Leading the Way to Health Information Exchange in the Electronic World

(To order the complete report, please contact our Resource Center & Library via e-mail or at (781) 768-2502.)

Guidelines for the Use of Patient-Centered E-mail

Daniel Z. Sands, M.D., M.P.H.
Beth Israel Deaconess Medical Center and Harvard Medical School

Relevance: E-mail Use in Patient Care

Historically, communication between a patient and a provider took place through personal encounters or written documents. Once the telephone was introduced in the late 19th century, physicians and patients began, not without trepidation, to use this form of communication as well, despite concerns over maintaining patient privacy. Today the telephone is ubiquitous in the industrialized world, and the practice of "telephone medicine" has enabled managed care and has spurred an entire industry of telephone triage.

In the latter half of this century, the development of electronic paging and voice messaging extended the capacity of the telephone as a communication medium. The introduction and wide acceptance of the fax machine provided still more options for patients and providers. In the mid-1970's, electronic mail (e-mail) was introduced. Its use remained limited to academia and research labs for many years. It was slow to be embraced by the health care profession, although some institutions, like Boston's Beth Israel Hospital, were early adopters. (1)

In the 1990's e-mail exhibited exponential growth resulting from users' increased comfort with computers, inexpensive hardware and software, the proliferation of the World Wide Web, and employer-provided e-mail services. The adoption rate of e-mail, now as common as the fax machine in business settings, has been extraordinary. According to industry estimates, by the year 2001, more than half the U.S. population will be using e-mail. (2)

E-mail is useful in patient care as health care providers must deal with multitudes of non-emergency scenarios on a daily basis. Interruptions from non-urgent messages through paging have been shown to interfere with patient care and to increase provider stress levels. (3) E-mail is also valuable because many health care providers are highly mobile, seeing patients in multiple inpatient and outpatient settings while performing research and teaching.

As outpatient care has become more complex, multidisciplinary teams of providers are needed. These teams require improved forms of communication to manage patients effectively. The asynchronous nature of e-mail makes it ideal for this purpose.

The growth of managed care and capitation is also changing communication in health care. Manually processing patient requests for referrals places administrative burdens on the system; e-mail can simplify this type of clerical communication. Further, capitation has provided incentives to physicians to seek alternative methods of caring for patients in addition to face-to-face encounters.

Important characteristics of e-mail for policy consideration are:

- Asynchronousness: Parties do not have to use e-mail at the same time to communicate. This property explains why e-mail supporters praise its use over that of the telephone--e-mail eliminates the problem of "telephone tag." Because e-mail can be read and acted upon at any time, it permits providers to "time-shift" and manage patient e-mail messages when convenient. Conversely, this same property, unfortunately makes it is easy for e-mail messages to be forgotten and not answered promptly.
- Informality: Since increasing numbers of people use computers at work, they have become comfortable with e-mail and have found it an efficient way to communicate informally. As a result, people often communicate information through e-mail that they would not be willing to share in person or in writing. Because messages cannot generally be retracted (except within some institution-specific e-mail systems) this frankness can lead to embarrassment.
- Permanence*:* Although as informal as a conversation, e-mail can be saved and stored in a way that face-to-face and telephone conversations cannot. The benefit is that e-mail can be self-documenting (an e-mail message, once printed or saved along with contextual materials, speaks for itself and does not require additional documentation). This same property means that e-mail can be infinitely recoverable. Recovery of old e-mail messages which were thought to have been deleted is now a cottage industry.
- Lack of richness: Since most e-mail is text based, it is difficult to communicate humor, warmth, sensitivity and other emotions.

Although the telephone and fax machine were adopted with little discussion about their appropriate uses and risks, it is worth discussing issues and setting policy regarding the use of e-mail for several reasons:
E-mail is generally transmitted unencrypted over an open computer network and can be intercepted and read. There is weak federal legislation comparable to wiretapping laws to protect e-mail. [4]

1. As e-mail is transmitted, copies may be left on many different computers. Even copies of e-mail messages that were "deleted" can be recovered years later.

2. There are no standards for addressing e-mail. E-mail addresses cannot be determined or verified, and are frequently changed. There is no easy way to verify the sender of an e-mail message.

3. E-mail is a relatively new medium and one that users need to learn to employ to its greatest benefit.

4. The widespread acceptance of e-mail as a means of communication suggests that it will be difficult to avoid its use in the future to communicate with patients and providers.

This paper addresses issues arising from the use of patient-centered e-mail between patients and providers, between providers and providers and between payers and providers. It also supplies recommendations to health care organizations and providers trying to establish policy to govern the use of e-mail in patient care.

Importance of E-mail Policy for Health Care Institutions

Risk Management

Risk management is the major reason that policy regarding use of e-mail in health care settings is important. (5) The individual patient is at greatest risk, but health care providers or institutions may incur risk as well. Legal issues in patient-provider e-mail were recently reviewed. [6]

A summary of risk management concerns follows with associated legal issues:

Risks	Issues	Concerns

Confidentiality	Health-related information is felt to be confidential, especially when dealing with psychiatric illness, substance abuse, sexually-transmitted diseases, and other infectious diseases.	The largest risk to disclosure of health information is fear that it could lead to employment or social discrimination, financial ruin, invasion of privacy or embarrassment.
Indelibility	To a health care provider or institution, e-mail can be both beneficial and detrimental from a risk prevention standpoint. Since e-mail provides a virtually indelible record of correspondence between patient and provider, interactions can be recounted more accurately than recollections of telephone or personal conversations.	Plaintiffs' attorneys routinely require health care organizations to produce e-mail as evidence. E-mail has proved to be incriminating evidence in several high-profile cases outside of health care, as the Microsoft case exemplifies. [7]

Risks	Issues	Concerns
Interception	Because e-mail is usually transmitted unencrypted over the public Internet and stored on and forwarded from many computers, there is risk of interception. Because of the sheer volume of e-mail on the Internet the *probability* of risk is low, but the stakes are high, and there is need for concern.	An estimated 30 million Americans have access to e-mail at work. [8] These computers and the e-mail on them is usually owned by the employer. The right of employers to look at their employees' e-mail has been upheld by some courts. [9]
Incorrect addresses	E-mail addresses are often quite cryptic and, even when logical, are difficult to assume because there are no conventions that dictate the proper form of an address (e.g., john_smith@company.com or jsmith@company.com or john.smith@company.com or johns@company.com).	In some situations this results in non-delivery of the message. In other cases this may result in the delivery of the message to the wrong individual, resulting in anything from minor nuisance to major embarrassment.
Incorrect routing	Incorrect routing of e-mail is common.	Typically this occurs when one forwards a message to a third party unbeknownst to the original author. Also, an e-mail recipient may reply to all recipients of a message when meaning to reply only to the sender. Finally, one can send an e-mail message to a group of people with each name in the "to" field, revealing each person's address to everyone in the group.
Turnaround time	A delayed response may result from the non-receipt of e-mail, recipient not reading any e-mail, recipient not reading a specific message, or delayed response for other reasons.	If patients expect that a response will occur within a certain timeframe but does not, resulting in harm to a patient, the physician could be liable. Escalation procedures can prevent this.
Identity verification	It is impossible to verify the true identity of the sender of an e-mail or to ensure	If an e-mail message is sent to an unintended recipient, resulting in harm

	that only the recipient can read it.	to a patient, the physician could be liable.

Many of these concerns can be addressed through the use of encryption and authentication techniques (public-private key algorithms being the most useful) along with the careful applications of a patient-provider agreement for the use of e-mail.

Benefits

E-mail can provide competitive advantages to health care providers and organizations that leverage it properly by:

- Increasing inter-provider communication, resulting in better-coordinated and more cost-effective care.
- Allowing patients to participate more fully in their care and decrease the alienation that health care consumers find in the health care system.
- Removing communication barriers between patients and providers while not overwhelming providers with additional tasks. A recent study showed that the amount of additional time required to answer e-mail messages was small; (10) because time can be shifted it is not another interruption in an already busy day.
- Reducing the number of non-urgent telephone calls and pages for providers. Discrete data transmissions like blood glucose values and blood pressures, and clerical matters such as requests for managed care referrals and prescription renewals, can all be handled efficiently through e-mail.
- Improving communication to manage more effectively the patient's health and to reduce health services utilization.
- Sending patients educational material and sharing health related Web-sites.
- Providing an improved record of communications between a patient and provider (documentation of phone conversations is often inadequate or neglected).

With any new technology, there are risks and benefits as well as the potential for effective use and abuse. E-mail is no different in this regard. By establishing guidelines for providers and patients, e-mail can be used most effectively in patient care.

Policy considerations

Policy Framework

Because technology and its role in society are in a state of flux and there is a paucity of case law and legislation bearing upon the use of e-mail in patient care, it is impossible to mandate guidelines for all health care organizations. Some organizations will choose to be extremely cautious in their choice of guidelines, while others will be more liberal and permit less restricted use of the medium. The tone of a policy can run the spectrum from liberal encouragement to active discouragement.

E-mail policies will be difficult to enforce, yet health care organizations may be held accountable for their employees' adherence to written guidelines. The purpose of this document is to help health care organizations and providers review their options and develop guidelines that are robust and in keeping with their organizational cultures.

There are general issues for all forms of patient-centered communication through e-mail, and issues specific to patient-provider and inter-provider communications. The general issues are:

General Issues	Concerns	Policies Should Address
Patient identification	Use of patient identification numbers can be helpful but is not useful when communicating with people outside one's health care organization.	• How will patients be definitively identified? • When providers are discussing a patient in e-mail, how do both parties know which patient is being discussed? • When a patient is e-mailing a provider, how will that provider know which patient sent the e-mail?
Directory Management	Since few computerized patient registration systems have a field for e-mail address, and even fewer organizations routinely record, let alone update, this information, this rapidly becomes problematic. A patient e-mail address field in the organization's patient registration database (also called a Master Patient or Master Member Index) can be managed with data elements like phone numbers, address, fax number, etc. Ideally, whoever identifies and updates this information should be able to update it online. Maintaining the information will uniquely link the patient identity to the e-mail address.	• How do providers ensure the correct addressing of e-mail, both to providers and patients? • Who, if anyone, maintains directories of patient e-mail addresses? • How can one link an e-mail address to a specific patient in the practice?
General Issues	**Concerns**	**Policies Should Address**
Inclusion in the Record	A great deal of communication does not make it into the patient record, such as telephone calls and informal consultations. Generally, providers decide what should and should not be included in the record. Since e-mail is almost eternally recoverable and others may possess copies of e-mail, it may make sense to include	• Should patient-identifiable e-mail messages be included in the patient's record? When? • What about messages that are relatively free of clinical content? • If it is decided that all or some e-mail messages should be incorporated into the record, what is the process for doing so? • How are electronic patient records that are capable of accepting e-mail messages directly handled? • Should e-mail be printed and sent to the

	everything in the record. However, there may be messages that are relatively free of content and add nothing to the record. If one adopts a policy of including *all* patient-centered e-mail in the record, this practice would be the only example of a patient being able to write directly into his/her health care record.	medical record department for inclusion in the patient's paper record? • Should copies of all outgoing messages (especially from providers to patients) be kept?
Confidentiality	Every health care organization should have guidelines in place which cover confidentiality of patient information.	• Policy should be broad enough to include information transmitted by written communication, telephone, fax, and e-mail.
Security	Unencrypted e-mail poses a potential risk. There is currently no trusted digital certificate authority for health care, and the use of this technology - although fairly straightforward with most popular e-mail products - is by no means universal. By insisting on encryption organizations may either create an unenforceable policy or they may quash the use of e-mail in patient care.	• Policy should address encryption with public-private key systems and digital certificates.
Comfort with the medium	People should use e-mail only when they feel comfortable with reading and writing e-mail. Effective use of e-mail is a skill learned over time, and we can expect that eventually everyone will become as comfortable with e-mail as they are with using a telephone. People should not be forced to use e-mail.	• Should providers be mandated to use e-mail with their patients? • Should providers be required to respond to e-mail from other providers?
Appropriate use of e-mail	Because it is an asynchronous means of communication e-mail should not be used in emergencies or in any time-sensitive situations.	• How are escalation procedures handled if a response is not received in a reasonable amount of time, for patient-provider and for inter-provider communications? • Because of confidentiality concerns with unencrypted e-mail, policies should address use of e-mail to transmit sensitive information.
Archiving policies	If an organization opts to include all patient-centered e-mail in the patients' records, that	• What procedures are in place to archive e-mail servers? • Should organizations periodically destroy all

	material must be archived and maintained in accordance with state laws pertaining to medical records.	unsaved e-mail after a period of time and not archive the e-mail files at all beyond that, subject to advice of counsel?
Computer systems policies	Many concerns about e-mail are amplified in organizations that do not encourage privacy of passwords or have lax policies for data security.	• Policies should address users in health care organizations sharing password or e-mail accounts. • Policies should address timed log offs for computers in shared work areas to prevent accidental or intentional exposure of private e-mail files, and should encourage users to log off after using devices in common areas.

Issues specific to Provider-Patient e-mail are:

Provider-Patient E-mail Issues	Concerns	Policies Should Address
Who may receive	Providers may want their own e-mail addresses kept from patients or they may be willing to share it only with selected patients. In these situations, practices might consider having an e-mail triage system in place.	• Routing of all e-mail from patients to e-mail addresses accessed by one or more triage nurses, which may be practice-specific • Should nurses handle e-mail themselves and, when necessary, route the mail to the appropriate provider?
Who may initiate	Instituting a policy whereby providers will not initiate unsolicited e-mail to patients would limit the provider's liability somewhat, much in the way that some providers use great caution when leaving messages on a patient's answering machine or voice mail.	• Should providers be able to send unsolicited e-mail to patients?
Routing of e-mail	Prohibiting routing of e-mail will significantly impair physician workflow.	• Should e-mail from one patient be forwarded to other providers or staff without the specific or blanket permission of the patient? • Is it acceptable to have patients agree with providers ahead of time that they will route e-mail to office staff or consultants when it is necessary?
Permissible transactions	Use of e-mail to discuss sensitive information or issues can increase the consequences to the patient if such messages are viewed by third parties.	• How do organizations stipulate that providers use e-mail to communicate about subjects that are particularly sensitive, such as substance abuse, HIV status, sexually transmitted diseases, and psychiatric illness?

Standards for group mailings	Patients' names, e-mail addresses, and health information should not be inadvertently disclosed to other patients.	• Whenever e-mail is sent to multiple patients, should their addresses be placed in the blind carbon copy (bcc) field of the e-mail, to keep recipients identities unknown to one another?
Quoting text	Responses to e-mail messages out of context can lead to misunderstanding.	• Should all message responses to the patient include the text of the original message to enhance readability and maintain context?
Encryption options	Many people do not have universal encryption (a standard e-mail program and a public-private key pair) available to them.	• Encrypted e-mail can be offered to the patient. • Should patients have the ability to waive any encryption requirement?
Access to e-mail	Not all patients are able to use e-mail, and permitting patients to communicate with their providers via e-mail may improve the access of some patients inequitably. (11) These barriers will probably dissolve over time as computers and Internet access become less expensive, as public access to the Internet through FreeNets, kiosks, schools and public libraries becomes more ubiquitous, and as people take advantage of free computers and Internet access given in exchange for advertising and personal information. (12)	• Policies should address patients without access to e-mail.

Provider-Patient E-mail Issues	**Concerns**	**Policies Should Address**
Informed consent and agreement	Whenever health care providers subject patients to risk, it is important to disclose these risks. Although e-mail is not a procedure, it does expose patients to a small potential risk. In reality, this risk is probably less than that posed by many of the drugs administered and procedures performed by health care providers without a formal consent procedure. What is debatable is the form this consent should take. Written informed consent requires more	• It is prudent to include some sort of informed consent in an e-mail policy. • How formal or informal should consent be? • Should different consent agreements be maintained for each patient? • If a patient will not consent to the guidelines that are proposed, is it acceptable for a provider to refuse e-mail access for that patient?

	formality and is usually reserved for procedures associated with greater risk. Because of the time involved in obtaining a written informed consent, often an informed consent discussion will take place and a physician will document in the record that the discussion took place. It is impractical for a provider to maintain different agreements with each patient.	

A Strategy to Implement these Guidelines

One strategy used by the author (a primary care physician) is to provide his e-mail address as part of a rubber stamp on the back of his card. This stamp also contains a summary of the appropriate uses of e-mail and the fact that e-mail cannot be assumed to be confidential. The card and e-mail address is only given to patients once they agree to the guidelines on the card. He documents the patient's agreement with the guidelines and informed consent in the context of his clinical note.
These essential guidelines reproduced on his card are:

- That (unencrypted) e-mail is not entirely secure
- That employers may view e-mail sent using their work-provided e-mail system
- That e-mail should not be used for emergencies or time-sensitive issues
- That if a response is not timely the patient should escalate
- That patients should keep copies of e-mail they receive from the provider
- That the provider may (or will) keep copies of e-mail that a patient sends
- What the provider's policies are for routing of patient e-mail
- In addition, the physician's e-mail "signature" contains a statement about e-mail confidentiality, warnings about its use in emergencies, and his telephone number, fax number and address.

Web-based E-mail

One way to avoid many of the concerns about e-mail security is to incorporate a policy that e-mail between patients and providers take place only through a specially developed Web forms-based e-mail system. This system allows any patient with a Web browser to communicate with a health care organization through an encrypted private channel called a *secure sockets connection*. This connection is the technology that has enabled Web-based commerce to take place.

Although Web forms ensure encrypted, secure communication, they are not a practical technology for a small organization to utilize. It requires that the organization own a Web domain name, host a Web site, purchase a secure Web server, and have the expertise to develop and manage such a system.

From the patient and provider's point of view, such a system may not be as comfortable a communication medium as an e-mail program, and access to e-mail is often easier to obtain than rapid connections to the Web.

Organizations may choose to implement Web-based e-mail and encourage their patients and providers to use it. Organizations that provide only Web-based e-mail instead of providing effective policy and tools for the use of

regular e-mail may find that their providers and patients will choose to use regular e-mail anyway.

Provider-Provider E-mail Issues

Many of the issues discussed previously also pertain to provider-provider e-mail. Following are a few additional issues.

Policies should address:

- Should providers have a patient's general or specific permission to forward his/her e-mail to another provider?
- Should inter-provider communications be included in the patient record?
- Should copies of inter-provider communications be sent to the patient? This decision should be consistent with any existing policies about sharing written communication between providers with patients.
- Accurate identification of the patient is critical. It would be wise to include policy on patient identification numbers in the body or subject line of e-mail messages for inter-provider communications. Identification of a patient in inter-institutional communications is more difficult in the absence of a universal patient identifier.

Providers need to be aware of the issues of transmission of unencrypted e-mail and of their organizations' health information confidentiality policies.

Provider-Payer E-mail Issues

Many of the issues discussed previously also pertain to provider-payer e-mail. Following are a few regulatory issues.

Policies should address:

- There is a HCFA policy that states that authentication and encryption is required for transmission of all information about Medicare patients to and from HCFA. [13]
- There is a requirement for security standards in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that deals with transmission of patient-specific information to and from payers. [14]

Enforcement

Ultimately, policies need to be enforceable and enforced. Use of e-mail is a private activity that is frequently practiced. To enforce an e-mail policy, one must be able to monitor both the identities of the senders and recipients of e-mail and the content of their e-mail messages. Enforcement is thus quite difficult. If breaches are discovered, policy should address disciplinary consequences similar to those for breaches of patient confidentiality.

Legal Compliance

It is essential that organizations strive to uphold all relevant laws when creating policy. These laws include:

- Provider's duty to maintain confidentiality (see Alberts v. Devine, 395 Mass. 59, cert. denied, 474 U.S. 1014 (1985).

- Patient privacy - Massachusetts Privacy Act (M.G.L. c. 214, 1B.)
- HIPAA: Health Insurance Portability and Accountability Act of 1996 (PL 104-191, 110 Stat. 1988 (1996) (codified in portions of 29 U.S.C., 42 U.S.C. and 18 U.S.C.)

A variety of other state and federal laws, including constitutional, statutory, and common law relating to such issues as privacy, defamation, and harassment, discrimination and other labor law issues, including:

- Federal Privacy Act of 1974 (5 U.S.C. 552a)
- Federal Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510)
- Massachusetts Patients' Bill of Rights, 1979 (M.G.L. c.111, "70E)

Since the law is constantly evolving in this area, health care organizations may want to consult experienced counsel for help in developing written compliance policies. Management and employees should be made aware of these policies and reminded of their concomitant obligations.

Conclusions

E-mail is useful for communicating with and about patients. It is transforming relationships between patients and providers and improving communication among health care teams. Like any communication medium, e-mail is not perfect. It is useful in some situations and not useful in others, and thus it nicely complements other forms of communication. Because of its rapid and widespread adoption in society, the ultimate use of e-mail in patient care is unavoidable.

There are risks associated with the use of e-mail in patient care, just as there are risks associated with most things in medical care. The risks are more potential than real, but they do need to be acknowledged and understood by all parties using e-mail to transmit patient-specific information. Patients may be willing to take these risks for the added convenience that e-mail has to offer. It is essential that we learn to use e-mail safely and effectively. Although technology will evolve and many of the concerns expressed in this document will resolve themselves, we cannot wait and hope that patient-centered e-mail will go away until all the complex issues are worked out. Both patients and providers will be using e-mail either with or without our support. Appropriate guidelines for the use of e-mail in patient care are an important first step. These guidelines must evolve in accordance with advances in research and technology and with changes in legislation.

Endnotes

1. Sands DZ, Safran C, Slack WV, Bleich HL. "Electronic Mail Use in a Teaching Hospital." *Proc Symp Comput App Med Care*, 1993; 306 - 310.

2. Bielski V "Modern Malpractice." *Hippocrates* (November/December 1996)

3. Katz MH and Schroeder SA. "The sounds of the hospital. Paging patterns in three teaching hospitals." *NEJM* December 15, 1988; 319(24):1585 -1589.

4. Electronic Communications Privacy Act, 18 U.S.C. "" 2510-2522, 2701-2711.

5. Conklin, Charles B. MBA. "Risk Management Ramifications of E-Mail in a Hospital." *Forum* (September 1998): 8-9.

6. Spielberg, Alissa R., JD, MPH. "On Call and Online: Sociohistorical, Legal, and Ethical Implications of E-Mail for the Patient-Physician Relationship." *JAMA* 280, no. 15 (October 1998): 1353-59.

7. E.g., Smith v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); Bourke v. Nissan Motor Corp., No. B068705 (Cal.Ct. App. 7/26/93, unreported).

8. Cavanaugh MF. "Workplace Privacy in an Era of New Technologies." *Messaging Magazine* (May/June 1996)

9. *Smith vs. Pillsbury Co*, 914 F Supp 97 (ED Pa 1996)

10. Borowitz SM and Wyatt JC. "The Origin, Content, and Workload of E-mail Consultations." *JAMA* (October 21, 1998; 280;15): 1321 - 1324.

11. Mandl KD, Kohane IS, Brandt AM. "Electronic Patient-Physician Communication: Problems and Promise." *Annals of Internal Medicine* (September 15, 1998; 129;6): 495 - 500.

12. http://www.free-pc.com

13. Health Care Financing Administration. "Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and other Sensitive HCFA Information" (Washington, D.C.: HCFA, November 24, 1998) http://www.hcfa.gov/security/isecplcy.htm

14. Notice of Proposed Rule Making for Security and Electronic Signature Standards. http://aspe.os.dhhs.gov/admnsimp (Subpart C of 45 CFR 142.102 would secure health information used in any electronic transmission or stored format. Health plans would be required to accept and apply the security standard to all individual health care information electronically maintained or transmitted.)

Additional information

Additional information about patient-provider e-mail and guideline proposals are available from the American Medical Informatics Association