Risk Review
a Publication of Princeton Insurance

Princeton Insurance
Partnership. Prevention. Protection.

November 2007

Your Direct Link to Better Risk Management Practices

Physician-Patient E-Mail: Reducing Risk to the Physician Office Practice

By Lilly Cowan, JD, ARM, CPCU, Princeton Insurance Healthcare Risk Consultant

"Physician-patient electronic mail is defined as computer-based communication between physicians and patients within a professional relationship, in which the physician has taken on an explicit measure of responsibility for the patient's care."[1]

[Note: The purpose of this document is not to provide rules on specific issues, but rather to identify concerns that a healthcare provider needs to consider when implementing a new communication technology, such as e-mail, with patients.]

Traditionally, written (paper) and verbal (in person or telephone) communications have been the main means of communicating health information between physicians and their patients. More recently, however, along with their greater reliance upon advanced technology systems to manage office practice functions (e.g. billing, payroll, referrals, medical records, etc.), physicians are increasingly choosing electronic mail ("e-mail") as an alternate method of communicating with their patients.

E-mail can be a useful tool in the practice of medicine. It is a relatively simple, convenient and inexpensive application for both physicians and patients. A few of the benefits of using e-mail, which can help the physician provide quality care, are:

- It facilitates communication with patients since it can be sent and answered at any hour, and it eliminates "phone tag" – the physician and patient don't need to be available at the same time to communicate effectively.
- It facilitates quicker reporting results of diagnostic tests and laboratory studies to the patient, written follow-up instructions and clarification of advice provided in the office can be sent, referral information (phone & addresses) can be sent, educational materials can be provided more easily and (perhaps) at less cost.
- It automatically creates a written record of each communication between physician and patient, thus removing doubt as to what information was conveyed.
- Frequently used educational hand-outs can be formatted for a practice's home page, e-mail messages can enable the user to click on a "live" link (URL), which launches a web browser and takes the user directly to indicated resources on particular topics.

While there can be many benefits of e-mail communication, there are also liability issues associated with its use. Potential exposures include, but are not limited to, the following:

- breach of confidentiality of a patient's personal health information;
- failure to provide a timely response to a patient's e-mail, that could result in a delayed diagnosis or diagnostic error
- failure to comply with the health information privacy and security rules of the Health Insurance Portability and Accountability Act ("HIPAA") of 1996; [1,2]

The following strategies may help reduce liability risks of communicating in this way.

Content & Privacy

- Develop an e-mail policy that specifies the uses and limits of physician/patient electronic communications.

continued on page 2

Vice President of Healthcare Risk Services
Tom Snyder x5852

Manager, Healthcare Risk Services
Phyllis DeCola x5897

Phone: 609.452.9404
www.RiskReviewOnline.com

Princeton Insurance
Partnership. Prevention. Protection.
30 Years of Excellence

We welcome your feedback, comments and suggestions. Please feel free to contact us if you have a question or to send us your ideas for improving this site.

- Inform patients of the policy, so that they are aware of permissible transaction types: prescription refill requests, appointment scheduling and reminders; and inappropriate topics: HIV, mental health-related or other sensitive PHI, etc.
- Develop an informed consent form for use via e-mail that includes permissible uses of their patient information; obtain the patient's written authorization, which should be documented in the medical record with a copy provided to the patient.
- Ask patients to enter the category on the subject line of their e-mail message, with name and patient identification number in the body of the message.
- Do not send group mailings in which recipients are visible to each other; use blind copy feature; never forward patient identifiable information to third parties without the patient's express permission.
- Inform patients whenever their treating physician is not available; provide the covering physician's name for those times, noting that he/she may respond to their e-mail.

Responses

- Set up an automatic reply to acknowledge receipt of messages; determine a reasonable turnaround time for responding to patient messages and adhere to it.
- Advise all patients to use alternate forms of communication for any matter that cannot wait at least 72 hours to be addressed.
- Use automatic messaging features to direct patients to go to an emergency department or call 911 in the event of an emergency.
- Avoid anger, sarcasm, criticism, and libelous references to third parties in your messages.

Security, Storage and Retention

- Recognize that e-mail will always have inherent insecurity, in that it can be intercepted, misdirected or forwarded, that could result in a person's medical record or other personal information being seen inadvertently by the wrong person, at the sender's or receiver's end.
- HIPAA is federal law that applies to a physician practice (known as a "covered entity"), that electronically transmits healthcare information. Regulations were developed to protect the **security** and **privacy** of protected health information ("PHI"). PHI includes information in medical records and other individually identifiable health information.
- These regulations require physicians (1) to implement a security policy (protect PHI against unauthorized access); and (2) to notify patients about privacy and confidentiality procedures in effect for the practice (conditions under which PHI may be transmitted or disclosed). However, a "reasonableness" standard gives covered entities the flexibility to select solutions they consider appropriate for their circumstances.[3]
- Consider the use of encryption technology (e.g. password-protected) to safeguard electronic PHI; alternative approaches include secure Web portals, secure messaging networks and virtual private networks ("VPN"). Inform patients if encryption is not used.
- Implement a mechanism to ensure that all software is up-to-date, that includes regularly checking for security updates or patches.
- Once the original sender transmits the e-mail, he/she no longer controls its re-transmission. Physician practices may want to implement a policy that any e-mail containing PHI should include a statement: "This message may not be forwarded."
- Perform regularly scheduled back-ups (e.g. weekly) of e-mail onto long-term storage; define "long-term" to be consistent with the time period that applies to retention of paper records for a given jurisdiction.
- When appropriate, physicians should save electronic and/or paper copies of e-mail communications with patients in the patient's office medical record.
- Develop archive and retrieval mechanisms for any and all electronically stored patient information, including that stored in e-mails, your Web pages, word-processing files, databases stored in electronic memory systems, such as magnetic disks (computer hard drives), optical disks (e.g. CDs) and archival media or back-up tapes (that may be managed and stored off-site for disaster recovery).

Electronic Information in Litigation

- Electronic discovery ("e-discovery"):[4] Recently, the Federal Rules of Civil Procedure were amended to address advances in electronic data. These federal procedure rules will govern discovery of electronic health information ("e-discovery") in malpractice cases brought in the federal court system. Under the new rules, all electronically stored information that the disclosing party may use to support its claims or defenses, unless otherwise privileged from discovery, must be disclosed. [5]
- The new rules cover not only information in an electronic medical records system and other health information systems, but all data in electronic form, including e-mail, instant messages and healthcare providers' Web pages. The significance of this is that discoverable electronic information may include data that has not traditionally been considered to be part of the patient's medical record.
- New Jersey has adopted electronic discovery rules that mirror the federal rules.[6] Since most medical negligence cases are filed in state courts, the expansion in scope of discovery of electronic health information will no doubt create challenges to those parties that have to produce requested electronic documents.

E-mail is increasingly being used as a means of communication between patients and their physicians. E-mail can be used to provide follow-up care, clarify instructions to patients, send test results, make appointments or provide Web links to additional educational resources. However, while there can be advantages with using email over traditional forms of communication, there are also concerns, including issues of privacy and security, that should be recognized and addressed appropriately. ❖

References

[i1] Guidelines for Physician-Patient Electronic Communications; AMA. www.ama-assn.org

[i2] The U.S. Dept of Health & Human Services, Office for Civil Rights (OCR) - HIPAA, is the official central governmental hub for all HIPAA issues, including rules, standards and implementation guidelines: http://www.hhs.gov/ocr/hipaa/. Submit questions about health information privacy to OCR by e-mail to: OCRPrivacy@hhs.gov. Contact OCR by telephone at (866) 627-7748.

[i3] http://www.hhs.gov/ocr/hipaa/; HIPAA Compliance Handbook, Aspen Publishers, 2007 Ed., see: Special Topics in Security Regulation, pages 4-18 – 4-20.

[4] E-discovery in health care litigation, Mary-Jo Rebelo, Esq., available at http://www.physiciansnews.com/law/207rebelo.html

[5] Electronic Health Records Raise New Risks of Malpractice Liability, J. Korin and M. Quattrone, NJ Law Journal, 6/19/07.

[6] New Jersey Rules of Court, Part IV-Rules Governing Civil Practice in Superior Court; Ch.III. Pretrial Discovery; Rule 4:10-2. Scope of Discovery; Par. (a), (c) and (e) amended, and new par. (d)(4), (f) and (g) adopted July 27, 2006, to be effective Sept. 1, 2006. Rule4:18-1: Production of Documents, Electronically Stored Information, et.al.; Par. (a) and (b) adopted July 27, 2006 to be effective Sept. 1, 2006❖