HVPA Guidelines for Physician-Patient eMail Communication  
May 2004

Introduction:
Electronic mail (email) can be a useful tool in the practice of medicine and can facilitate communication within a patient-physician relationship. When using email to communicate with patients, physicians hold the same ethical and legal responsibilities to their patients as they do during other encounters (face-to-face, letter, telephone). Issues of privacy, confidentiality and security must be addressed. HIPAA regulations do not prohibit or discourage communications via email. As with other forms of communications, health care providers must implement safeguards to protect the privacy and security of individually identifiable health information maintained or transmitted electronically.

Definitions:

Security: Online communications between health care providers and patients should ideally be conducted over a secure network, with provisions for authentication and encryption. Standard email services (AOL, Comcast) typically do not meet these guidelines. Health care providers need to be aware of potential security risks, including unauthorized physical access and security of computer hardware, and guard against them with technologies such as automatic logout and password protection.

Encryption: Scrambling information (into ciphertext) so that intercepted messages cannot be read.

Authentication: The health care provider has a responsibility to take reasonable steps to authenticate the identity of correspondent(s) in an electronic communication and to ensure that recipients of information are authorized to receive it.

Confidentiality: The health care provider is responsible for taking reasonable steps to protect patient privacy and to guard against unauthorized use of patient information.

Informed Consent: Prior to the initiation of online communication between the physician and patient, informed consent should be obtained from the patient regarding the appropriate use and limitations of this form of communication. This agreement should become part of the legal documentation and medical record when appropriate.

Physician Email Communication Guidelines

- Ideally, providers and patients should communicate through a secure email server using encryption technology. Examples of vendors providing secure email can be found in Appendix A. If a secure email server is not used, the physician must inform the patient that email communications should not be considered secure.

- Email correspondence should not be used to establish a patient-physician relationship. Rather, email should supplement other, more personal, encounters.
• Use of email for urgent matters should be avoided whenever possible.

• Avoid anger, sarcasm, harsh criticism and libelous references to third parties in messages.

• Never forward patient-identifiable information to a third-party without the patient’s express permission.

• Do not use patient’s email address for marketing purposes.

• Do not use unencrypted wireless communications with patient-identifiable information as it may be intercepted.

• Double-check all “To:” fields prior to sending messages.

• Keep practice emails separate from personal emails.

**Patient Considerations**

• Patients should receive “right to notice” of privacy practices for protected health information.

• Inform patient of the expected turn-around-time for the practice to respond to email.

• Inform patient of what action to take if they do not receive a response within the expected timeframe.

• Communicate to the patient the information will your office deem appropriate for email. What information is not appropriate?

• Disclose to the patient who may have access to email communications within the practice and for what purpose.

• Explain any filter, authentication, security, or encryption measures used by the practice.

• Develop criteria to eliminate email communication method with patients who are not compliant with agreed upon communication terms.

• Instruct patients to put category of transaction in subject line of message for filtering:
  • Prescription refill
  • Appointment
  • Medical Advice
  • Billing Questions
Office Practice Action Plan:

- Determine how often email will be read? (Daily, Twice Daily, Every hour?)

- Determine who will be responsible for opening emails. Will one person read the emails and forward to the appropriate recipients?

- Develop a confidentiality notice “header” for email communications to indicate the information included in the email is confidential medical communication (example below):

  “CONFIDENTIALITY NOTICE: This communication contains information from [your practice name] that may be CONFIDENTIAL, LEGALLY PRIVILEGED, PROPRIETARY or otherwise protected from disclosure. This information is intended for use only by the person to whom it is addressed. If you are not the intended recipient, any use, disclosure, copying, distribution, printing, or any action taken in reliance on the contents of this communication, is strictly prohibited.”

- Establish the process for handling administrative inquiries such as insurance and appointment information, prescription refill requests, etc.?

- Determine who will read email when physicians are out of the office? How will patients be informed that physicians are out of the office on vacation?

- Configure automatic reply to acknowledge receipt of messages.

- Print messages (if no EMR), with replies and confirmation of receipt, and place in patient’s paper chart.

- Use password-protected screensavers for desktop workstations.

- Develop patient education brochure

- Develop/obtain/retain patient consent form

- Update confidentiality policies and procedures to incorporate email communication references. Corresponding staff training and awareness should be implemented.

- Office policies and procedures should address at a minimum:
  - Verification requirements for sending and receiving addresses
  - Procedures for handling misdirected mail (both sent and received)
  - Patient education on good email practices and limitations on security
  - When email is considered appropriate and when it is not
  - What types of information may be transmitted through email
  - Documentation in medical record of email correspondence
  - Virus protection program with regular updates of virus programs
  - Proper retention and destruction procedures to ensure all vulnerable areas are covered.
Resources

American Academy of Family Physicians. Using email to communicate with patients. 
http://www.aafp.org/x21276.xml


http://134.174.100.34/AHIMA/JAHIMA_Murphy.htm

Sands DZ. Guidelines for the use of patient-centered email. Massachusetts Health Data Consortium.

Stanford Hospital and Clinics – Medical staff update online. Policy on fax, email protects privacy. June 2003 

LAW
04/04
Appendix A:
Encrypted eMail & Secure Messaging Services
May 2004

• HealthyEmail

http://www.healthyemail.org

  note: offering a two-year free license to secure email program Zixmail to physicians

• RelayHealth

http://www.relayhealth.com

• Medem

http://www.medem.com

• MyDocOnline

https://www.mydoconline.com

• Medfusion

http://www.medfusion.net