Provider-Patient E-mail: With Benefits Come Risks

Save to myBoK

by Dixie B. Baker, PhD

If you've ever played phone tag with your doctor, you can appreciate the benefits of e-mail. But for all its advantages, provider-patient e-mail is not without challenges. Here's how to protect your organization.

The majority of Americans now consider e-mail and instant messaging preferred means of communications, and nearly all (90 percent according to a 2002 survey) would like to be able to use e-mail to communicate with their physicians.[1] However, physicians are less receptive to provider-patient e-mail exchanges.

A 2001 survey reported that while 93 percent of physicians used the Internet, only 14 percent used e-mail to communicate with patients.[2] This survey and others have identified a variety of concerns that impede e-mail communications between providers and their patients, including:[3,4,5]

- threats to patient privacy/noncompliance with regulations
- potential malpractice liability
- may disturb the balance between physicians' traditional role as caregivers and patients' desire to participate in decision making regarding their care
- may widen social disparities in healthcare outcomes
- may create barriers to access in healthcare
- patients may use e-mail for urgent needs, resulting in potential harm to themselves
- providers may use e-mail inappropriately
- providers may be overwhelmed by the volume and length of messages
- providers may not be reimbursed for e-mail exchanges with patients

Despite these concerns, e-mail communication between providers and patients offers both convenience and quality benefits. For patients, e-mail can improve accessibility to information and care, increase satisfaction, and enable them to be more involved in their own care. For physicians, e-mail can enrich the provider-patient relationship, create self-documenting electronic records of interchanges, and enable more effective time management. However, with these benefits come risks that need to be understood and addressed.

Below, we'll take a closer look at how e-mail works and the risks inherent to this method of communication. Then we'll explore how to mitigate these risks through policy and technology.

How E-mail Works

Identifying the risks associated with physician-patient e-mail requires a basic understanding of the enabling technology. "E-mail Protocols," below, depicts graphically how an e-mail message is transmitted from the sender's screen to the recipient's desktop.

Internet Protocols

Wires and radio signals comprise the physical network that gets e-mail from one place to another. As a "network of networks," the Internet consists of various physical networks joined together through connection points called "nodes." An Internet node is simply a computer that has announced that it can be used as a sort of way station that helps Internet traffic get to its destination.

Internet Protocol (IP) enables the nodes to figure out where to send the traffic. IP breaks the e-mail into pieces and stores each piece in a packet. A packet is like a postcard in that the name and address of the recipient are stored in a specific section (called the "header"), and the message is stored in another specific section (called the "data field"). IP breaks a message into multiple postcards. And like a postcard, both the header and the data field can be read by—and changed by—whoever handles it on its way to the addressee.

Each node looks at each packet header and then sends the packet on to a node that will get it closer to the destination domain, which is the part of the e-mail address that follows the @ sign. IP is a "best effort" protocol whose sole objective is to deliver a packet to its intended destination. As such, it provides no service guarantees: no protection of the packet's content, no assurance that a message actually came from whom it claims to be from, no guaranteed delivery, and no verification that the content of the message received is identical to what the sender wrote.

Each individual packet may travel over a different route to get to the same destination, so the Transaction Control Protocol (TCP) serves as the organizer by making sure all the packets have arrived and are put into the right order at their destination. Once the packets are back in order at their destination domain, the Simple Mail Transfer Protocol (SMTP) is used to direct it to the e-mail server.

E-mail Server

The e-mail server listens for incoming and outgoing messages on designated ports. When it detects an incoming message, it searches for an e-mail account for the intended recipient, formats the message, and appends it to the message file associated with the addressee named before the @ sign. When it detects an outbound message, it appends the sequenced packets to a queue of mail destined for a particular user within a specified domain.

The server uses one of two protocols to deliver e-mail to the client: the Post Office Protocol (POP) or the Internet Mail Access Protocol (IMAP).[6,7] The primary difference between the two is that POP simply accumulates e-mail and when the client asks for it, downloads everything it has accumulated. IMAP, on the other hand, is more sophisticated. It parses the e-mail file into individual messages and maintains consistency between the server and the client. Both protocols copy e-mail to the user's desktop, where it can be viewed by passersby and anyone with access to the e-mail client.

E-mail Client

The e-mail client is the software that enables the user to read and compose e-mail messages. It may reside on the same machine as the server, on the user's private workstation, or be an extension of the Web browser. The client is responsible for both delivering e-mail from the server to the user and for taking messages composed by the user and delivering them to the server via SMTP. When the user wants to review her e-mail, her client connects to the server and asks for her e-mail file. If the server uses POP, it downloads the entire file to the user's machine. Using IMAP, the client receives a list of all message headers, and the user can select which messages to download.

The user can also "delete" e-mail on the client or server. However, deleting e-mail does not result in totally expunging the information from the client or server. In some e-mail software, deleting a message simply moves it from an inbox folder to a deleted folder. Also, when computer systems delete information from a hard disk, the image remains until it is overwritten.

A New Level of Risk

HIPAA does not directly address e-mail in any of its standards. However, because e-mail between physicians and patients involves protected health information (PHI) in electronic form, both the privacy and security rules apply.[8,9] Central to the security rule is the concept of risk assessment, which serves as the basis for selecting what safeguards to implement.

Risk assessment involves identifying vulnerabilities and then estimating the probability that a threat will exploit those vulnerabilities to cause harm. This probability is known as risk. "Risks Associated with E-mail," below, summarizes the vulnerabilities associated with this method of communication, identifies potential threats that could exploit these vulnerabilities, and describes the associated risk.

Mitigating Risk through Policy

The risks identified in "Risks Associated with E-mail" can be mitigated through the enforcement of policies relating to three broad areas:

- Quality of care: policy addressing risks that pose potential harm to the patient
- Patient privacy: policy addressing risks to the confidentiality of PHI
- Legal liability: policy addressing risks relating to potential malpractice law suits

A number of professional organizations have set forth policy relating to e-mail, including the American Medical Association, the American Medical Informatics Association, and the non-profit physician-outreach program HealthyE-mail.[10,11,12,13] The policy specified here draws from published policies that address the risks identified above and incorporates privacy policy contained in the HIPAA privacy rule. These policies can be enforced through various combinations of administrative practices and procedures, sanctions, physical protections, and technology, so we have attempted to use wording that avoids dictating implementation strategy.

Quality of Care

To mitigate risks that pose potential harm to patients:

- Patients and providers shall exchange e-mail only through a practice-authorized e-mail service
- Patients sending e-mail to providers shall use a standard, structured format with the following fields completed: patient's name, identification number (if applicable), subject (selected from list of subjects approved for e-mail discussion), sensitivity level (selected from list of sensitivity indicators), criticality level (selected from list of criticality descriptors), and time within which response is needed (selected from list of options)
- E-mail shall not be used for emergencies or time-critical situations
- E-mail shall not be used to discuss highly sensitive subject matter, such as HIV test results or mental health issues
- E-mail shall not be used to discuss complex subjects. If a long explanation is needed, or if an e-mail string with the patient is prolonged, a telephone call or scheduled face-to-face discussion shall be used
- Upon receipt of an e-mail message from a patient, a response shall immediately be sent to the sender acknowledging receipt and stating the practice's turn-around policy for e-mail
- Upon completion of the actions required by the subject of a patient's e-mail, the patient shall be notified
- A prioritization scheme for e-mail messages shall be established, with expected turnaround times
- For periods of absence in which e-mail will not be serviced, upon receipt of e-mail, an out-of-the-office reply shall be sent indicating the estimated date of return and instructions on whom to contact for immediate assistance
- Messages containing important medical information or advice shall include a request for a reply from the patient and shall be flagged as "unresolved" until an acknowledgment is received
- An electronic and/or paper copy of every e-mail message between the provider and the patient shall be retained in the patient's record, along with confirmation of receipt and any response
- E-mail administration practices and procedures shall be clearly documented, with responsibility and accountability clearly established

Patient Privacy

To mitigate risks that threaten the confidentiality of PHI:

- Display devices used for reviewing e-mail shall be physically protected to discourage casual viewing by unauthorized individuals
- All e-mail containing PHI, including all e-mail between physicians and patients, shall be digitally signed and encrypted for transmission
- E-mail messages addressed to a group of patients shall be sent such that each recipient sees only his or her name (for example, put physician's name in "To" field and all patients' names in "Bcc" field)
- Each individual user (patient or physician) shall be uniquely identified and authenticated prior to sending or reviewing any e-mail
- E-mail may be forwarded only to e-mail addresses authorized for the purposes of treatment, payment, or healthcare operations and to e-mail addresses for which the patient has given his or her informed, written consent
- Patients' e-mail addresses shall not be used for marketing purposes

- Each individual user shall be advised of her or his responsibility for protecting access to provider-patient e-mail, both within and outside the business office. The advisement shall include both the protection of authentication data (for example, passwords) and the protection of displayed information (on a monitor or hand-held device)
- All patient-identifiable e-mail sent over wired and wireless networks shall be encrypted
- Patients and providers shall be advised to take precautions to ensure that their e-mail is addressed only to the person(s) they intend. This includes double-checking fields prior to sending a message and making sure the e-mail client software did not automatically fill in an incorrect address after the first few characters were typed
- Following a predefined period of inactivity, the user's e-mail session shall automatically be deactivated via automatic logoff or locked screen and re-authentication shall be required to reactivate the e-mail session
- The e-mail system shall be backed up regularly, and the back-up media shall be protected from unauthorized access

Legal Liability

To mitigate risks relating to potential malpractice law suits:

- E-mail policy and guidelines shall be made available to patients and staff in both paper and electronic forms
- Prior to communicating with a patient via e-mail, the patient's written, informed consent shall be obtained, and a copy provided to the patient. The standard informed-consent agreement shall:
    - articulate guidelines governing the types of transactions (such as prescription refills and appointment scheduling) and sensitivity of subject matter (for example, allergy test results versus HIV test results) that can appropriately be addressed via e-mail
    - advise the patient of privacy risks associated with the use of e-mail
    - describe the organization's privacy policy and the security features in place to protect patient e-mail
    - explain the patient's own responsibilities with respect to the use of e-mail; identify the individuals who may have access to the patient's e-mail
    - inform the patient that e-mail will be retained in his or her record
    - hold the healthcare organization harmless for information loss due to technical failures
- Patients shall be informed that failure to follow e-mail policy and procedures will result in termination of e-mail communications with them
- An approved list of e-mail addresses for patients who have given their written consent for e-mail exchanges shall be maintained, and physicians shall send e-mail only to addresses on this list
- E-mail addressed to physicians shall be screened, sorted, prioritized, and escalated in accordance with the predefined rules established for the practice
- All e-mail between the provider and the patient shall be archived and maintained in accordance with applicable state laws regarding medical record retention
- A standard block of text shall be appended to each e-mail message sent to patients. This text shall contain the physician's full name, contact information, a warning that the e-mail is confidential and intended only for the addressee, and reminders about security and the importance of using alternative forms of communication for emergencies

Enforcing Policy through Technology

A complete technology solution to enforce these e-mail policies would:

1. Authenticate each user prior to allowing them to read or send e-mail
2. Ensure that each user can view only those e-mail messages intended for him or her
3. Automatically send an acknowledgment of receipt to each message received
4. Enable the provider to configure an automatic out-of-the-office reply for use during extended periods of absence
5. Automatically append a standard block of text to each e-mail message sent to a patient
6. Digitally sign the message with the sender's private key
7. Validate the sender's key upon opening of an e-mail message
8. Encrypt messages for transmission
9. Automatically label all e-mail "Confidential"
10. Present a template containing pre-defined fields, with those required fields highlighted

11. Ensure that all required fields were completed before sending the message
12. Scan the text of each constructed message prior to sending it to detect key words and phrases indicative of sensitive subject matter, such as “HIV” and “abortion,” and display a reminder that e-mail is not appropriate for extremely sensitive exchanges
13. Automatically screen incoming e-mail, sort in accordance with established priority rules, and escalate critical messages
14. Automatically store a copy of each e-mail message and response in the patient’s electronic record
15. Detect multiple addressees in the “To” field and suggest that the sender use the “Bcc” to prevent individual addressees from seeing other addressees’ names
16. Automatically terminate the e-mail session after a period of inactivity
17. Send e-mail only to addresses stored in the electronic address book, and allow only authorized users to add names to the address book

Many common e-mail programs provide capabilities to address the first five features above, and most can be extended to provide digital signatures and encryption. Some e-mail programs also provide features to label messages and to develop templates. However, not all patients will use the same e-mail program, and different e-mail systems may not be seamlessly interoperable.

The most straightforward approach for attaining the comprehensive technology solution that incorporates all 17 features listed above is to implement a server-based e-mail solution in which physicians and patients exchange e-mail messages within a secured, centrally managed, and controlled Web environment.

With this approach, providers and patients would authenticate themselves to the e-mail service, most likely using passwords or some combination of a password and a private encryption key. Private keys could be distributed to the users and stored encrypted on the users’ hard disks or on a removable medium, with the password used to decrypt the key when it is needed for authentication or digital signature. Users would connect through their Web browser over Secure Sockets Layer (SSL) to view or construct e-mail on the server, where it would be protected in accordance with the practice’s security policy. A Web-based e-mail implementation would enable enforcement of e-mail structure to support electronic screening, sorting, and prioritizing of incoming e-mail, as well as the centralized management of patient authorizations. In addition, this solution could detect whether e-mail has been read and warn when it is not read after a specified period of time.

E-mail offers a familiar and convenient communication channel between patients and their physicians and can be used to enrich the provider-patient relationship. However, a number of risks associated with e-mail technology and with e-mail usage need to be effectively managed to protect the patient’s privacy and safety, and the physician’s practice. Fortunately, well-documented policies and thoughtful technology selection can provide a strong foundation for this valuable healthcare benefit.

Risks Associated with E-Mail

Vulnerability	Threat	Risk
Packet contents may be viewed at any node	Individual with access to node through which packet passes; IP “sniffer” software	• PHI is disclosed to unauthorized person
Packet contents may be modified at any node	Individual with access to node through which packet passes; IP “sniffer” software	• Message content is modified in transit
E-mail is asynchronous, and receipt is not acknowledged	Technical problem or unavailable recipient	• E-mail is not received or is not read by the intended recipient

No means of authenticating identity of sender or receiver	Individual masquerading as physician or patient	• Patient receives alarming e-mail forged bysomeone masquerading as her physician • Physician's e-mail sent to patient is read by someone else, resulting in unauthorized disclosure of PHI
IP provides no quality-of-service guarantees	Node through which packet passes	• Transmission delays cause recipient to receive critical message too late for its recommendations to be effective
E-mail resides on server until it is downloaded to client (POP) or deleted (IMAP)	E-mail administrator	• PHI is disclosed to unauthorized person • Patient reads physician's e-mail too late for its recommendations to be effective
E-mail messages "deleted" by client or server may remain after deletion	Other user with access to system from which e-mail was "deleted"	• PHI is disclosed to unauthorized person
Many e-mail addresses are similar, and some client software automatically completes an address after the first few letters	Physician mistyping e-mail address; client completing address incorrectly	• Private e-mail is sent to individual with e-mail address similar to that of patient, resulting in unauthorized disclosure of PHI
All addresses in "To" field are viewable to all recipients	Physician sending "form" e-mail to group of patients	• Identities (PHI) of all patients to which message is sent are disclosed
E-mail leaves indelible record of communication	Plaintiff's attorneys in malpractice law suit	• E-mail provides incriminating evidence of communication between patient and physician
Criticality of e-mail message sent to provider is not intuitively obvious	Patient or family member who does not realize criticality of medical situation	• Needed care is delayed or denied due to lack of attention to e-mail indicating a critical condition
Unpredictability of responses from patients receiving medical results, observations, or advice to medical advisements	Provider with insufficient information or poor judgment regarding patient's responses	• Patient overreacts to lab report or physician's message, resulting in panic or undue stress until patient is able to personally communicate with physician • Patient misunderstands physician's instructions conveyed in e-mail and responds inappropriately
E-mail accessibility encourages frequent and long	Chronic e-mailer	• Critical condition of chronic e-mailer is given insufficient attention

e-mail messages from some patients		
Internet access is not equally available to everyone	Lack of availability of home computer	• Patient lacking convenient access to Internet receives physician's e-mail too late for its recommendations to be effective
E-mail is not integrated with clinical repository	Lack of interface between e-mail server and clinical data repository; lack of standardization of data entered via e-mail	• Important information conveyed via e-mail is not factored into physician's decision making

E-mail Protocols

Notes

1. Taylor, Humphrey and Robert Leitman, eds. "Patient/ Physician Online Communication: Many Patients Want It, Would Pay For It, and It Would Influence Their Choice of Doctors and Health Plans." *Health Care News* 2, no. 8 (April 10, 2002). Available at www.harrisinteractive.com.
2. Taylor, Humphrey and Robert Leitman, eds. "New Data Show Internet, Website, and E-mail Usage by Physicians All Increasing." *Health Care News* 1, no. 8 (February 26, 2001). Available at www.harrisinteractive.com.
3. Landro, L. "Doctors Fear E-mail's Effect on Care, Privacy, Liability." *Wall Street Journal* (June 2, 2003).
4. "Patient/Physician Online Communication: Many Patients Want It, Would Pay For It, and It Would Influence Their Choice of Doctors and Health Plans."
5. Mandl, Kenneth D., Isaac S. Kohane, and Allen M. Brandt. "Electronic Patient-Physician Communication: Problems and Promise." *Annals of Internal Medicine* 129, no. 6 (1998). Available online at www.annals.org/cgi/content/full/129/6/495.
6. Myers, J. and A. Rose. "Post Office Protocol—Version 3." Network Working Group, Internet Engineering Task Force, May 1996. Available online at www.ietf.org/rfc/rfc1939.txt.
7. Crispin, M. "Internet Mail Access Protocol—Version 4rev1." Network Working Group, Internet Engineering Task Force, December 1996. Available online at www.ietf.org/rfc/rfc2060.txt.
8. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157. (August 14, 2002.) Available online at http://aspe.hhs.gov/admnsimp.
9. "Health Insurance Reform; Security Standards; Final Rule." 45 CFR Parts 160, 162, and 164. *Federal Register* 68, no. 34 (February 20, 2003). Available online at http://aspe.hhs.gov/admnsimp.
10. "Guidelines for Physician-Patient Electronic Communications." American Medical Association (May 16, 2003). Available online at http://www.ama-assn.org/ama/pub/category/2386.html.
11. The AMA Council on Ethical and Judicial Affairs also has established an ethics policy regarding the use of e-mail with patients.
12. Kane, Beverly and Daniel Z. Sands. "Guidelines for the Clinical Use of Electronic Mail with Patients." *Journal of the American Medical Informatics Association* 5, no. 1 (1998): 104-111. Available online at www.amia.org/pubs/other/email_guidelines.html.
13. "E-mail and the Clinical Practice." *HealthyE-mail*. (February 2003). Available online at www.healthyemail.org/docs/PhysicianEmailGuide.pdf.

***Dixie Baker** (DIXIE.B.BAKER@saic.com) is corporate vice president for technology and chief technology officer for enterprise and health solutions at Science Applications International Corporation.*

Article citation:
Baker, Dixie B. "Provider-Patient E-mail: With Benefits Come Risks." *Journal of AHIMA* 74, no.8 (September 2003): 22-29.