Patient-centered E-mail: Developing the Right Policies

by Gretchen Murphy, MEd, RHIA

Patients and providers are increasingly communicating via e-mail. But healthcare organizations are slow in adopting policies to address important issues and manage this new communication form. Here's what you can do to develop some measures.

Like most industries, healthcare is undergoing unprecedented change. As such, it is struggling to understand the effective use of technology in supporting its current and future states. With the Internet and its derived technologies now added to the paradigm, the healthcare industry has become caught in a fundamental and irrevocable change in the way it conducts business processes.[1]

Where e-mail is available, we spend less time on the phone. We use it to set up and confirm meetings; we send attachments to colleagues for comment and mutual work. We even conduct meetings via e-mail. Virtually all organizations today are conducting business via e-mail. This is business communication at the start of the new millennium.

For HIM professionals, however, e-mail presents challenges as well as benefits. One particular facet of the new technology that we haven't caught up with yet is e-mail as clinical communication among providers and between providers and their patients.

HIM professionals have always worked to ensure that the best interests of patients are kept in mind, especially in terms of confidentiality and security. Now, patients have become our customers in a new way. By one estimate, more than 40 percent of patients in the United States use e-mail to contact health professionals.[2] Increasingly, e-mail is taking the place of phone calls to reach patients. It empowers the patient in new ways and brings new expectations as well.

While we want to serve customers in the best way possible, we need a framework in this area. We want good practice to drive the technology-not the technology to drive the practice. We need answers to fundamental questions like:

- what role does electronic mail play in health information management?
- what are the actions that ought to be under way to use it effectively?
- how can we learn from others' experience?
- how can we lead in the practice environment?

How do we, as HIM professionals, provide leadership and promote realistic management of this new tool for provider to patient communication? That's the question this article attempts to answer. We need to address the confidentiality and security aspects of e-mail between provider and patient, including informed consent. We need new business processes to manage the provider-to-patient e-mail communication function itself. We need to modify HIM practice to accommodate e-mail as clinical documentation appropriate for patient records. And we must continue to develop knowledge and understanding of the technology involved.

Technology, Laws, and Standards

During the l990s, the adoption rate of e-mail has been extraordinary. According to industry estimates, by the year 2001, more than half the US population will be using e-mail.[3] In 1998, 33 percent of 10,000 physicians polled used e-mail to communicate with their patients-a 200 percent increase over the year before.[4]

In healthcare, e-mail offers improved access to health services and efficiency of communication. What's more, it can be useful in patient care because providers must deal with an increasing number of nonemergency scenarios each day. The

asynchronous nature of e-mail makes it ideal for managing care through multidisciplinary teams and other settings.[5] It also is the first medium to offer patients a way to easily contribute directly to their own records.

Yet we remain cautious. While advances have been made in encryption, experts contend that Internet-based e-mail still poses security risks.[6] The technical options for forwarding and sharing messages allow e-mail users to send and receive information at the touch of a button, and errors in transmission can occur. Clinicians worry that patients may not use it appropriately, with the result that important messages may be missed.

Despite such concerns, providers are eager to use e-mail. In fact, organizations continue to be caught between underdeveloped policies and procedures and customer expectations in this area.

At the same time, laws are also evolving. Not only is electronic mail discoverable for legal purposes, but the proposed security rules for the Health Insurance Portability and Accountability Act (HIPAA) call for detailed attention to security issues, including e-mail. The current and future environment will need thoughtful monitoring as health information managers prepare for and implement the new activities.

Accreditation and Standards-What Role Do They Play?

With the advent of HIPAA, healthcare organizations are focusing on understanding the new requirements of secure handling of health information. While we have developed confidentiality and security policies for licensing and accreditation purposes for many years, the new challenges are unique. The requirement to transfer electronically stored health information in a secure manner has healthcare professionals scrambling to understand how to establish both the policy and operations level and the technical infrastructure required to support it.

In the past two years, standards development organizations have focused on a number of security issues. Of these organizations, the American Society for Testing and Materials (ASTM) has published several standards to assist organizations in developing policy and technical approaches to make this practice happen. For example, Standard E1869-97 calls for encryption for electronic mail. While this and other ASTM standards documents are continuously developing, they offer an initial reference point for organizations.[7] For more information, visit the ASTM Web site at www.astm.org.

Provider-to-Patient E-mail and the Clinical Record

A major concern for HIM professionals is the effect of e-mail on the patient record. What should be done with it? How should it be maintained?

Because e-mail serves as a way for physicians to direct patients on their individual care plans as well as a way for patients to respond about their treatments, this information becomes part of the clinical record.

Providers and others who work with e-mail recommend including it in the patient record. One provider includes e-mail directions to patients on the back of his business card, including brief instructions, recommended cautions, and a notice that he may save e-mail in his patients' records.[8]

How organizations evaluate this recommendation and others like it depends on culture and organizational structure. Integrated delivery systems and managed care environments that rely on intranets to coordinate patient care and health services may expect more pressure to formalize e-mail in clinical record business processes. Adding e-mail to patient records as additional interfiled paper in the day-to-day operations of managing patient record systems is the challenge.

How Can We Learn From Others' Experience?

How can we learn from others' experience in forging policies regarding patient-provider e-mail? Some good resources are already in place today. The most notable commentary was issued by a task force that developed the basis for a position statement adopted by the American Medical Informatics Association (AMIA) in l998. This position paper offers extensive suggestions on aspects of e-mail in the clinical environment.

We see the influence of this work on several healthcare organization's Web sites. Both the Stanford Medical Group and Kaiser Permanente provide patients with instructions on how to use e-mail to communicate with providers.[9,10] Other organizations,

such as Partners HealthCare System, are working to establish policies to assist their patients in moving forward with secure e-mail.[11]

The Community Health Information Technology Alliance (CHITA)-Agora model policy, developed through the Foundation for Health Care Quality in their Three-State Privacy project, consolidates contributed ideas from these sources as well as from Washington state members of the project. Recently funded by a Robert Wood Johnson grant to expand the project to five states, the current effort is known as the Healthkey Project and is committed to demonstrating secure e-mail communication through model privacy practices and pilot site evaluation.[12] "E-mail Draft Policy," [below] features the draft model policy currently under review by project participants and includes specific language on provider-to-patient e-mail.

Finally, the updated AHIMA practice brief published in the February 2000 *Journal of AHIMA* provides specific guidelines for health information managers.[13] The brief draws on a number of references, including the AMIA position paper, and provides comprehensive direction to practitioners.

In reviewing common policy elements in these and other sources, we can identify a number of areas where organizations have developed specific policy and procedure components. In "Patient-to-Provider E-mail Policy Provisions and Elements," [below] we can see six detail areas that are addressed within the broad tasks of confidentiality-based informed consent, operational directions for e-mail use, and clinical record applications. Details in one or more policies and procedures include the following recurring themes:

- confidentiality policies are updated to include e-mail communication
- patient informed consent for using e-mail to communicate with their provider is in place
- patient instructions on using e-mail effectively are provided via Web sites as well as within consents
- established boundaries for e-mail use are stated by policy and included in communications to patients
- the patient record is cited as the repository of e-mail communication between patient and provider
- technical security provisions are called for as the basic foundation to moving ahead with provider-patient e-mail

The matrix illustrates these policy topics with a cross reference to sources. Within these six areas, we can see common focus areas as well as the diversity in application.

Forming an Action Plan

What should you do now? Even though your individual organization may not officially sanction provider-to-patient e-mail, chances are it's happening. Reports of providers who communicate with their patients by e-mail are growing.[14] Regardless of policy, health information departments are likely receiving copies of e-mail correspondence with requests to file them in the record. While we may continue to resist, legal advice and leaders in our field recommend we find a way to accommodate this new form of documented clinical communication. Consider starting on the following:

- First, **update current confidentiality policies to incorporate references to e-mail if they are not already in place.** This may be as simple as modifying current language to specify that patient-identifiable health information in any form (examples included) is maintained in a confidential manner. You might also make reference to organizational policy in the material developed for patient communication. If a policy is not yet in place, develop a new one that specifically addresses e-mail users, authentication, confidentiality, security provisions, and usage rules. Patient role may be included or may be a separate policy.
- Second, **develop a notice and consent form for patients who wish to use e-mail to communicate with their providers.** The notice should advise patients of the confidentiality policy and security issues and inform them about who will see their health information. It also should clearly point out the need for patients to adopt privacy practices. See the notes at the end of this article for examples that charge patients to handle their information in a secure manner. If your organization is working on Web-based access for patients, connect with that effort. Visit the Web sites for the resources listed in our matrix for examples.
- Third, **prepare directions for patients and providers on how to use e-mail for care purposes and develop the procedures required to support them.** This is particularly important where e-mail messages serve as documentation in the clinical record. Directions should include information on how patients are to identify themselves, the specific kind of messages that are appropriate for e-mail, and how patients should escalate issues when necessary. Cautions against using e-mail for emergency messages and sensitive health problems should be included. Organizations may begin with

inviting patients to communicate on topics such as making or confirming appointments or requesting pharmacy prescription refills. It should also be made clear to staff that e-mail is discoverable for legal purposes.

- Fourth, **work with clinical and operational staff to define the usage boundaries for electronic mail.** How information is shared and forwarded and rules for handling it should conform to your organization's role-based access guidelines. Organizational security frameworks that designate clinical staff access apply to e-mail as well. Where e-mail is screened for triage purposes, staff training to process and refer messages and confidential handling of e-mail printouts may be needed.
- Fifth, **work with the medical record committee to reach consensus about placing the e-mail into the patient record.** Emerging recommendations call for including e-mail to be placed in the record when it refers to specific healthcare directions or response to treatment. But when e-mail communication becomes voluminous, operational costs will be an issue. Where e-mail can be stored electronically and retrieved as part of the patient's electronic health record, new work will be required to determine the most effective way to maintain and retrieve the information. If including e-mail as clinical documentation in the patient record is optional, criteria for inclusion might be patterned after telephone encounter documentation guidelines. The matrix consensus is not clear in this area. In some cases, it has not yet been addressed.
- Finally, **develop technical security measures that address e-mail to meet the HIPAA requirements.** Note the attention paid to encryption on the matrix. Technical security practices focus on user ID requirements and remote access protection as well. As a targeted practice area for HIM professionals, security policies and technical provisions continue to expand current HIM roles.

Organizational Security Framework

From the broad perspective, security provisions are built from privacy principles, organizational policies, and security practices to support health information business processes. Policy development, revised procedures, and applied technical provisions are certainly a priority for healthcare organizations and health information managers today.

The unique aspect of patient-to-provider e-mail creates both opportunity and challenge on a day-to-day basis. The role of the patient record in documenting the care process is being expanded as new forms of documentation evolve. By monitoring the potential in these communication options and assessing organizational preparedness, we are better prepared to propose collaborative projects to support change in a planned manner.

Patient-to-Provider E-mail Policy Provisions & Elements

Policy provisions addressed	Massachusetts Health Data Consortium	Stanford Medical Group	Kaiser KPNCR	Partners Draft Policy	CHITA-Agora Model Policy	AHIMA Practice Brief
Patient informed consent for e-mail	•		•	•	•	•
Confidentiality policy update		•	•		•	•
Patient instructions						
Directions to patients	•	•	•	•	•	•
Patient ID directions	•	•	•	•	•	•

Form/structure for messages	•	•	•	•	•	•
Permissible content		•	•		•	•
Sensitivity caution	•	•	•		•	
Usage boundaries						
Who initiates message	•			•	•	
Rules for sharing	•			•	•	•
Group mailing to patients	•				•	•
Clinical record inclusion						
Retained in the clinical record	•		•		•	•
Optional				•		
Technical security practices						
E-mail encryption	•		•	•	•	•
User ID	•		•	•	•	•
Sanction for breaches					•	
Protect remote access	•		•		•	•
*Web access						

E-mail Draft Policy

CHITA-Agora Project Privacy Task Force

Sept. 6, 1999

Electronic mail has become an integrated tool in all business processes. This policy defines appropriate use of ((ORGANIZATION NAME)) e-mail systems and applies to all users including, but not limited to, employees, medical staff, contractors, students, and volunteers. This policy further applies to all usage of ((ORGANIZATION NAME)) electronic mail systems where the mail either originated at a ((ORGANIZATION NAME)) computer or network, or is received into a ((ORGANIZATION NAME)) computer or network from an external mail system. This policy assumes use of the public Internet and interaction with patients and other members of the public at large.

Procedure

1. User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via ((ORGANIZATION NAME)) electronic mail system(s). In addition to this policy, users of e-mail are required to comply with the ((BROAD INFORMATION SECURITY POLICY NAME)) and the ((INTERNET USAGE AND CONNECTIVITY POLICY NAME)) found in the ((ORGANIZATION/DEPARTMENT POLICY MANUAL NAME)).

Electronic mail is intended to be used as a business tool to facilitate communications and information exchanged needed to perform an employee's job. All messages originated or transported within or received into ((ORGANIZATION NAME)) electronic mail system are considered to be the property of ((ORGANIZATION NAME)).

Users have an obligation to use e-mail appropriately, effectively, and efficiently.

Users should be aware that all e-mail transmissions are made by permission of ((ORGANIZATION NAME)) and are identified with the ((ORGANIZATION NAME)) name. Discretion should be used to ensure that the image or reputation of ((ORGANIZATION NAME)) is not diminished or negatively affected.

2. Prohibited Use of Electronic Mail

The following are some specific examples of prohibited usage of ((ORGANIZATION NAME)) e-mail systems. This list is not to be considered all-inclusive. Further questions regarding appropriate use of electronic mail should be directed to the employee's supervisor or the ((INFORMATION SECURITY ADMINISTRATOR TITLE)).

2.1 Do not use e-mail for urgent or time-sensitive communications.
2.2 Do not use e-mail to transmit highly confidential or sensitive information, e.g., discussion of HIV status, mental illness, chemical dependency, and workers compensation claims.
2.3 Do not attach ((XXX)) files for transmission by e-mail (describe limitations to e-mail attachments, e.g., large database files, etc.).
2.4 Do not use e-mail addresses for marketing purposes without explicit permission from the target recipient.
2.5 Do not share professional e-mail accounts with family members.

3. User Privacy of Electronic Mail

((ORGANIZATION NAME)) recognizes that users may have reasonable expectations of privacy with regard to electronic messages received and/or stored on the ((ORGANIZATION NAME)) information system. However:

3.1 ((ORGANIZATION NAME)) reserves the right to access the electronic mail system for the purpose of ensuring the protection of legitimate business interests and proper utilization of its property. Such purposes may include, but are not limited to:
3.1.1 locating and retrieving lost messages;

3.1.2 performing duties when an employee is out of the office or otherwise unavailable;

3.1.3 maintaining control of the system by analyzing message patterns and implementing revisions as needed;

3.1.4 recovering from systems failures and other unexpected emergencies; and

3.1.5 investigating those suspected breaches of security or violations of policy with probable cause.

3.2 Supervisors and/or administrators must advise and receive approval from the ((INFORMATION SECURITY ADMINISTRATOR TITLE)) of their intent to review an employee's messages prior to accessing employee files.

4. Confidentiality of Electronic Mail

Users of the ((ORGANIZATION NAME)) electronic mail system may have the capacity to forward, print, and circulate any message transmitted through the system. Therefore,

4.1 Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

4.2 Information of a confidential or sensitive nature received or transmitted via electronic mail must be protected. Refer to the ((BROAD INFORMATION SECURITY POLICY NAME)) located in the ((ORGANIZATION/DEPARTMENT POLICY MANUAL NAME)) with regards to the protection of confidential information.

4.3 E-mail communication systems are not secure; mail sent via the Internet or other external systems can be intercepted and read by individuals other than the intended recipient. Therefore, when e-mail is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information. (Examples of such information include patient information, personnel actions, performance appraisals, sensitive business/legal information, etc.) Specific safeguard measures are as follows:

4.3.1 Information considered confidential or sensitive must be encrypted during transmission of the data. This can be accomplished by:

4.3.1.1 utilizing the internal encryption capability built into the e-mail software (Note: this may vary depending on IS configuration.)

4.3.1.2 utilizing some other approved encryption system and/or service (further questions regarding encryption should be directed to the ((INFORMATION SECURITY ADMINISTRATOR TITLE)).)

4.3.2 A notation referring to the confidential or sensitive nature of the information should be made in the subject line to further safeguard the confidentiality of electronically submitted data.

4.3.3 Confidential or sensitive information may be distributed to multiple recipients; however, the use of distribution lists is prohibited.

4.3.4 Confidential or sensitive information is to be distributed only to those with a legitimate "need to know."

5. Physician/Clinician Use of E-mail

Guidelines for using e-mail in a clinical setting include:

5.1 Obtain patient's informed consent for use of e-mail. Written forms should:

5.1.1 Itemize communication guidelines, e.g., establish turnaround time for messages (do not use e-mail for urgent matters), inform patients about privacy issues, establish types of transactions and categorize e-mail messages by transaction type, etc. (see sample communication guidelines.)

5.1.2 Provide instructions for when and how to escalate to phone calls and office visits.

5.1.3 Describe security mechanisms in place.

5.1.4 Indemnify the ((ORGANIZATION NAME)) and/or the appropriate healthcare institution for information loss due to technical failures.

5.1.5 Waive encryption requirement only at patient's insistence. Documentation of this waiver must be kept on file. Under no circumstances should unencrypted wireless communications be used with patient-identifiable information.

5.2 Never forward patient-identifiable information to a third party without patient's express permission.

5.3 Double-check all "TO" fields prior to sending messages.

5.4 Use a banner at the top of each e-mail message stating "This is a CONFIDENTIAL medical communication."

5.5 Electronic mail used in a clinical setting constitute a form of progress note. In the absence of an electronic patient record that allows inclusion of e-mail messages, each e-mail message should be printed in full and a copy and placed in

the patient's paper record. Efficient archiving can be accomplished by:

5.5.1 Include the full text of the patient's query in the e-mail reply.

5.5.2 Copy (cc:) the reply to the sender.

5.5.3 Print the sender's copy (which includes the initial message and reply) and file it in the patient record unless an acknowledgement is expected. When such an acknowledgement has been requested, e.g., when important medical advice has been given, the printed (chart) copy should not be filed until this confirmation is received.

5.6 Printers must operate in an area that is accessible to staff only and not to patients.

6. Retention of Electronic Mail

6.1 Perform at least weekly backups of mail onto long-term storage (as applicable to paper records.)

6.2 INSERT: Policy for length of storage on back-up systems.

6.3 INSERT: Policy/procedure for establishing e-mail repository, e.g., on local machines, ISP mail server or both.

6.4 INSERT: Procedure for clearing e-mail from the archive server/s.

7. Compliance

Employees and users of the ((ORGANIZATION NAME)) electronic mail system(s) who are found to be in violation of any part of this policy are subject to disciplinary action up to and including dismissal.

Responsible Unit

((INFORMATION SECURITY ADMINISTRATION DEPARTMENT NAME))

Approved by:

((COMMITTEE NAME)), ((DATE APPROVED))

Reviewed and Revised:

((DATE OF REVISIONS))

ATTACHMENTS: e.g., Procedures for Encrypting Messages

Notes

1. Kohn, Deborah. "Preparing the Environment for Internet-Derived Technologies." In *Electronic Health Records: Changing The Vision.* Murphy, G.F., Hanken, M.A., Waters, K.A., eds. Philadelphia: W.B. Saunders, l999, p. 144.

2. "E-mail Contact Between Doctor and Patient." *Medical Practice Communicator* 6, no. 4 (1999): 5. Available at http://www.medscape.com/.

3. Sands, Daniel Z. "Guidelines for the Use of Patient Centered E-mail." White paper. Massachusetts Health Data Consortium, l999. Available at http://www.mahealthdata.org/.

4. *Ibid.*

5. Mandl, K.D., Kohane, I.S., Brandt, A.M. "Electronic Patient Physician Communication: Problems and Promises." *Annals of Internal Medicine* 129 (1998): 495-500.

6. Navighurst, Craig. "Unlocking the Mailbox." *American Medical News,* September 13, l999.

7. "Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-based Patient Records." ASTM standard no. E1869-97. Available at the ASTM Web site at http://www.astm.org/.

8. "Danny's Clinical Use of E-mail Page." Available at http://clinical.caregroup.org/ePCC/.

9. "Electronic Mail Services." Available at the Stanford Medical Group Web site at www.med.stanford.edu/shs/smg/email.html.

10. "Doctor Appointments and Advice Available Online." Available at the Kaiser Permanente Web site at www.kaiserpermanente.org/locations/colorado/newsroom/releases/online.html.

11. "Guidelines for Clinical Electronic Mail Communication." Partners HealthCare draft policy, May 3, 1999.

12. CHITA-Agora Project Privacy Task Force. "Electronic Mail (E-MAIL) Draft Policy 1.2." September 6, 1999.

13. Hughes, Gwen. "Practice Brief: E-mail Security (Updated)." *Journal of AHIMA* 71, no. 2 (2000): insert.

14. Mandl, K.D., Kohane, I.S., Brandt, A.M. "Electronic Patient Physician Communication: Problems and Promises."

Gretchen Murphy *is director of the health information administration program at the University of Washington, Seattle, and a member of the Journal of AHIMA's editorial advisory board. She also serves as chair of the CHITA-Agora privacy task force, Healthkey Project, Foundation for Healthcare Quality. She can be reached at gcmurphy@uwashington.edu.*

Article citation:
Murphy, Gretchen. "Patient-centered E-mail: Developing the Right Policies." *Journal of AHIMA* 71, no.3 (2000): 47-54.
