about the privacy and security of an individual's information. E-mail between patients and physicians (or other health care providers) must be secured under the privacy rule of the Health Insurance Portability and Accountability Act; when transfer of protected health information (PHI) occurs, even if private, such a communication falls under HIPAA's guidelines. In today's electronic age, it is increasingly likely that protected health care information will be subject to fraud. HIPAA addresses the privacy and security of health care information in its Privacy and Security Rules, which enforce standards applied to PHI. This paper will focus on HIPAA's role in e-mail communications in health settings, particularly as it relates to the privacy of the information exchanged between doctor and patient.

Introduction

Successful communication between patients and their doctors has, for decades, been established as playing a key role in the provision of quality health care (Bertakis, 1977), contributing to greater patient involvement during office visits, improved compliance with therapeutic recommendations and clinical outcomes, and high rates of patient and physician satisfaction (Rao, Anderson, Inui, & Frankel, 2007). It has become clear that successful patient-physician communication is not limited to face-to-face contact; three-in-four ambulatory medical contacts are made by telephone (Ries, 1987), and the vast majority of medical problem-related telephone calls can be adequately managed on the telephone – without a physician having the need to see his/her patient (Curtis, 1988).

Use of the Internet has increased dramatically, and many individuals use electronic mail (e-mail) to communicate with their family and friends about health issues (Baker, Wagner, Singer, & Bundorf, 2003; Liederman & Morefield, 2003; Pal, 1999). A sizeable percentage of patients – 85% in one study – indicated that e-mail is a good way to communicate with physicians (Neill, Mainous, Clark, & Hagan, 1994) and 9 in 10 wish they had the ability to do so (Harris Interactive, 2002). In reality, however, very few patients acknowledge that they actually have communicated with their physicians electronically. In a study by Sittig, King, and Hazlehurst (2001), only 6% of patients had ever sent an e-mail message to their physician/provider; similarly, Moyer, Stern, Dobias, Cox, and Katz (2002) reported only 10.5% of e-mail users had ever done so. And while greater than 90% of physicians are using computers for personal/professional reasons, as few as 7% admit exchanging e-mail with their patients (Lacher, Nelson, Bylsma, & Spena, 2000); only ~30% of pediatric doctors have been known to use patient-physician e-mail (PPEM) (Rosen & Kwoh, 2007).

Such studies suggest that e-mail has the potential to improve the quality of health care, encourage patient-physician communication, and enhance professional relationships among physicians. Despite this promise, e-mail communication is underused in the medical setting due to important legal and ethical questions (DeVille & Fitzpatrick, 2000). At the heart of this matter is the issue is the privacy of a patient's medical records. Privacy and security concerns increase reluctance, among physicians and patients alike, to communicate via e-mail (Ellis, Klock, Mingay & Roizen, 1999; Moyer et al., 2002; Sittig, King, & Hazlehurst, 2001). Non-secure messages (i.e., those that are unencrypted) may be intercepted and read by unauthorized individuals, e-mail may be left open on the screen of a computer, allowing unauthorized individuals to see them, and computer terminals may be shared at work or at home, minimizing privacy (Freed, 2003). As a result, creating an e-environment that is secure and reliable has become a mission-critical element of each and every practice in the healthcare industry, from those providing patient care to those who oversee the daily management of business operations (Kowalczyk, 2004).

Enter the Health Insurance Portability and Accountability Act (HIPAA) of 1996 – P.L. 104-191 (U.S. Congress, 1996). Originally sponsored by Senators Edward Kennedy and Nancy Kassebaum, HIPAA was passed to protect health insurance coverage for workers and their families when they change or lose their jobs. At the same time, Congress saw the need to address growing public concern

* James H. Stephens, DHA, MHA, BS, FACHE; Distinguished Fellow in Healthcare Leadership; Assistant Professor; Jiann-Ping Hsu College of Public Health, Georgia Southern University, Statesboro, GA 30460-8015. E-mail: jstephens@georgiasouthern.edu; Telephone: 912-478-5958; Fax: 912-478-0171

Anthony V. Parrillo, PhD, MS, BA, CHES; President & CEO, E11even Consulting Service, Statesboro, GA; Chapter: Gamma Upsilon

* Corresponding Author

about the privacy and security of personal health data, so the task of writing rules on privacy eventually fell to the Department of Health and Human Services (DHHS); after several modifications, the HIPAA Privacy Rule was issued (United States Department of Health and Human Services [USSDHHS], 2003). The law requires health care entities (including hospitals, doctors, health plans, labs, pharmacies, and billing/claims agents) to protect the privacy of a patient's e-health information, the public key that allows protection against hackers (Austin, 2006). HIPAA sets the gold standard for privacy in the electronic age, but to what extent is patient confidentiality really protected, especially as it relates to e-mail communication? What benefits and shortcomings are there for health care consumers? Who is covered by HIPAA? What is the scope of coverage - i.e., what is covered by HIPAA and what is not; who is covered by HIPAA and who is not? What are the implications for the future?

This paper will focus on HIPAA's role in e-mail communications in health settings, particularly as it relates to the privacy of the information exchanged between doctor and patient. Specifically, the paper presents a brief overview of HIPAA, and addresses the privacy and security standards that appear in the legislation; in addition, the paper reviews how HIPAA addresses the security of e-mail communication and the fundamental importance of encryption to health care consumers. Finally, the paper discusses the bill's implications, including concerns related to security, availability, and protection of information. Among the chief goals in writing this paper is to foster a fuller under-standing of HIPAA and how it relates to the protection of health information in an electronic age.

Overview of HIPAA

The Health Insurance Portability and Accountability Act of 1996 implemented new rules for health care consumers and providers; the legislation mandates compliance with its Privacy and Security Rules. HIPAA laws apply to a covered entity (healthcare providers, clearinghouses, and health plan payers that meet certain conditions). In essence, most providers are covered entities if they employ an electronic-based office – meaning that they function by storing/exchanging health information via "…the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, private net-works, and the physical movement of removable/transportable electronic storage media" (45 CFR, Part 160, 1996).

HIPAA e-mail security applies specifically to PHI, not simply personal information. PHI is any individually identifiable health information about health status, the provision of health care, or payment for health care. This is often interpreted rather broadly and includes any part of a patient's medical record or payment history that can be "…transmitted by electronic media; maintained in any medium described in the definition of electronic media; or transmitted in any other form or medium" (45 CFR, Part 160, Subpart A, Section 103, 1996). As such, all administrative, financial, and clinical data on a patient are considered to be PHI and are to be treated with special care (see Table 1).

HIPAA mandates the implementation of administrative and technical rules (or standards) in five areas: electronic transaction standards, standard code sets for information, unique health identifiers for employers and providers, security and digital signatures, and privacy of individually identifiable health information. Healthcare organizations are obliged to establish both policies and procedures to protect the confidentiality of PHI with regard to their patients. HIPAA provides patients with greater control over how their PHI is used and disclosed. In essence, HIPAA seeks to establish standard mechanisms for electronic data interchange, security, and confidentiality of all healthcare related data and communication (including e-mail). There are two main compliance components under the Administrative Simplification provisions of the law: the Privacy Rule and the Security Rule. Health care providers who electronically transmit health information in connection with certain transactions must comply with both these rules (American Health Information Manage-ment Association, 2003).

Privacy and Security Standards

The HIPAA Privacy Rule took effect on April 14, 2003. It regulates the use and disclosure of certain information held by covered entities and sets standards for protecting the rights of patient information. Covered entities must follow the laws that grant each individual the right to the privacy and confidentiality of their health information (i.e., information on health status, provision of health care, or payment for health care that can be linked to an individual) (Terry, 2009). Stated another way, public health information is subject to an individual's rights as to how such information – oral, written, or electronic – is used or disclosed (45 CFR, Part 164, 1996).

Taking the Privacy Rule one step further, the DHHS was charged with developing the Security Rule to cover electronic PHI (ePHI). To this end, the security rule ensures a minimum level of secuity so that ePHI remains private and protected; it outlines a broadly flexible model for security management across the health care industry, and allows heightened protection against hackers, resulting in more secure, reliable information systems that help health data from being lost or accessed by unauthorized users (Austin, 2006). A key point at which this occurs is direct access to electronic forms of protected health information – not limited to purely oral or written communication (Burton & Kangas, 2009; Privacy Rights Clearinghouse, 2010).

The Privacy and Security Rules focus on protecting health data through information safeguards, and require covered entities to implement the necessary and appropriate means to secure and protect such data. Additional guidelines have been developed that address organizational and administrative concerns, along with technical and physical safeguards to reduce risk (Medem Network, 2006).

Table 1

List of 18 Identifiers That Must Be Treated With Special Care According to HIPAA

#	Identifiers
1	Names
2	All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Census Bureau: 1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3	Data (other than year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4	Phone numbers
5	FAX numbers
6	Electronic mail address
7	Social security numbers
8	Medical record numbers
9	Health plan beneficiary numbers
10	Account numbers
11	Certificate or license numbers
12	Vehicle identifiers and serial numbers, including license plate numbers
13	Device identifiers and serial numbers
14	Web Uniform Resource Locators (URLs)
15	Internet Protocol (IP) address numbers
16	Biometric identifiers, including finger, retinal, and voice prints
17	Full face photographic images and any comparable images
18	Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

Source: U.S. Department of Health and Human Services (2003)

E-Mail Communications Under HIPAA

In terms of how patient and physician now relate, e-mail has transformed communication, treatment, and care; millions of transactions are processed each day via e-mail at a fraction of the time and costs previously associated with hard copies. However, if left unprotected, or unavailable, e-mail can interfere with a healthcare organization's primary mission of providing high-quality patient care.

Within HIPAA, the terms *required* and *addressable* are used to describe levels of compliance. The term required designates full compliance; complying with a given standard is mandatory and, therefore, must be followed. When addressable is used, a given standard must be implemented, unless assessments and in-depth analyses conclude that such an implementation is not reasonable and/or appropriate, given the setting; regarding such addressable standards, organizations interpret each Security Standard separately and deal with each piece independently to determine appropriate compliance levels and the needs of the organization (Burton & Kangas, 2009).

The General Rules as they apply to these standards reflect a technology neutral approach; this means that organizations have some flexibility as it pertains to the types of systems that they choose to employ and no specific recommendations, as long as requirements for protecting e-communication are met. Some privacy advocates have argued that this flexibility can provide too much latitude to adequately cover the intent of the rule. As a result, three sets of recommendations and standards were developed (Burton & Kangas, 2009):

- Administrative safeguards guide personnel training and staff management regarding PHI and require an organization to reasonably safeguard (administrative, technical, and phys-ical) information and electronic systems.

- Physical safeguards are implemented to protect computer servers, systems, and connec-tions, including individual workstations. This section covers security concerns related to physical access to buildings, access to workstations, data backup, storage, and obsolete data destruction.
- Technical safeguards affect PHI that is maintained or transmitted by electronic media. This section addresses issues involving authentication of users, audit logs, checking data integrity, and ensuring data transmission security.

The American Recovery and Reinvestment Act (ARRA) signed into law February 2009 includes new, more comprehensive provisions for HIPAA. These clauses are in Section D of the bill known as the Health Information Technology for Economic and Clinical Care Act (HITECH); it provides heightened enforcement of HIPAA and stiffer penalties for privacy and security violations, and sets aside billions of dollars to invest in electronic health records (EHR) implementation and exchange.

For those organizations already required to abide by HIPAA (the covered entities of HIPAA), HITECH adds: mandatory yearly audits by DHHS personnel to ensure compliance, explicit fines (up to $1.5 million/year for disclosures of protected health information, Business Associate Agreements with vendors and partners (mandatory), and reporting requirements (to DHHS and the media) on the unauthorized disclosure(s) of protected health information. For HIPAA Business Associates, the bill imposes even more stringent changes, including: responsibility for following all Privacy and Security regulations with respect to all protected health information received and liability for unauthorized use or disclosure of protected health information (Cohen, 2009; Kangas, 2010).

Importance of Encryption for E-Mail Communications

Electronic mail is now fully embedded as a business tool in health care organizations, and is likely the top, mission-critical application used by a company. E-mail not only serves as a communication tool, but also in the transfer of sensitive, critical health data; it has become increasingly important to provide a secure, robust, and manageable way to protect these data. The technology created for this purpose involves encryption, "…the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR, Part 164, Subpart C, Section 304, 1996, p.15). Stated in a simpler way, encryption is one method of rendering electronic PHI unusable or indecipherable to unauthorized persons.

In reality, e-mail transmissions can readily be intercepted by those knowing how to do it over the standard Post Office Protocol 3 (POP3) protocol used in low-end e-mail hosting applications, or in many free e-mail services such as Yahoo, MSN, Verizon, etc. Threats do not always come from an external source, and are not always intentional; thus, messages must be encrypted "…from e-mail endpoint to e-mail endpoint…" (Stanley, 2007, p. 3). Mail servers using Microsoft (MS) Exchange have this ability to provide secure, en-crypted e-mail. Physicians need to be sure that their hosted e-mail accounts are use secure platforms; this ability to encrypt achieved by adjusting a few properties in MS Exchange-based e-mail accounts, whether using applications like Outlook and Thunderbird, or using web mail. Adjustments must be made on both incoming and outgoing servers, which are commonly under the Internet Message Access (IMAP) or the Simple Mail Transfer (SMTP) protocols. By adjusting these properties, e-mail is sent over a Secure Socket Layer (SSL), providing a level of encryption impossible to decrypt if the message were to be intercepted. Such encryption ensures that, even if e-mail messages were to be intercepted, they would be illegible because only the sender and the recipient possess the encryption keys to decode the message. Most important, securing e-mail in this way is compliant with HIPAA regulations under HITECH (USDHHS, 2009).

Security risks for e-mail commonly include unauthorized interception of messages en route to recipients and messages being delivered to unauthorized recipients. These risks are addressed in the Security Rule's technical safeguards (USDHHS, 2005), mainly regarding the following (Figure 1):

- Person and Entity Authentication. All required procedures must be implemented for identification verification of entity or party requesting access to PHI. This means the identity of the person seeking information must be confirmed within the information system being utilized.
- Transmission Security. Addressable data integrity controls and encryption reasonable and appropriate safeguards.
- Each healthcare organization using e-mail service must determine, based on technologies used for electronic transmission of PHI, how the Security standards are met.
- Addressable specifications that include automatic logoff, encryption, and decryption.

Implications of HIPAA for E-Mail

The subdivision of the law most relevant to e-mail is the rule that requires secure messaging solutions for the following key requirements for exchanging PHI over the Internet (Wilson, 2006). It applies encryption, authentication, and authorization controls to e-mail, attachments, web-forms, or web-pages to ensure their integrity, and it secures e-mail or other data without impacting an organization's existing workflow. Policies and middleware work with existing content scanning engines, mail servers, or web-servers and it applies compliance protection based on specific terms such as patient social security numbers. It also enables data to be protected and delivered by securing servers, and extends

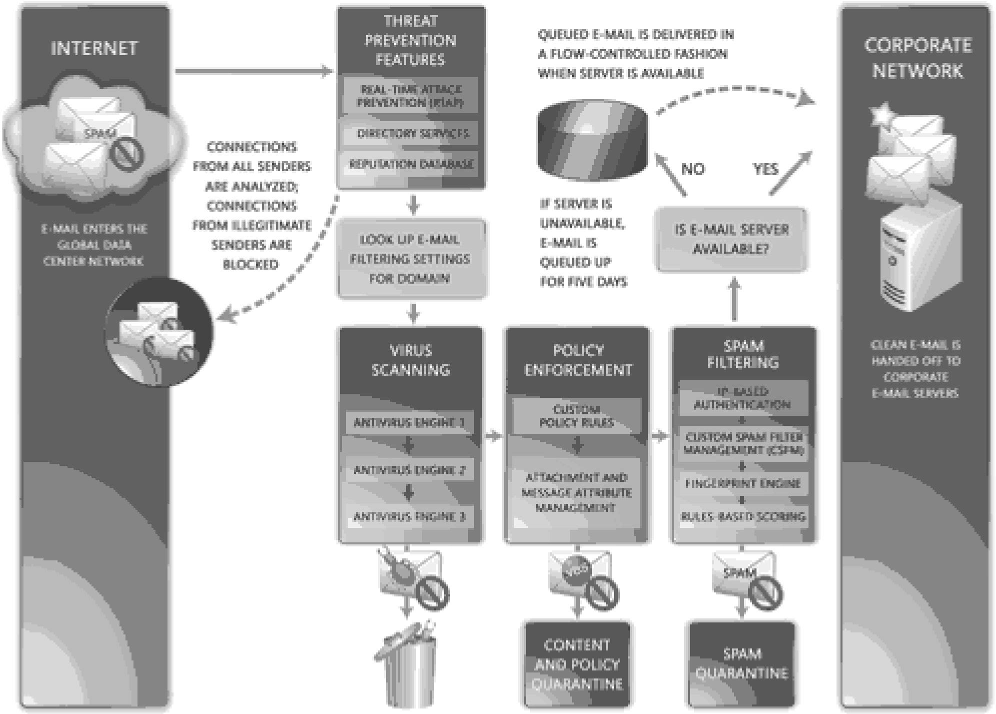
INTERNET
SPAM
E-MAIL ENTERS THE GLOBAL DATA CENTER NETWORK
CONNECTIONS FROM ALL SENDERS ARE ANALYZED; CONNECTIONS FROM ILLEGITIMATE SENDERS ARE BLOCKED
THREAT PREVENTION FEATURES
REAL-TIME ATTACK PREVENTION (RTAP)
DIRECTORY SERVICES
REPUTATION DATABASE
LOOK UP E-MAIL FILTERING SETTINGS FOR DOMAIN
VIRUS SCANNING
ANTIVIRUS ENGINE 1
ANTIVIRUS ENGINE 2
ANTIVIRUS ENGINE 3
POLICY ENFORCEMENT
CUSTOM POLICY RULES
ATTACHMENT AND MESSAGE ATTRIBUTE MANAGEMENT
CONTENT AND POLICY QUARANTINE
SPAM FILTERING
IP-BASED AUTHENTICATION
CUSTOM SPAM FILTER MANAGEMENT (CSFM)
FINGERPRINT ENGINE
RULES-BASED SCORING
SPAM
SPAM QUARANTINE
QUEUED E-MAIL IS DELIVERED IN A FLOW-CONTROLLED FASHION WHEN SERVER IS AVAILABLE
NO
YES
IF SERVER IS UNAVAILABLE, E-MAIL IS QUEUED UP FOR FIVE DAYS
IS E-MAIL SERVER AVAILABLE?
CORPORATE NETWORK
CLEAN E-MAIL IS HANDED OFF TO CORPORATE E-MAIL SERVERS

Figure 1. The integrated e-mail security and filtering solution (Bohm, 2007). Source: Microsoft/TechNet (http://technet.microsoft.com/en-us/library/bb676292(EXCHG.80).aspx)

protection to e-mail after delivery to a recipient's Inbox. It provides capabilities to ensure that patient information has been properly disclosed in accordance with existing corporate policies; it also provides for integration with an organization's existing authentication infrastructure.

E-Mail Security Concerns

The complexity of securing and making e-mail available grows every day. For one thing, e-mail has become a de facto distribution method in the increasingly sophisticated world of viruses, phishing attacks, fraud, spyware, and blended-threat techniques. In addition, spam continues to be a pervasive problem; the result is lost productivity, wasted network/storage resources, and liability for organizations that are not doing what they can to deal with the problem. Finally, the diverse and remote nature of most healthcare Information Technology (IT) networks poses additional challenges for typical IT staff. Ensuring that the proper security technology is installed on all devices – from desktops to hand-held computers to remote e-mail servers – can be a daunting challenge (Grove, 2003; Stanley, 2007).

E-Mail Security and Availability

Building secure and flexible solutions for a dynamic IT environment can pose a challenge for IT groups in healthcare organizations, but there are cost-effective ways to achieve such solutions. A layered approach is recommended, one that starts at the earliest point of entry onto the network, through to the end-user and beyond to archiving and storage systems. As a first line of defense, security should focus on user education and awareness regarding e-mail usage policies and best practices. For instance, users should know to avoid replying to spam messages, using unsubscribe links, following links in suspicious e-mails, opening e-mail attachments where there is no clear business relevance, or where the intention is suspect (i.e., the attachment may contain a virus or vulnerability patch), and paying attention to virus hoaxes (Wolf & Bennett, 2006).

Beyond user education, technology is still needed to stop e-mail threats. The most common virus content found in e-mail is the product of mass-mailer programs. Gateway-based antivirus scanners may be used to identify and distinguish mass-mailer threats so they can be removed before causing harm. A policy to delete attachments when the presence of a suspect extension type is detected can also be used. Building a resilient, secure foundation is oftentimes just as important as maintaining the security and availability of e-mail information. The need to build the infrastructure on a resilient foundation, one that is robust in its ability to meet growing demands, resistant to failure, and able to quickly recover when failure occurs, is of paramount importance in the health care setting. Storage management and clustering software are key technologies that can be used to construct this scalable e-mail infrastructure (Wolf & Bennett, 2006).

Addressing availability starts with ensuring protection of the e-mail data, utilizing a backup and recovery solution.

To minimize the disruption to business operations, backup software should offer a single management tool that combines all backup and recovery operations, providing management, alerting, reporting, and troubleshooting technologies at the same time. It is also important that health care organizations take advantage of both tape and disk storage technology, with its advances in disk and snapshot-based protection, off-site media management, and automated disaster recovery. In the final analysis, the right storage management solution will allow administrators to perform nearly all storage-related tasks online without having to take storage offline for the purpose of performing these regular maintenance functions. Clustering technology should be able to mirror data for redundancy and automatically move data from failing disks to healthy ones to cut the downtime from unplanned events, or to quickly move an application from a failed server to a healthy one (Wolf & Bennett, 2006) (see Table 2).

Implications for the Field

Performing daily transactions via electronic technologies is now accepted, reliable, and necessary as a way of doing business for the nation's health care industry, and email has emerged as a highly popular communications tool in recent years. Its capacity to convey important information swiftly and easily has transformed it into a communications workhorse (Holz, 2005). Collaborative efforts among health care providers have improved the delivery of quality care to all patients in addition to the recognized increase in administrative efficiency through the effective use of e-mail and other types of electronic communication. As a result, electronic communications have become the standard in the healthcare industry as a way to conduct business. What's more, patients have become more comfortable with e-mailing their physician's office to schedule appointments, discuss lab results, or request refills on medication; interacting with web-savvy patients has become part of the routine in a medical practice: real-time authorizations for medical services, transcribing, accessing, and storing health records, appointment scheduling, and submitting claims for payment of services provided are examples of how this is done. Medicare, and some other insurance payers, also recognize and pay for online consultations – known as mouse calls (Lowes, 2009) – where the health provider and patient interact over the web – i.e., telemedicine has become a larger part of the overall picture, particularly in rural areas (Burton & Kangas, 2009).

As e-mail seemingly enhances every facet of healthcare in the 21st Century, the benefits continue to be mitigated by security and privacy concerns. E-mail has evolved into a mission-critical issue for individuals and groups in healthcare organizations. As a result, flexible solutions to both security and availability must be employed. Given the large volume of protected health information in electronic form, HIPAA privacy requirements implicate the security and integrity of technological systems and processes; technological security must be applied as covered entities use their electronic systems to comply with HIPAA's regulations. Security measures must be customized for use in the health care industry and will grow more relevant as the trend towards electronic storage and maintenance of PHI continues.

Health educators, particularly those working in medical care settings, have a notable role to play as this evolution occurs (i.e., until physicians become more comfortable with communicating with patients via email). Within medical care facilities, health educators tend to work one-on-one with patients and their families. In this setting, in addition to educating patients about diagnosis, lifestyle change, and a host of other issues, health educators traditionally work closely with physicians, nurses, and other staff (Breckon, Harvey, & Lancaster, 1998).

As a result, during this transition period, health educators will serve as true patient-physician liaisons, a role for which they are in every respect prepared. The Seven Areas of Responsibility, the comprehensive set of competencies and sub-competencies that define the role of the health education specialist (National Commission for Health Education Credentialing, Inc., 2011), specifies that health educators act in specifically such a role for consumer groups, individuals, and health care providers: assessing needs for assistance (6.3.1); prioritizing requests for assistance (6.3.2); establishing consultative relationships (6.3.4); and defining the parameters of effective consultative relationships (6.3.3). As it applies to patient-physician e-mail communication, this currently works best for health educators employed in medical care settings, such as Health Maintenance Organizations – Kaiser Permanente uses health educators in its company-wide program of secure patient-physician e-mail messaging (Zhou, Kanter, Wang, & Garrido, 2010) – but all health educators can benefit from a detailed understanding of the issue.

The future may be just round the corner, given recent developments. First, and foremost, HIPAA includes recommendations – communication safeguards – and a profile of risk analysis designed to increase e-security and assist in picking a secure e-mail service provider. For those in health care settings, administrative, physical, and technical safeguards include solutions that meet (or exceed) HIPAA's Security Standards; protect data integrity; and demonstrate the delivery of flexible, scalable services. Second, a stricter set of safeguards were added to the HITECH section of ARRA, requiring agencies to tighten up their in-house e-mail and web-hosting functions (Kangas, 2010), and requires a yearly audit by the Department of Health and Human Service. This portion of the law addresses administrative access to assign (or change) user passwords, in-house controls to validate user access, audit controls that track user access and file access, methods that allow access to users based on role or function, automatic log-off after a specified time of inactivity, and data transmission security. It also concentrates on issues related to the unlimited attributes of electronic documents or e-mail transfers, ability for encryption, emergency access for data recovery, and minimal server downtime. Finally, guidelines on secure data backup and storage, secure data disposal,

Table 2

Example of Comprehensive Services and the HIPAA Rules They Satisfy (© Lux Scientiae, Inc.)

HIPAA Rule	1. View E-Mail with Secure Web-Mail, POP, or IMAP	2. Send Email with Secure Web-Mail or SMTP	3. End-to-End Encryption with SecureLine combined with 1 and 2	4. Secure Collaboration (Web Aides)
Access Control: Unique User Identification	√	√	√[1]	√[1]
Access Control: Emergency Access	√	√	√	√
Access Control: Automatic Logoff	√	√	√[2]	√[2]
Audit Controls	√	√	√[2]	√[2]
Integrity	√[3]	√[3]	√	√
Person or Entity Authentication	√[3]	√[3]	√	√
Transmission Security > Integrity Controls	√	√	√	√
Transmission Security > Encryption	√	√	√	√
Device and Media Controls > Data Backups	√	√	√	√
Device and Media Controls > Data Disposal	√	√	√	√

[1] A secure document storage service and use of the SecureLine application for communications may assume that recipients have special passwords for their "secure data access certificates" (PGP or S/MIME). These passwords can be stored in "Escrow," a special secure password database if the users so choose. In these cases, passwords can be retrieved in case of emergency or in case of loss.

[2] A secure document storage service and use of the SecureLine application for communications encrypts the data so that only the intended recipient(s) can ever view the data. The encryption process also allows the recipient(s) to verify that the data was not altered since it was sent or stored.

[3] SSL/TLS solutions encrypt the message during transport to and from the company servers and your personal computer. E-mail sent from the Company to external addresses is not necessarily secured without the use of SecureLine (see Solution #3).

Solution #3 provides complete transport layer and end-to-end e-mail security compatible with any e-mail user anywhere, no matter what software he/she may use.

Source: Burton and Kangas, 2009; USDHHS, 2003.

user-friendly, web-based access without the necessity of third party software, and privacy in not selling or sharing its client contact information are provided (Burton & Kangas, 2009; USDHHS, 2003).

Conclusions and Recommendations

Technology security has become increasingly important as covered entities use their electronic systems to comply with HIPAA's regulations. The security measures that have been adopted – and adapted – for use in the health care industry's electronic communication will grow more relevant as the trend towards electronic storage and maintenance of protected health care information continues, particularly in light of the passage of HITECH provisions and regulations. There are few studies that document the effectiveness of e-security measures; in time, businesses with large volumes of public health information in e-form will increasingly comply with HIPAA and improve the security and integrity of its systems. With this projected improvement, physicians may be more likely to e-mail their patients. Future research should be conducted to assess physician and patient perceptions, and possible concerns, in this area, particularly as it becomes more widespread.

In addition, there are several other areas of research that might warrant future attention. First, the development of a tool to measure the success of patient-physician e-mail communication; scales and questionnaires could allow for self-administration when possible, and include measures for different types of healthcare settings. Second, research on the predictors of successful physician-patient e-mail messaging; conducting studies to understand what variables best predict successful health outcomes as a result of e-communications between physicians, patients, and health educators. Finally, develop interventions that promote a greater understanding of health information for patients; creating and evaluating interventions that are varied according to content, target group, and setting. Research in these areas will provide important information to assist health practitioners in understanding how the secure patient-physician e-mail communications improve health.

References

45 CFR, Part 160, Subpart A, Section 103 (1996). *General Administrative Req uirements, General Provisions: Definitions.* Chicago, IL: Illinois State Medical Society. Document was prepared by Andrew H. Melczer, Vice-President, Health Policy and Research, February 20, 2003.

45 CFR, Part 164, Subpart C, Section 304 (1996). *Security Standards for the Protection of Elec-tronic Protected Health Information: Definitions.* Chicago, IL: Illinois State Medical Society. Document was prepared by Andrew H. Melczer, Vice-President, Health Policy and Research, February 20, 2003.

American Health Information Management Association: Policy and Government Relations Team (2003). *Final rule for HIPAA security standards*. Retrieved from http://library.ahima.org/spedio/groups/public/documents/ahima/pub_bok1_017594.html

Austin, S. (2006). E-mail: So fast, so convenient, so…risky? *Nursing, 36*(1), 76.

Baker, L., Wagner, T. H., Singer, S., & Bundorf, M. (2003). Use of the internet and e-mail for health care information: Results from a national survey. *Journal of the American Medical Association, 289*, 2400-2406.

Bertakis, K. D. (1977). The communication of information from physician to patient: A method for in-creasing patient retention and satisfaction. *Journal of Family Practice, 5*, 217-222.

Bohm, D. (2007). *Stopping junk e-mail with exchange hosted filtering*. edmond, WA: Microsoft Corporation. Retrieved from http://technet.microsoft.com/en-us/library/bb676292(EXCHG.80).aspx

Breckon, D. J., Harvey, J. R., & Lancaster, R. B. (1998). C*ommunity health education: Settings, roles, and skills for the 21st century.* Gaithersburg, MD: Aspen Publishers.

Burton, B. K. & Kangas, E. (2009). *HIPAA e-mail security management in e-mail communications.* Retrieved from http://luxsci.com/extranet/pdf/HIPAA-Email.pdf

Cohen, M. R. (2009). *Strategic implications of the HITECH Act: A CCI group white paper.* Homer Glen, IL: Cardinal Consulting, Inc.

Curtis, P. (1988). The practice of medicine on the telephone. *Journal of General Internal Medicine, 3*(3), 294-296.

DeVille, K. & Fitzpatrick, J. (2000). Ready or not, here it comes: The legal, ethical, and clinical implications of e-mail communications. *Seminars in Pediatric Surgery, 9*(1), 24-34.

Ellis, J. E., Klock, P. A., Mingay, D. J., & Roizen, M. F. (1999). Use of electronic mail for post-operative follow-up after ambulatory surgery. *Journal of Clinical Anesthesia, 11*(2), 136-139.

Freed, D. H. (2003). Patient-physician e-mail: Passion or fashion? *Health Care Management*, *22*(2), 265-274.

Grove, T. (2003). Summary analysis: The final HIPAA security rule. HIPAA Advisory, February, 2003. Retrieved from http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm

Harris Interactive (2002, April 11). Many patients willing to pay for online communication with their physicians [Press release]. Retrieved from http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=446

Holz, S. (2005, May-June). Establishing connections: Today's communications technologies have shifted the dynamic. *Communication World.* Retrieved from http://findarticles.com/p/articles/mi_m4422/is_3_22/ai_n14730061/?tag=content;col1

Kangas, E. (2010). *HIPAA 2010: HITECH impact on email and web outsourcing*. Westwood, MA: Lux Scientiae, Inc.

Kowalczyk, L. (2004, April 27). Is e-mailing the future of doctor-patient relations? *Boston Globe*, p. D2. Retrieved from http://www.lexisnexus.com

Lacher, D., Nelson, E. Bylsma, W., & Spena, R. (2000). Computer use and needs of internists: A survey of members of the American College of Physicians-American Society of Internal Medicine. *Proceedings of the American Medical Informatics Association Symposium*, 453-456.

Liederman, E. M. & Morefield, C. S. (2003). Web messaging: A new tool for patient-physician com-munication. *Journal of the American Medical Informatics Association, 10*(3), 260-270.

Lowes, R. (2009). Getting paid for mouse calls: Healthcare is slowly figuring out how to make online consults pay. *Physicians Practice, 19*(4), Retrieved from http://www.physicianspractice.com/mobile-health/content/article/1462168/1589000

Medem Network (2006). *eRisk working group for healthcare's guidelines for online communica-tion*. San Francisco, CA: Medem, Inc. Retrieved from http://www.calrhio.org/crweb-files/docs-privacy/20061121/2006%20eRisk%20Guidelines%20Final.pdf

Moyer, C. A., Stern, D., Dobias, K., Cox, D. T., & Katz, S. J. (2002). Bridging the electronic divide: Patient and provider perspectives on e-mail communication. *American Journal of Managed Care, 8*(5), 427-433.

National Commission for Health Education Credentialing, Inc. (2011). *Responsibilities and competencies of health educators*. Retrieved from http://www.nchec.org/credentialing/responsibilities/

Neill, R. A., Mainous, A., Clark, J. & Hagan, M. D. (1994). The utility of electronic mail as a medium for patient-physician communication. *Archives of Family Medicine, 3*(3), 268-271.

Pal, B. (1999). Email contact between doctor and patient. *British Medical Journal, 318*, 1428-1430.

Privacy Rights Clearinghouse (2010). *Fact sheet 8a. HIPAA basics: Medical privacy in the elec-tronic age*. Washington, DC: Privacy Rights Clearinghouse/UCAN.

Rao, J. K., Anderson, L. A., Inui, T. S., & Frankel, R. M. (2007). Communication interventions make a difference in conversations between physicians and patients: A systematic review of the evi-dence. *Medical Care, 45*(4), 340-349.

Ries, P. (1987). Physician contacts by sociodemographic and health characteristics, United States, 1982-83. *Vital Health Statistics, 10*(161). Hyattsville, MD: National Center for Health Statistics.

Rosen, P. & Kwoh, C. K. (2007). Patient-physician e-mail: An opportunity to transform pediatric health care delivery. *Pediatrics, 120*(4), 701-706.

Sittig, D. F., King, S., & Hazlehurst, B. (2001). A survey of patient-provider e-mail communication: What do patients think? *International Journal of Medical Informatics, 61*(1), 71-80.

Stanley, N. (2007). *The strategic importance of e-mail encryption: Securing business data and e-mail traffic through its journey.* Northamptonshire, United Kingdom: Bloor Research.

Terry, K. T. (2009). Patient privacy: The new threats. *Physician Practice, 19*(3). Retrieved from http://www.physicianspractice.com/index/fuseaction/articles.details/articleID/1299.htm

U.S. Congress (1996). *Health Insurance Portability and Accountability Act of 1996.* P.L. 104-191, 110 Stat. 1936. House of Representatives: 104 H.R. #3103; Senate: 104 S. #1028. Retrieved from http://www.dhhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf

USDHHS. (2003, February 20). *Health insurance reform: Security standards, final rule.* Federal Register, 68(34), 8333-8381. Washington, DC: Office of Civil Rights. Retrieved from http://regulations.vlex.com/vid/insurance-reform-portability-accountability-26899307

USDHHS (2005, June 6). *Secretary Leavitt takes new steps to advance health IT: National collaboration and RFPs will pave the way for interoperability* [News release]. Washington, DC: Office of the Secretary. Retrieved from http://archive.hhs.gov/news/press/2005pres/20050606.html

USDHHS (2009). *Guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009.* Retrieved from http://patientprivacyrights.org/media/HHS_Breach_RFI_05.09.pdf

Wilson, J. (2006). Health Insurance Portability and Accountability Act privacy rule causes ongoing concerns among clinicians and researchers. *Annals of Internal Medicine, 145*(4), 313-316.

Wolf, M. & Bennett, C. (2006). Local perspectives of the impact of the HIPAA privacy rule on research. *Cancer, 106*(2), 474-479.

Zhou, Y. Y., Kanter, M. H., Wang, J. J., & Garrido, T. (2010). Improved quality at Kaiser Permanente through e-mail between physicians and patients. *Health Affairs, 29*(7), 1370-1375.

Editor’s Note: The State of the Journal Coming Soon

Having served as Editor of *The Health Educator* since Spring of 2002, I am fast approaching a decade of service in this capacity. Now that nine years have passed and 18 issues have been published, it seems an opportune time to pause for reflection. Such reflection is not to be mere cogitation on my part, of course. It’s time to seek the Eta Sigma Gamma membership’s input on the best means by which to deliver our journal and other pertinent issues.

I have already informally polled the Editorial Associates of our journal for their takes on the pros and cons of eliminating print publishing of *The Health Educator* in favor of an electronic delivery format. Based upon their overwhelming positive response to investigating this option, I will seek the input of the membership in the next few months. No decision has been made to go this route; I am merely investigating the options we might have at our disposal. At the same time I seek input on this, however, I would like to collect additional information that will give the membership a strong sense of the “state of the journal.” For instance, how many members actually read one or more articles per issue as opposed to those who merely peruse the table of contents? Do members perceive the articles to be useful in their study and practice of health education or simply a venue for publication for those who need to publish or perish?

To accomplish this task I have asked the Editorial Assistant for *The Health Educator*, Maureen Liefer, to be involved as her work in formatting the journal will be influenced by results. In addition, I have engaged a PhD student in health education at Southern Illinois University to assist with data collection, management, and analyses. While it is likely to be a significant challenge to get a high response from the membership of Eta Sigma Gamma, nevertheless, the time has come to make the attempt. Please be looking for and ready to answer a survey in the near future!