AMERICAN ACADEMY OF PEDIATRICS

CLINICAL REPORT
Guidance for the Clinician in Rendering Pediatric Care

Robert S. Gerstle, MD, and the Task Force on Medical Informatics

E-mail Communication Between Pediatricians and Their Patients

ABSTRACT. This report addresses specific e-mail patient communication issues relevant to pediatricians and their appropriate use of e-mail in the office setting. The report briefly reviews: 1) e-mail privacy and security concerns; 2) e-mail in the office environment; 3) the legal status of e-mail; and 4) available e-mail technologic solutions. ***Pediatrics*** **2004;114:317–321;** ***electronic communications, health care delivery, medical liability, e-mail, pediatrics.***

ABBREVIATIONS. HIPAA, Health Insurance Portability and Accountability Act; PHI, protected health information.

The American Academy of Pediatrics Periodic Survey of Fellows No. 51 documented that of the 1616 active US members reporting from October 2001 to February 2002, 14% already use e-mail to communicate with patients. Reasons cited for using e-mail included managing requests for prescription refills (54%), communicating test results (41%), and scheduling appointments (37%). Reasons for not using e-mail to communicate with patients included lack of physician time (52%), lack of office staff time (42%), concerns about privacy or confidentiality (45%), lack of interest in communicating via e-mail (38%), and too few patients with e-mail (34%).[1] The volume of e-mail sent daily in the United States was expected to exceed 9 billion messages in 2003.[2] A Harris Interactive survey reported in April 2002 that "about 90% of US adults who use the Internet say they would like to communicate with their physicians online . . . ."[3] The study went on to report, "56% said that ability to communicate with their physician online would help influence their choice of physician."

The popularity of e-mail is attributable to some of its unique characteristics, namely its ability to allow asynchronous communication and rapid message transfer, making it a hybrid of the telephone and the written letter.[4] As it is used, e-mail is a more informal means of communication than the letter, but more rapidly transmitted. Like a letter, it can be sent or read by the recipient at convenient times, avoiding "telephone tag." In addition, it is "self-documenting," providing a lasting copy for future reference. Thus, it is no surprise that pediatric patients and their families share the desire to use e-mail to communicate with their pediatricians.[3–5] E-mail would seem to offer physicians and patients obvious benefits for facilitating communication. Therefore, it may seem somewhat surprising that there has been relatively slow adoption of e-mail as a patient communication tool by pediatricians and other physicians.[4] There are many reasons for this, including but not limited to concerns about maintaining the confidentiality of e-mail, physician concerns about the potential volume of e-mail correspondence, and potential legal issues.[1,5]

BACKGROUND: E-MAIL TECHNOLOGY

The transmission of e-mail messages requires: 1) access to a global network of linked computers, called the Internet; 2) the existence of an addressing system that enables messages to be routed through that network of computers to their correct destinations; and 3) programs that split messages into standard-sized "pieces," pack them into electronic "envelopes" or packets that have address information for routing each packet, and reassemble the message at the intended destination.

By design, the Internet is a very robust communication system with an architecture that was structured to maintain communication in case of national disasters that might result in the destruction of significant amounts of the national communications network (such as in the case of nuclear war). Messages transmitted across the Internet are not normally encrypted; nor is there typically authentication of author identity. Lack of encryption allows those with access to the Internet network to intercept, read, or potentially alter messages as they pass to their final destinations. These risks are not unique to e-mail. Telephones can be tapped (legally or illegally); scanners can monitor portable telephone communications; traditional mail can be intercepted, read, or altered, and letters can be forged. Despite potential confidentiality and security risks, it seems on the basis of volume alone that most people are comfortable using e-mail, particularly for relatively trivial or mundane communication needs. The perceived benefits of this fast, asynchronous, and relatively inexpensive form of communication appear to outweigh the risks to most users.

The guidance in this report does not indicate an exclusive course of treatment or serve as a standard of medical care. Variations, taking into account individual circumstances, may be appropriate.

PRIVACY AND SECURITY RISKS

Physicians have special ethical and legal obligations to maintain the privacy and confidentiality of their communications with and regarding patients. Additionally, pediatricians and others who provide medical services to children and adolescents have special burdens and responsibilities by the nature of their patient population.[6,7] E-mail communication with patients adds complexity and responsibilities for the pediatrician, the office staff, and the patient and patient's family.

Pediatricians have the legal responsibility, whenever health information is requested by or communicated to an individual, to ensure that: 1) the individual has a legitimate right to release or gain access to that information before releasing or communicating that information by letter, by phone, in person, or by e-mail; 2) the information is directed only to those having a right to receive it; and 3) the information is accurately transmitted and received. These are the requirements to ensure the authenticity, confidentiality, and integrity of information exchange.[8,9]

Authenticity refers to a recipient's ability to positively know the identity of an individual sending a communication.[10] Anyone can send e-mail with virtually anyone's name attached to it. The inability of e-mail to provide methods of authentication presents a significant risk to patients and physicians. E-mail authentication has been one of the more difficult issues to address when using e-mail for medical communication. Two general solutions to the authentication problem, digital certificates and secure networks, will be discussed briefly later in this report.

Confidentiality refers to the need to protect information from those who have no legitimate right to the information presented.[11] Risks to patient confidentiality occur when multiple individuals (eg, family members) share the same e-mail address, when access passwords are not used or are not kept secured, when computers are left on and unattended without logging out of e-mail, or when e-mail at work or at school is used for personal communication. Using e-mail on systems that belong to employers, other organizations, or schools presents particular problems. Many e-mail users do not know that most organizations and companies, as policy, consider organizational e-mail to be their property and reserve the right to read e-mail on their systems. Another threat to confidentiality results from the ease with which e-mail messages can be misaddressed and erroneously sent to unintended recipients, instantaneously broadcast to multiple recipients, or forwarded by others to unintended recipients.

Integrity of message transmission refers to having absolute knowledge that the message received was unaltered and identical to the one transmitted and that the message was sent and received by the appropriate person.[11] Because e-mail messages can be intercepted, especially by hackers who break into an e-mail server but also by individuals who might gain access to another's personal electronic mailbox, there may be justifiable concern about integrity of messages. Of more concern is that a message sent to one individual might be altered by the recipient. The altered message, its intent perhaps drastically changed, might then be forwarded to another person.

E-MAIL IN THE PHYSICIAN OFFICE ENVIRONMENT

Office e-mail and confidentiality policies, procedures, and processes need to be in place before e-mail with patients can successfully, safely, and effectively be used in the office. Merely distributing or advertising a practice's e-mail address to patients may have unintended consequences. This address will rapidly become quite public, resulting in the office receiving a variety of unsolicited e-mail. A major concern is that individuals who are not current office patients may e-mail the office with medical questions. Office processes may get mired with the volume of e-mail received. The practice needs a way to determine which messages are from "legitimate" or established patients or families and needs to decide whether it will respond to queries from nonpatients. Distinguishing which messages are from current patients from those that are not can be difficult. E-mail address names may be aliases (eg, Superstud2) or common or nonunique names (eg, David Miller or Jose Rivera). Pediatric offices typically identify patients by the child's name but may have problems identifying e-mail from a parent, particularly if the message does not reference the child's name and birth date. Incorporating structured e-mail forms that require specific patient identifying information (eg, first and last name, date of birth, and practice identification or Social Security number) to be completed as part of the message helps simplify patient identification. In addition, the use of passwords as a means of identification and access can diminish the risk of outside or inappropriate access to communications.

Another concern beyond identification is that of e-mail attachments. E-mail attachments can cause a variety of problems, including the transmission of computer viruses (potentially paralyzing the computer system), the use of excessive memory, the need to read and print messages and attached documents for inclusion in patient records (using staff resources), or the need for versions of software that are not available on the office system. To rectify this issue, pediatric offices can consider restricting the use of attachments as part of patient messages. Attachments might be restricted to reports or attachments from professional sources, such as other physician offices, emergency departments, and hospital medical records departments. Having the ability to control which users may append attachments can lend a lot of flexibility to an e-mail system.

Occasionally, situations occur in which an office may want to have the ability to block the receipt of e-mail from certain individuals. E-mail systems that allow the office the ability to inactivate passwords or block e-mail from specific individuals can effectively restrict e-mail system access for selected patients by the office when necessary.

It is very important for practices to set realistic expectations for e-mail and communicate those expectations to families. Patients must understand what the office considers a reasonable response time for nonurgent messages and must understand that emergency communication is appropriately handled by telephone, not by e-mail. Communications that are usually appropriate for e-mail include routine appointment requests, billing questions, routine prescription refill requests, provision of follow-up information, and chronic disease management questions. By providing patients with office e-mail policies in written form before they receive an e-mail password, posting the policies on the practice Web site, and verbally reinforcing these policies, pediatricians and their staffs can help patients to understand and adhere to the appropriate use of e-mail.

There are other considerations the pediatrician needs to address before providing pediatric patients with e-mail access to the office. Policies can address the age at which pediatric patients can begin to send e-mail to the office themselves. Will children and parents receive the same brochures and sign the same consents (or assents)? Will parental permission be required before a child can receive a password to access office e-mail? Although there are not necessarily any right or wrong strategies, patients and their parents must know and understand office practices and policies.

Patients typically desire to communicate by e-mail with their physician's office to schedule appointments, refill prescriptions, resolve billing questions, request referrals, obtain test results, get forms or immunization records completed, ask nonurgent medical questions, or provide medical follow-up. Most of these tasks can be delegated to an appropriate office staff member. Patients must understand who in the office will read and triage e-mail as well as the limits to privacy that messages will have in the office. Patients must know when, for example, messages addressed to a particular individual in the office, even about personal matters, may be first subjected to clerical or nurse review. E-mail systems that can automatically triage messages to the appropriate office staff member, depending on the type of message, can improve efficiency and patient confidentiality. Patients can be informed that by restricting e-mail messages to one issue per message, message triage efficiency and patient confidentiality might be enhanced. The office also needs to have policies and processes to address messages that arrive when a pediatrician or designated office staff person is unavailable or has elected not to have the messages forwarded to them, and to address e-mail received on weekends, holidays, or whenever the office is closed. Routine policies can be incorporated into a patient e-mail brochure, and the policy can be reinforced using the "auto reply" feature included in most e-mail software, stating when action will be taken on messages and telling the patient to call the office for more urgent matters. Copies of e-mail messages with responses can be incorporated into patient charts. Patients can be advised to retain copies of e-mail sent by the office to avoid their forgetting or misunderstanding the intent of messages.

A well-constructed patient brochure outlining office e-mail policies and the appropriate use of e-mail will help control patient expectations and prevent misuse of e-mail by patients. Although some offices may require patients to sign a consent form allowing e-mail communication, it is more important that patients and parents clearly understand the differences among, and appropriate use of, each available form of communication. It is a good practice to document that each patient has been provided with written information that addresses the appropriate use of e-mail and office policies and procedures that support e-mail. This information can be provided before office e-mail addresses or access passwords are given to patients.

Drawing an analogy to telephone communications, e-mail communication is another way to enhance patient communication and satisfaction and to build goodwill. Just as there are no regulations that preclude charging patients for telephone advice, except as may be contained in insurance contracts, there are no restrictions on charging patients for advice rendered by e-mail. Some insurers have begun to consider e-mail an important part of chronic disease management and have started to selectively reimburse physicians for e-mail communication related to disease management.[12,13] More plans are expected to begin reimbursing clinicians for online consultation for both acute and chronic conditions. Because e-mail self-documents, it can provide the evidence of medical work that telephonic communication does not offer. Thus, insurers have been more willing to consider reimbursement for e-mail interactions. *Current Procedural Terminology*[14] codes for care plan oversight (99374-99380) already exist and are reimbursable under some insurance plans.[15] Case management services telephone calls (99371-99373) presently are restricted to telephone use but might be broadened in the future to include e-mail services.

LEGAL STATUS OF E-MAIL IN HEALTH CARE

The Health Insurance Portability and Accountability Act (HIPAA)[8,9] privacy and security regulations apply to e-mail communications that contain a patient's protected health information (PHI), as defined in HIPAA privacy regulations.[16] HIPAA requires encryption of messages when sending PHI over the Internet. If the pediatrician is using a third party to manage the e-mail system, HIPAA privacy regulations require a written business associate agreement with the service provider. HIPAA privacy regulations require that physician offices provide each of their patients or patient's families with an outline of the office's privacy practices. Final HIPAA security regulations[9] released on February 20, 2003, require physician office networks to have appropriate protection (firewalls and physical security) to prevent unauthorized individuals from gaining access to clinical e-mail or medical records, and to have appropriate safeguards to prevent the loss or unauthorized access to or distribution of PHI. Privacy regulations under HIPAA also require the ability to provide for author and user authentication for e-mail transmissions.

Just as for telemedicine, issues related to medical licensing and jurisdiction can be raised when communicating with patients and providing patient care or advice across state lines by e-mail. Although it is unlikely the pediatrician would be in jeopardy of prosecution for practicing medicine without a license by giving medical advice to an established patient via e-mail, it is important that pediatricians check their state's law on this issue. Some states have begun to address this issue in their state medical practice legislation, with the possibility of requiring a state medical license for such transactions.

There can also be medical liability risks related to providing "medical care" by e-mail or Internet communication. Before medical liability can exist, one must demonstrate that a patient-physician relationship has been formed. The establishment of the patient-physician relationship, or "duty," has not been well clarified when using e-mail or the Internet exclusively to provide advice in the absence of any physical contact. Arguably, an analogy can be drawn to the situation in which a physician provides general information on a local radio or television broadcast. In such cases, in which information is general in nature and not meant to diagnose or treat a specific individual, there is no relationship or duty established. Although case law has not been well established, there have been concerns raised as to whether a patient-provider relationship would be initiated when advice is given in an online forum ("bulletin board" or "chat room"). However, in cases in which there is a previous patient-physician relationship or in which a Web site is created to solicit patient queries, the risk of medical liability is greater.

Failure to meet patients' service expectations or follow one's own office policies and procedures can result in liability. The situation in which a physician fails to respond in an appropriate time frame to a patient e-mail, resulting in an adverse outcome, for example, might present a liability risk, emphasizing the need to educate patients about the appropriate use of e-mail and about appropriate response time expectations. Patients must be instructed and must understand when it is appropriate to escalate queries by telephoning the office directly. Although e-mail is widely used, neither the legal nor medical liability communities have significant precedents for dealing with potential e-mail communication risks. Pediatricians should monitor for the development of such precedents in the future.

E-MAIL TECHNOLOGIC SOLUTIONS

There are two commercially available solutions to the problem of providing authenticated, confidential, secure e-mail: secure servers or digital signatures.[17] Each of these approaches affords remedies for authentication of identities and facilitates secure communication with patients. No system, however, is perfect. Any system depends on patients and providers recognizing their responsibilities to keep passwords private and secure and to log off of systems properly when leaving computers unattended.

The secure server solution is analogous to doing banking online. The pediatrician's office must initially authenticate the identity of the patient, such as at the time of an office visit, and provide a sign-on code and temporary password specific to that individual. When the patient logs on to the system for the first time, he or she then changes the temporary password to a new and confidential one known only to the user. When a message is sent to that patient's system mailbox by the office, a secondary nonsecured notice is sent to the patient's identified home e-mail account alerting the patient to log on to his or her secure mailbox on the system. Logging on is accomplished securely using the patient's confidential password and via the Web browser's secure socket layer. Secure socket layer transmission across the Internet is encrypted between the mail server and the patient. Only the individual with the password to that account has access to it. From the secure mailbox, patients can also securely send messages back to the pediatric office. Such messages reside on the server, and the office logs on to the mail system securely, as does the patient. In this type of system, unencrypted messages containing medical information never travel on the Internet.

Digital signatures rely on the use of "keys" to encode (encrypt) messages sent across the Internet. The sender of a message has a private key that is used for coding the message. The receiver has a complementary public key to decode the message, thus making it readable.[18] These keys are not physical devices but rather strings of random characters that are used in the mathematical encrypting algorithm. Authentication of identity occurs before a key is released to a user, and a certification authority handles management of public and private keys. Authentication can still be an issue depending on the identity control mechanisms used.[17,18] Presently, these systems are complex to administer and cumbersome to use. However, in the future, perhaps by using smart cards or biometric forms of authentication (eg, fingerprint readers), these systems may grow in popularity.

Commercially available e-mail systems can provide added value beyond simply the ability to transmit and receive e-mail. They can provide e-mail encryption, authentication, and password management; can facilitate automatic triaging of messages on the basis of message type; and can provide the ability to "auto-fax" prescriptions to pharmacies. Some systems can assign "rights" to certain users (such as to append attachments) or allow for associated business transactions (charges for communications) to be handled online. Costs of these systems can vary widely, but for a very modest cost, most offices can implement basic secured messaging.

CONCLUSION

Successful communication between patients and pediatricians is an essential element to providing quality care and maintaining patient satisfaction. Although under certain circumstances, only face-to-face communication is appropriate, there are other times when other forms of communication, including direct telephone contact, facsimile transmission, traditional mail, and now, e-mail would be appropriate—although they should not be considered interchangeable. Pediatricians and their patients must be aware of the risks, benefits, and limitations of any form of communication. E-mail is still an emerging vehicle for communication. Its ability to allow for the rapid asynchronous transmittal of messages and to "self-document" makes it particularly popular despite the potential confidentiality risks. These risks can be acceptably minimized with appropriate forethought and planning.

Task Force on Medical Informatics, 2001–2002
Edward M. Gotlieb, MD, Chairperson
Robert S. Gerstle, MD
Allan S. Lieberthal, MD
Richard N. Shiffman, MD
S. Andrew Spooner, MD, MS
Melvin S. Stern, MD

Staff
Aiysha Johnson, MA

REFERENCES

1. American Academy of Pediatrics, Division of Health Policy Research. *Periodic Survey of Fellows 51: Use of Computers and Other Technology, Executive Summary.* Elk Grove Village, IL: American Academy of Pediatrics; 2003
2. Walker J. The electronic records committee and state standards [slide presentation]. Columbus, OH: Ohio Historical Society; 2001. Available at: http://www.ohiohistory.org/resource/lgr/DeptofEd.ppt. Accessed August 9, 2003
3. Harris Interactive. Many patients willing to pay for online communication with their physicians [press release]. Rochester, NY: Harris Interactive; April 11, 2002. Available at: http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=446. Accessed August 9, 2003
4. Bauchner H, Adams W, Burstin H. You've got mail: issues in communicating with patients and their families by e-mail. *Pediatrics.* 2002;109:954–956
5. Kleiner KD, Akers R, Burke BL, Werner EJ. Parent and physician attitudes regarding electronic communication in pediatric practices. *Pediatrics.* 2002;109:740–744
6. American Academy of Pediatrics, Pediatric Practice Action Group and Task Force on Medical Informatics. Privacy protection of health information: patient rights and pediatrician responsibilities. *Pediatrics.* 1999;104:973–977
7. American Academy of Pediatrics. Confidentiality in adolescent health care. *AAP News. April* 1989:9.Available at: http://www.aap.org/policy/104.html. Accessed August 9, 2003
8. Department of Health and Human Services, Office for Civil Rights. Medical privacy—national standards to protect the privacy of personal health information. 45 CFR §160, 164 (2000). Available at: http://www.hhs.gov/ocr/hipaa/finalreg.html. Accessed August 9, 2003
9. Department of Health and Human Services. Health insurance reform: security standards: final rule. *Federal Register.* February 20, 2003. Available at: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf. Accessed August 9, 2003
10. Brooks P, Leyland P. Security: privacy, authenticity, and integrity. Available at: http://www.ac.uk.pgp.net/pgpnet/secemail/q4/node4.html. Accessed November 7, 2003
11. US Dept of Homeland Security. Critical infrastructure glossary of terms and acronyms. Available at: http://www.ciao.gov/ciao_document_library/glossary/C.htm. Accessed November 7, 2003
12. University of Illinois at Chicago, Division of Specialized Care for Children. Fee schedule for medical home services. Available at: http://internet.dscc.uic.edu/forms/medicalhome/0302.pdf. Accessed August 9, 2003
13. Bottom Line Medical Administrative Consultants, Inc. *Telephone Management: How Much Is Your Practice Losing?* Lake Wales, FL: Bottom Line Medical Administrative Consultants Inc; Available at: http://bottomlinemedicalconsultants.com/telephonemngmnt.html. Accessed August 9, 2003
14. American Medical Association. *CPT 2003: Standard Edition. Current Procedural Terminology.* Chicago, IL: American Medical Association; 2002
15. Appleby J. Insurers, doctors ponder implications of e-consultations. *USA Today. March 26,* 2001:1B, 5B
16. Health Insurance Portability and Accountability Act. Pub L No. 104-191 (1996)
17. Beer K. Secure messaging strategies for healthcare IT professionals. Available at: http://www.privacysecuritynetwork.com/healthnews/symposia/emailstrat.htm. Accessed November 7, 2003
18. VeriSign. What is a digital ID? Available at: shttps://digitalid.verisign.com/client/help/id_intro.htm#what_is_id. Accessed August 9, 2003

GENERAL SOURCES

Kane B, Sands DZ. American Medical Informatics Association white paper: guidelines for the clinical use of electronic mail with patients. *J Am Med Inform Assoc.* 1998;5:104–111

Burrington-Brown J, Hughes G. *AHIMA Practice Brief: Provider-Patient E-mail Security.* Chicago, IL: American Health Information Management Association; 2003. Available at: http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_019873.html. Accessed August 9, 2003

American Medical Association. *Guidelines for Physician-Patient Electronic Communications.* Chicago, IL: American Medical Association; 2001. Available at: http://www.ama-assn.org/ama/pub/category/2386.html. Accessed August 9, 2003

Bisker S, Tracy M, Jansen W. *Guidelines on Electronic Mail Security: Recommendations of the National Institute of Standards and Technology.* Special Publication 800-45 6. US Department of Commerce, National Institute of Standards and Technology; 2002

Gerberick, Dahl A. Encryption and secure e-mail, an overview. Available at: http://64.78.52.225/initiatives/e-mail/background/Encryptn+SecureEmailOverview.doc. Accessed August 9, 2003

All clinical reports from the American Academy of Pediatrics automatically expire 5 years after publication unless reaffirmed, revised, or retired at or before that time.