E-mail as a Provider-Patient Electronic Communication Medium and Its Impact on the Electronic Health Record

This practice brief has been retired. It is made available for historical purposes only.

Practice Brief

Background

The American Medical Association defines provider-patient e-mail (electronic mail) as computer-based communication between providers and patients within a professional relationship, in which the provider has taken on an explicit measure of responsibility for the patient's care.[1] Electronic communications have been shown to be effective in facilitating communication among providers and patients, thereby allowing for greater continuity of care and more timely interventions.[2]

Provider-patient electronic communications, such as e-mail and text messaging, are healthcare organizational business records and are therefore subject to the same storage, retention, retrieval, medicolegal, privacy, security, and confidentiality provisions as any other patient-identifiable health information.[3] As such, organizations need to develop policies to manage e-mail records just as they manage any other medical records.[4]

Approximately 19 percent to 38 percent of providers currently use electronic communications with their patients.[5] Growth in e-mail use is being hampered by the lack of reimbursement for these types of communications for Medicare patients. However, some third-party payers have begun to reimburse in some instances, with demonstrated improvements in both cost and workflow. If Medicare reimbursement for electronic provider-patient communications occurs, electronic communications between provider and patient are likely to increase.[5]

Examples of provider-patient e-mail applications include

- Appointment scheduling
- Prescription refill
- Transferring lab reports or results
- Patient education

Although e-mail communication is most common, other means of provider-patient electronic communications include

- PDA text messaging
- Online consultations
- Online prescribing
- Web messaging
- Digital transfer of lab reports or results

Benefits

Time/production/workflow efficiencies: Electronic communication can reduce interruptions caused by phone calls, reduce nonessential office visits, and save time relative to communication by telephone. Traditional telephone calls are not always a practical means of communication. Often, one of the parties is not available to communicate or does not have the time or appropriate information at hand to complete the communication. Telephone messages are not always private or confidential. Many telephone messaging systems do not allow enough time to leave complete messages. E-mail allows both parties to read and respond to the message when it is convenient to do so. E-mails allow for enough space in the document to send a complete message. Finally, because e-mail messages allow for attachments of supporting documentation, Web site and e-mail addresses can be added to complete the communication.

Improved quality of care: E-mail can improve communication between provider and patient by documenting instructions, educational materials, or interpretation of lab results, or it can allow for more timely communication of test results to patients. E-mail allows both the provider and the patient more options than traditional face-to-face, written, and telephone interaction so communication is enhanced.

- **Cost efficiencies:** Using e-mail for provider-patient communications can result in cost savings as compared to a face-to-face encounter.
- **Provides a business record of the conversation and transaction:** Unlike face-to-face conversations or telephone conversations, e-mail communication provides a ready-made record of the communication.
- **Liability protections:** An e-mail message documents the precise communication between provider and patient.
- **Convenience:** Providers and patients can schedule time to send or answer e-mail messages.

Risks

Security and Privacy Risks

- An e-mail message may be intercepted and threaten patient privacy. E-mail message content can be altered and/or forwarded to unintended recipients.
- Numbers and letters in an e-mail address can be easily transposed, and e-mail may be delivered to the wrong person or not delivered at all.
- Difficulty can arise in establishing or confirming the identity of the patient in an e-mail request. A patient name without other identifiers may be insufficient to establish the identity of the patient. Accepting e-mail mes-sages containing only the patient name and/or e-mail address without other identifiers can result in confusion with other patients with like names and e-mail addresses. The individual sending the e-mail may not be the patient, but an imposter using the patient's e-mail.
- Group e-mail messages present a risk for loss of confidentiality. Individual confidentiality is not protected when recipients are able to see the names and/or e-mail addresses of other group e-mail recipients.
- Word documents sent as attachments that stay on a hard drive present a risk for unauthorized access and breach of confidentiality.
- Clinicians answering patient e-mail messages from an unsecured location such as home computers could present a problem. Protected health information would be retained on private personal computers and in files maintained by Internet service providers.
- Opening an attachment with a virus may cause serious damage.

Administrative and Medicolegal Risks

- Delays in turnaround time could nullify the benefits of the electronic medium. Work flow efficiencies potentially gained from e-mail are lost if a patient does not receive a response and initiates either further e-mail messages or telephone calls that require a response as well. E-mail can serve as a protection against liability because precise communication between the provider and patient is documented. This can become a liability, however, if the provider's documentation is not complete or lacks timeliness.
- Misfiles or lost communications can nullify the benefit of an electronic medium. E-mail messages provide precise documentation between the provider and patient only if the documentation can be easily referenced and retrieved.
- Electronic communication can be misinterpreted due to lack of verbal and nonverbal cues. Electronic communication requires a certain level of patient e-mail/ health literacy. It may be difficult for the provider to determine if the patient is able to understand the medical terms and concepts contained in the e-mail messages.
- Web pages used as links that are not "active" or contain information that is not credible present problems.

- E-mails are returned to the sender when addresses are incorrect or outdated.
- There is a lack of documentation that the intended recipient received and read the e-mail message sent by the provider.
- E-mail may overburden provider schedules.
- Laws may vary between states on use of e-mail for patient care or provider licensure requirements.
- Inappropriate utilization by patients, such as an emergency situation, could result in an adverse outcome for patients.

Recommendations

Security and Privacy

- Security is a primary concern. The e-mail system security must be sufficient to ensure, to the highest degree possible, the following
  -Nonrepudiation
  -Messages are read only by their intended recipients
  -Verification of delivery/receipt
  -Labeling of sensitive material
  -Control of access by those other than the provider
  -Security of computer hardware
  -Completeness
  -Trustworthiness[4]
- Strive to retain the integrity of the message and authentication of source.
- Whenever feasible, instruct users to copy and paste addresses or use the e-mail reply button.
- The availability of secured (encrypted) e-mail transmission will be the determining factor limiting the content and use of e-mail.
- Browser-based communication with patients has advantages because it provides additional security as compared to e-mail. For example, log-ins are required and audit trails are accessible. Security/encryption, physical security, structured messaging, approval/revocation options, and group access versus single access are more characteristics of browser-based communication.
- Maintaining a secure mail server is an ongoing process. A critical role in a secure mail server is an extensive network infrastructure (firewalls, routers, intrusion detection systems). Internet/intranet issues must be addressed. E-mail may be secure on an intranet and not secure on the Internet.
- Encryption software is available for wired and wireless communication. Configuration management is an essential part of maintaining a secure system. The complex mathematic algorithms involved in the highest levels of confidentiality increase e-mail size and slow servers. Also, encryption may interfere with virus scanning and mail content filtering. Administrative overhead is often required. Software must be monitored even after installation for upgrades, patches, and correct versus default settings, especially after a server crash.
- The HIPAA security rule provides guidelines as to the appropriate use of transmission security.[6] The associated risk to electronic protected health information should drive the decision to use transmission security tools. Following is the Department of Health and Human Services response to comments and questions regarding the use of encryption tools to secure protected health information transmitted from one point to another.[7]

> *Response: In general, we agree with the commenters who asked for clarification and revision. This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term "Communications/network controls" has been replaced with "Transmission security" to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.*
>
> *We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.*
>
> *Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use*

of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the Internet.

As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

We do not use the term "open network" in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis.

From Sec. 164.312, Technical Safeguards:

(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) Implementation specifications:
(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

- Cryptosystems provide a means to ensure confidentiality, authenticity, nonrepudiation, and integrity of e-mail messages. Three common types of cryptographic hardware and/or software systems are:

  -**Symmetric cryptography:** A single key is shared by the sender and the recipient. The encryption algorithm (e. g., data encryption standard [DES], 3DES) is much simpler and thus faster.

  -**Asymmetric cryptography (e. g., public key infrastructure):** Each user owns a pair of keys, one public and one private. The public key is given to the sender to encrypt the messages, and the corresponding private key is used by the recipient to decrypt messages. The encryption algorithm (e. g., Rivest-Shamir- Aldeman, a public-key cryptographic algorithm that hinges on the assumption that the factoring of the product of two large primes is difficult) has to match the decryption algorithm, which makes it very complex and thus much slower.

  -**Hybrid cryptography (e. g., pretty good privacy [PGP]):** This is a combination of symmetric and asymmetric cryptography. A session key is randomly generated for each message. The plain text is then encrypted with this session key. The public key-encrypted session key is then transmitted, along with the session key-encrypted cipher text, to the recipient. In this method, the encryption (session) key is securely distributed by the public key and the plain text is encrypted by faster symmetric cryptography.

- Virtual private networks (VPN) allow use of the public Internet to securely connect remote offices and employees at a fraction of the cost of dedicated, private telephone lines such as frame relay. A VPN supports at least three different modes of use:

  -**LAN-to-LAN internet working** connects two or more geographically separated networks, such as those at a main office and a remote branch office.

  -**Remote access client connections** allow telecommuters to safely log into company networks.

  -**Controlled access within an intranet** can also use VPN technology to implement controlled access to individual subnets on the private network.

The most important component of a VPN is the gateway. The symmetric encryption (e. g., 3DES) is done between gateways of two networks.

With the hype that has surrounded VPNs historically, the potential pitfalls or "weak spots" in the VPN model can be easy to forget. These four concerns with VPN solutions are often raised:

1. VPNs require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.

2. The availability and performance of an organization's wide-area VPN (over the Internet in particular) depend on factors largely outside of the organization's control.

3. VPN technologies from different vendors may not work well together due to immature standards.

4. VPNs need to accommodate protocols other than IP and existing (" legacy") internal network technology.

- Web e-mail with a domain name and secure socket connection provides a higher level of security than standard secured e-mail messages.[8] A secure Web server is purchased and managed by system security professionals.

- Hard drives used by providers for patient e-mail communication must be cleaned using a "wipe" utility before the processor is surplused or reassigned to another person.

Administrative and Medicolegal Recommendations

- Create a policy that establishes **criteria for the provider-patient e-mail communication** and consent process before initiating electronic communication with the patient. The provider and patient should have an established relationship. Differentiate among preexisting conditions, ongoing treatment, follow-up questions related to a previous discussion, and a new diagnosis and treatment addressed exclusively online. New diagnosis and treatment of conditions addressed exclusively online may increase liability.
- Develop procedures for the **patient's authorization/agreement** to use e-mail as a communication medium. The procedures must outline where patient authorization will be filed, how it will be retrieved, and what indicators or flags in the patient record, if any, show that the patient wishes to participate in electronic communication with the provider.
- Develop policies addressing issues that require the e-mail documentation to become **part of the patient record.**
- Establish and enforce **retention policies.** Original e-mail, with reply, should be filed in the electronic health record or printed for the paper record. The provider should initial and date the paper copy for the paper record.
- **Develop policies and procedures to guide the use of group e-mail messages** that describe the necessity of protecting the identities of individual group members from other members in the group and provide instructions to users (i. e., blind copy [bcc] feature).
- Develop criteria to **determine a patient's health literacy level** and ability to use an e-mail application.
- Establish procedures to **instruct the patient** to follow up in person or by phone for requests that do not meet content guidelines. Lengthy e-mail messages or prolonged correspondence with a patient may necessitate scheduling an appointment with the patient or calling the patient.
- Establish a policy for e-mail **turnaround time.** The policy should prioritize e-mail messages by type of request, clearly identifying what may constitute an urgent or emergent request. It should also include actions to take when the turnaround time is not met.
- Develop a policy and educate patients about **appropriate types of e-mail** (e. g., prescription refills, appointment scheduling, lab results).
- Laws regarding e-mail communication may vary between states. **Research** your state's laws and those of surrounding states regarding the use of e-mail for medical treatment. (Alllaw. com is a Web site for researching state laws regarding the use of e-mail for medical treatment.)
- Develop a policy that addresses **security issues** when using remote access. Providers must not communicate with patients in the context of their professional relationship using personal e-mail accounts such as America Online, Earthlink, or any other nonemployer e-mail system.
- Develop a policy that addresses the following **topics that should not be discussed in e-mail** transactions and procedures that include a response to patients whose e-mail addresses these issues:
  -Protected diagnoses or treatments such as mental health or chemical health (based on state or federal privacy regulations)

-HIV status
-Workers' compensation injuries and disability
-Urgent health conditions

- Develop and enforce policies **defining and prohibiting emergency e-mail messages.**
- Develop procedures addressing a **workable documentation mechanism** for responding to an e-mail via telephone call and responding to a telephone call via e-mail.
- Develop a policy and procedure to guide **termination** of a patient from e-mail communication (e. g., patient notice, registration indicator).
- Establish a methodology to **audit** all e-mail correspondence to ensure appropriate
  -Customer service
  -Quality of care provided via the e-mail communication
  -Quality of the response provided to the patient via e-mail
  -Review for possible legal risk issues
  -Patient privacy and confidentiality
  -Tracking e-mail messages returned because of incorrect address
- Organizational procedures for **cleaning computer hard drives** must be established and enforced.
- **Update current confidentiality policies** to incorporate references to e-mail if they are not already in place.

(See Appendix A, "HIM Managers Tasks and Skills with Regard to Administrative-Medicolegal Risks.")

E-mail Recommendations

- The provider's e-mail signature block should contain the provider's full name, contact information, response time, instructions for when response time is not met, and instructions for handling patient emergencies.
- Web pages used as links (or given to patients) should be credible, and links should be active. Links should be monitored often and updated as needed.
- One method of controlling misdirected e-mail is to not allow providers to initiate e-mail messages. The patient initiates the e-mail, and the provider responds by using the reply button.
- Use e-mail system functionality (e. g., automatic reply to acknowledge receipt, return receipt to confirm patient receipt, blind copy feature to uphold patient privacy).
- Establish a central patient registration database that will serve as a systemwide directory. A central directory will prevent duplications and errors in the patient's e-mail information. A central directory will allow for greater control, with prompt and easy updating of patient e-mail addresses and identifying information. Verify patients' e-mail addresses during appointment scheduling and/or patient registration.
- Patients must register e-mail addresses and provide identifying information in e-mail messages.
- Patient identifiers other than name are important (duplicate names). Medical record numbers will not be a relevant identifier if e-mail is being forwarded to another healthcare facility (e. g., referral).
- A healthcare entity should have a standardized template for e-mail in place to ensure the appropriate information is communicated and captured. This will also keep e-mail concise.
- Educate staff on appropriate e-mail etiquette. Sarcasm, anger, harsh criticism, and libelous references to third parties in e-mail messages are not appropriate.
- Whenever feasible, instruct users to copy and paste addresses or use the e-mail reply button.
- Patients should be informed of the e-mail policies and procedures in advance. The patient should knowingly authorize to communicate via e-mail in advance.

  (See Appendix B, "Documentation of Authorization to E-mail Discussion" and Appendix C, "Patient Authorization for E-mail Communication."

- When communicating confidential medical information via e-mail, a banner similar to the one below should be displayed prominently at the beginning of the e-mail message:

  > THIS CONFIDENTIAL COMMUNICATION CONTAINS INFORMATION PROTECTED BY PROVIDER-PATIENT PRIVILEGE.

- A statement of confidentiality should be posted on all e-mail correspondence such as:

The contents of this e-mail message and any attachments are confidential and are intended solely for addressee. The information may also be legally privileged. This transmission is sent in trust, for the sole purpose of delivery to the intended recipient. If you have received this transmission in error, any use, reproduction, or dissemination of this transmission is strictly prohibited. If you are not the intended recipient, please immediately notify the sender by reply e-mail or (area code) (phone number) and delete this message and its attachments, if any.

Patient Education: Confidentiality Recommendations

- **Inform patients** regarding practices of screening e-mail (e. g., if office personnel screen e-mail for the provider). Point out the need for the patient to develop privacy practices. Point out that patients are charged with the responsibility to handle their information in a secure manner.
- **Instruct patients** regarding the type of information that must be included in the e-mail message. The subject line should include the category or type of request to facilitate prioritizing and routing messages (e. g., appointment, prescription refill, lab results). The specific provider's name should be included as well.
- **Define patient identifiers,** besides the patient's full legal name, that will be used to verify patient identity and facilitate filing in the electronic or paper medical record. Suggested patient identifiers are
  -Date of birth
  -Last four to six digits of social security number
  -Phone number
  -Mother's maiden name
  -Password created by the patient

Organization **procedures must support the retention** of these data elements in the patient registration system, and e-mail templates may include these items on the form as prompts to the patient.

- Inform patients that the provider will **terminate** e-mail correspondence with patients who repeatedly do not adhere to the written e-mail guidelines.
- It is a commonly accepted axiom that communication is 7 percent words, 38 percent voice, and 55 percent body language. If this axiom is true, e-mail must be considered to be a communication media with **limited effectiveness.** Providers communicating via e-mail must be aware of its limitations and adjust their communication accordingly.
- Inform patients about the **risk** of loss of confidentiality when using their employer's e-mail account.
- Inform patients in advance if e-mail messages may be **forwarded** to other clinics/providers (e. g., referrals).
- Inform patients that e-mail communications are **retained** as part of the patient's permanent legal medical record.
- Inform the patient about **indemnity** for information loss due to technical failures.
- Patients should be educated about the **appropriate types** of transactions for e-mail communications. E-mail templates may be created to assist the patient in identifying the type of request (e. g., check boxes). Examples of when e-mail is appropriate include
  -Prescription renewals
  -Nonurgent medical advice
  -Test results, based on professional judgment
  -Insurance inquiries
  -Benefit information
  -Provider network information
  -Billing information
  -Scheduling/canceling/rescheduling appointments
  -Clinic/provider changes
  -Other nonurgent communication
- **Document** patient education in the patient's medical record and reference education materials given to the patient.

Electronic Document Management Recommendations

E-mail must be treated like any other healthcare organizational business record (e. g., patient medical record, patient financial record, employee record) because it is subject to the same course of evidentiary discovery and has a life cycle that requires management guidelines (i. e., it is created, indexed, searched, retrieved, routed, stored, and purged).

E-mail management is an enormous, complex problem. This problem is expected to get worse as the numbers and types of senders and receivers (e. g., providers and patients) increase exponentially. Therefore, the following guidelines are recommended:

- Identify existing, **enterprise-wide repositories** that securely store (or should store) e-mail records and attachments that merit evidentiary handling.
- Develop or acquire an easy-to-use yet **functionally robust e-mail management system** that includes a centralized archive. The e-mail management system should
  -Have **intuitive methods for identifying** e-mail classifications and retention rules. For example, one classification might be healthcare-related information that is linked directly to the master patient index. Another classification might be meetings and general business communication information. Different retention rules could be linked to each classification group.
  -Include dependable **search capabilities** as well as fast and efficient access to archives.
  -Have an "open architecture" allowing for **compatibility** with popular e-mail systems.
  -Enforce e-mail **archiving** policies. For example, when an individual closes an e-mail and is ready to discard or save it, a prompt should appear with a yes-or-no choice asking if the user would like to make this a part of any of the healthcare organization's "business" records (e. g., classification of patient medical records). This "opt in/out" e-mail capture function can be eliminated if the healthcare organization declares ahead of time that the e-mail must always be retained to comply with a regulatory, legal, or business need (e. g., an e-mail correspondence between a provider and a patient). In addition, this function can be managed in the background using Web technology so that, for example, each new patient added to the master patient index triggers a domain name, with all inbound and outbound e-mail captured for patientname. com.
  -Include **retention rules** that are triggered automatically by actions. This includes automatically deleting or encrypting a "patient class" of e-mail after X number of days/months/years so it cannot be accessed. (Note: Never archive encrypted e-mail records for fear of losing the algorithms or keys.)
- **Create** appropriate rules, policies, and procedures specific to each organization upon system deployment to eliminate the risk of purging e-mail attachments in a storage crisis. These systems quickly become overwhelmed by metadata and attachments.

- Establish a methodology to meet **HIPAA's** requirement for providing an accounting of disclosures.

(See also "Appendix D, "Summary of Best Practices for Provider-Patient E-mail Communication.")

Notes

1. American Medical Association. "Guidelines for Physician-patient Electronic Communication." Available at www. ama-assn. org/ama/pub/category/2386. html.
2. Institute of Medicine. "Key Capabilities of an Electronic Health Record System: Letter Report." Available at http://books. nap. edu/books/NI000427/html/index. html.
3. Kohn, D. "E-mail: Treat It as Just Another Record." *Advance for HIM Professionals.* Available at www. advanceforhim. com/common/editorialsearch/viewer. aspx? FN= 02oct28_ hip33. html& AD= 10/28/2002& FP= hi.
4. Kahn, R. "Beyond HIPAA: The Complexities of Electronic Records Management." *Journal of AHIMA* 74, no. 4 (2003). Available in the FORE Library: HIM Body of Knowledge at www. ahima. org.
5. "Handhelds Hot, E-mail Not for US Physicians." Press release issued Nov. 4, 2002, by the Healthcare Information and Management Systems Society. Available at http://www. himss. org/ASP/ContentRedirector. asp? ContentId= 23146.
6. "Health Insurance Portability and Accountability Act of 1996." Public Law 104-191. August 21, 1996. Available at http://aspe. hhs. gov/admnsimp/.
7. "Final Rule for Security Standards." Federal Register 68, no. 34 (February 20, 2003). Available at http://www. access. gpo. gov/su_ docs/fedreg/a030220c. html.
8. Rognehaugh, A., and R. Rognehaugh. *Healthcare IT Ter ms.* Chicago: Healthcare Information and Management Systems Society, 2001.

References

American College of Physicians. "The Changing Face of Ambulatory Medicine-Reimbursing Physicians for Computer-based Care." Available at www. acponline. org/hpp/e-consult. pdf.

Bowman, B. "Beyond the Telephone: Electronic Tools for Patient-provider Communications." *Group Practice Journal* 51, no. 1 (2002). Available at www. amga. org/ Publications/gpj/articles/CoverStories/ coverStoryJan02_ gpj. pdf.

Burrington-Brown, J., and G. Hughes. "AHIMA Practice Brief: Provider-Patient E-mail Security" (Updated June 2003). Available in the FORE Library: HIM Body of Knowledge at www. ahima. org.

California Health Care Foundation. "E-encounters." Available at www. chcf. org/documents/ihealth/EEncounters. pdf.

HealthyEmail. "Email and Clinical Practice." Available at www. healthyemail. org/and www. healthyemail. org/toolkit. php.

Kane, B., and D. Z. Sands. "Guidelines for the Clinical Use of Electronic Mail with Patients. *JAMIA* 5, no. 1 (1998): 104Ð 111.

Manhattan Research. "The Future of Medicine Is in the Hands of 205,000 Physicians." Available at www. manhattanresearch. com/thepulse. htm.

Medem. "eRisk Working Group for Healthcare: Guidelines for Online Communication." Available at www. medem/com/phy/phy_ eriskguidelines. cfm.

Medem. "eRisk Working Group for Healthcare: Guidelines for Online Communication [Addendum]." Available at www. medem. com/corporate/corporate_ Addendum_ A_ eRi skGuidelines. cfm.

Medem. "Secure Messaging and Online Consultation FAQ for Physicians." Available at www. medem. com/phy/phy_ faq_ physician. cfm.

Murphy, G. "Patient-centered E-mail: Developing the Right Policies." *Journal of AHIMA* 71, no. 3 (2000). Available in the FORE Library: HIM Body of Knowledge at www. ahima. org.

Patt, M. et al. "Doctors Who Are Using E-mail with Their Patients: A Qualitative Exploration." *Journal of Medical Internet Research* 5, no. 2 (2003). Available at www. jmir. org/2003/2/e9/index. htm.

Sands, D. Z. "Guidelines for the Use of Patient-centered E-mail." Available at www. mahealthdata. org.

Techencyclopedia. Available at www. techweb. com/encyclopedia/.

Tracey, M., W. Jansen, and S. Bisker. *Guidelines on Electronic Mail Security.* Washington, DC: National Institute of Standards and Technology, US Department of Commerce.

Glossary

Approval/revocation options: A patient must receive approval from the provider's office to communicate online. Likewise, the provider's office may revoke communication privileges at any time.

Archive: (1) To copy or move data onto a secondary disk or tape for backup or data retention purposes. Archived files are normally compressed to maximize storage media, and such programs may be called "archive programs" or "archiving programs." (2) To save data onto the disk. Moving rarely or never accessed computer files to an offline storage device such as magnetic tape or optical disk system. Archiving is a good practice to provide backup of important files as well as to save critical space on the system hard disk.

Audit trails: Created to track when messages were accessed, modified, and/or routed and by whom.

Authentication: Verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message.

Call back: A procedure for identifying a remote terminal. In a call back, the system disconnects the caller and then dials the authorized telephone number of the remote terminal in order to re-establish the connection. Synonymous with dial back.

Cipher: A cryptographic transformation that operates on characters or bits.

Cipher text or cryptogram: A message that has been encrypted or in unreadable or unintelligible format.

Configuration management: Management of the various configurations of the hardware and software components within the technical environment. For example, the automatic documentation of all components used to build executable programs. It is able to recreate each build as well as recreate earlier environments in order to maintain previous versions of a product. It may also be used to prevent unauthorized access to files or alert the appropriate users when a file has been altered. In relation to hardware, configuration management may be a database that contains information about the workstations, servers, bridges, routers, and other equipment on the network, such as type of equipment, model, etc. In relation to software, configuration management provides a history such as date of installation of the software, dates of changes to the software, version numbers, etc.

Cryptography: The art and science of hiding the meaning of a communication from unintended recipients.

Cryptosecurity: The security or protection resulting from the proper use of technologically sound cryptosystems.

Data encryption standard (DES): A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use.

Decipher: To undo the encipherment process and make the message readable.

Electronic-(e-): The "e" prefix, with or without the hyphen, may be attached to anything that has moved from the physical world to its electronic alternative (e. g., e-mail, e-commerce). "E" words have become synonymous with the Internet.

E-disease management: New electronic tools that support a more coordinated and proactive approach to managing chronic illness by providing patients with improved communication, access to information, and self-management tools.

E-encounter: A type of physician-patient electronic communication that is a two-way exchange of clinical information revolving around a particular clinical question or problem specific to the patient. It may be initiated by either the patient or the caregiver.

E-mail: The transmission of memos and messages over a network. Within an enterprise, users can send mail to a single recipient or broadcast it to multiple users. Mail is sent to a simulated mailbox in the network mail server or host computer until it is interrogated and deleted.

E-prescribing: An electronic prescription order/fulfillment route that directly interfaces with physician workstations and mail order or retail pharmacies.

Encipher: To make the message unintelligible to all but the intended recipients.

End-to-end encryption: Encrypted information that is sent from the point of origin to the final destination. In symmetric key encryption, this requires the sender and receiver to have identical keys for the session.

Group access versus individualized access: Groups of individuals, rather than individuals, can be targeted for messages. This guarantees that providers and staff members can actively respond to messages without affecting the office workflow.

Internet: The Internet is made up of computers in more than 100 countries covering commercial, academic, and government endeavors. Originally developed for the US military, the Internet became widely used for academic and commercial research. Users had access to unpublished data and journals on a huge variety of subjects. Today, the Internet has become commercialized into a worldwide information highway, providing information on every subject known to humankind.

Intranet: An in-house Web site that serves the employees of the enterprise. Although intranet pages may link to the Internet, an intranet is not a site accessed by the general public. The term as originally coined has become so popular that it is often used to refer to any in-house LAN and client/server system.

Log in: Each person must log in using a unique user name and password, limiting who can access what messages.

M-health: Mobile health; the use of PDAs, tablet computers, subnotebooks, smart phones, wireless networks, mobile hardware peripherals, and all related software for healthcare.

Personal digital assistant (PDA, wired/wireless): A handheld computer that serves as an organizer for personal information. It generally includes at least a name and address database, to-do list, and note taker. PDAs are pen based and use a stylus to tap selections on menus and enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between the PDA and desktop computer via cable or wireless transmission.

Physical security: Unlike e-mail where the message exists on an individual's computer, browser-based e-mail is located on secure servers located in high-security buildings designed to limit access only to authorized persons.

Plain text: A message in clear-text readable form.

Secure state: A condition in which no unauthorized subject can access any object.

Security/encryption: Browsers such as Internet Explorer and Netscape offer 128-bit encryption that provides additional protection from others getting access to private information or communications.

Security filter: A trusted subsystem that enforces a security policy on the data that passes through it.

Structured messaging: Structured messages are designed to streamline the communication process, minimizing the time necessary to respond to a patient's question or concern. They also limit abuse of the system.

Text messaging (wireless): Sending short messages to a smart phone, pager, PDA, or other handheld device. Text messaging implies sending short messages generally no more than a couple of hundred characters in length.

Wired communication: Generally refers to the physical cabling in a network. "Over the wire" means transmitting the signals onto the physical medium. Increasingly, the wire is no longer metal, but glass.

Wireless data communication: The transmission of data via airwaves. Wireless data includes paging, text messaging, e-mail, Web access, and other specialized data applications and specifically excludes voice transmission. Wireless data typically implies transmission to a mobile terminal such as a smart phone or PDA; however, fixed wireless applications transmit between stationary objects.

Appendix A

HIM Managers Tasks and Skills with Regard to Administrative-Medicolegal Risks

Level	Skill/Task	
Analysis	**Task**	Evaluate the risks and benefits of using provider/patient e-mail in the facility.
Analysis	**Task**	Develop policies and procedures on the use of patient/physician e-mail. Include the patient identifiers that will be required for e-mail (e. g., date of birth, social security number). The physician/provider signature block should include provider's full name, contact information, response time, instructions for when response time is not met, and instructions for handling patient emergencies.
Analysis	**Task**	Develop an authorization form for patients to complete prior to conducting e-mail. An authorization form should inform the patient of the risks involved with e-mail. Examples of the some of the potential risks (1) e-mail may be intercepted, altered, and/or forwarded to many; (2) e-mail address may be entered incorrectly and delivered to the wrong recipient; (3) sender may assume that a message was sent when it was not; (4) inability of some computers to open attachments; (5) possibility of misinterpretation of e-mail due to nonverbal feedback; and (6) attachments saved to the hard drive may present a risk for unauthorized access and breach of confidentiality.

Analysis	**Task**	Develop procedures for managing the authorization process such as (1) where the authorization form will be filed and how retrieved (2) what indicators or flags will be used to designate the patient's desire to participate in electronic communication, and (3) when and how the authorization process will be performed.
Analysis	**Task**	Develop patient selection criteria to identify patients suitable for e-mail correspondence (e. g., patient has seen the physician in the office within a specified time period, patient knows how to use the e-mail application, patient's health literacy level and language literacy level are adequate for this type of communication).
Analysis	**Task**	Develop and enforce policies and procedures for storing e-mail messages in the medical record. Determine what types of messages are to be saved in the medical record. Save messages in medical record when transaction is complete. Electronic messages are considered business records and should be stored accordingly. Provider should initial/date paper copy for paper record.
Analysis	**Task**	Develop policies and procedures to guide the use of group e-mails. The names of all of the individuals in the group should not be visible. The only name visible to the receiver should be the receiver and sender's name and e-mail address.
Analysis	**Task**	Develop policies addressing e-mail as part of the permanent medical record.
Analysis	**Task**	Evaluate state law to determine whether e-mail can be conducted with patients who live out of state. The state in which the provider/facility resides should be researched as well as surrounding states.
Analysis	**Task**	Apply HIPAA privacy and security regulations to the policies and procedures developed for patient-provider e-mail to ensure the protection of PHI.
Analysis	**Task**	Develop procedures for documenting telephone calls made in response to e-mails or responding to telephone calls via e-mail.
Analysis	**Task**	Establish procedures to audit e-mail correspondence for the following (1) customer service, (2) quality of care provided via e-mail, (3) quality of the response provided to the patient via e-mail (4) review for possible legal risks, (5) monitor patient privacy and confidentiality, and (6) evaluate adherence to organizational, industrial, legal, and regulatory guidelines.
Analysis	**Task**	Revise master patient index policy/procedures to address the capture of information from e-mail. Include the patient's e-mail address and other identifiers that will be used in verifying patient identity on e-mail correspondence.
Analysis	**Task**	Develop a standardized template for e-mail to ensure appropriate information is communicated and captured in a concise fashion.
Analysis	**Task**	Select an electronic messaging application or method that safeguards PHI and can be transmitted and received regardless of platform. Software should have encryption or other appropriate alternative that prevents unauthorized access or tampering with the electronic communication.
Analysis	**Task**	Develop polices and procedures on archiving and electronic backup of e-mail.
Application	**Task**	Update current confidentiality policies to incorporate references to e-mail if they are not already in place.
Application	**Task**	Establish a policy for e-mail turnaround time. The policy should prioritize e-mail messages by type of request, clearly identify what may constitute an urgent or emergent request, and describe the actions to take when the turnaround time is not met.
Application	**Task**	If the practice has a Web site, periodically check hyperlinks to verify status and remove any inactive or nonworking links. Maintain an archive of referenced Web sites, patient educational materials, and other information that is communicated electronically.
Application	**Task**	Educate staff and physicians on policies and procedures for patient e-mail. Include education on the proper content of messages and e-mail etiquette, when e-mail is appropriate/inappropriate,

		storing the e-mail in the medical record, etc. Include training on HIPAA security and privacy regulations with regard to e-mail and the potential risks associated with electronic messaging.
Application	**Task**	When communicating confidential medical information via e-mail, a banner should be displayed prominently at the beginning of the e-mail message such as, "THIS IS A CONFIDENTIAL MEDICAL COMMUNICATION. THIS COMMUNICATION CONTAINS MATERIAL PROTECTED BY DOCTOR-PATIENT PRIVILEGE."
Application	**Skill**	Knowledge of e-mail system configuration and document management capabilities (such as method for classifying e-mail messages).
Application	**Skill**	Ensure that information systems have access controls, firewalls, and computer-use policies in place that safeguard PHI.
Application	**Skill**	Sufficient knowledge of electronic messaging application, security controls, and platform to allow for effective communication with information systems professionals.
Application	**Task**	Manage physician and patient expectations on the use of e-mail (i. e., turnaround time, limitations of e-mail).
Application	**Task**	Obtain a signed authorization form from patient, and provide policy and procedure guidelines to patients on the use of patient-provider e-mail. Answer questions posed by the patient as necessary.
Understanding	**Task**	Providers should respond to patients by using the "reply to sender" button. Do not use the "reply all" feature just in case the sender copied the e-mail to others.
Understanding	**Task**	Generate an automatic reply to acknowledge receipt of patient's e-mail message and inform the patient about expected turnaround time and other general e-mail use policies.
Understanding	**Task**	Maintain a patient e-mail list in a central database or systemwide directory and keep the e-mail list secure.

HIM Managers Tasks and Skills with Regard to Patient Education and Confidentiality

Level	Skill/Task	
Analysis	**Task**	Define patient identifiers, besides the patient's full legal name, that will be used to verify patient identity and facilitate filing in the medical record. Suggested patient identifiers: date of birth, last six digits of social security number, patient's phone number, mother's maiden name, password created by the patient. Organization procedures must support the retention of these data elements in the patient registration system, and e-mail templates may include these items on the form as prompts to the patient.
Analysis	**Task**	Develop policies on the conditions in which patients may send or receive a patient-provider electronic communication. Examples may include ▪ Request for appointment ▪ Request for prescription refills ▪ Nonurgent medical advice ▪ Communications regarding billing ▪ Test results based on professional judgment ▪ Clinic changes ▪ Updating medical/surgical history ▪ Appointment reminders Include in policy in which situations e-mail should not be used (i. e. urgent or emergent situations, protected communications such as communicating HIV test results, mental illness, alcohol, or drug addiction). When problem is too complex to be handled with e-mail, patient should schedule an appointment with the physician. Develop guidelines on when to escalate from e-mail to phone call or an office visit.

Analysis	**Task**	Develop policies and procedures for verifying patient e-mail address on a periodic basis (e. g. annually, quarterly, at each visit).
Analysis	**Task**	Periodically review patient educational materials that are attached to e-mail to ensure they are current and still applicable.
Application	**Task**	Educate patients on the use of patient-provider e-mail to include ▪ Facility policies and procedures ▪ Potential risks and limitations of e-mail. Risks may include information that the use of e-mail in the workplace may be insecure even if using encryption, data contained on a workplace computer belongs to his or her employer and may be accessed at any time without his or her permission. ▪ Instruct patients on who processes e-mail and the situations in which their messages would be saved in their medical record. ▪ Instruct patients on format of e-mail (i. e., category in subject line, name and ID in the body of the message). ▪ Instruct patients on hours of e-mail operations and expected turnaround time of response.
Application	**Task**	Instruct patients that e-mail correspondence with the provider will not be allowed if they do not adhere to written guidelines. Develop a policy and procedure to guide the termination of patient from e-mail communication (patient notice, registration indicator that they do not participate in e-mail).
Application	**Task**	Document training in the patient's medical record, and reference training materials given to the patient.
Understanding	**Task**	Inform patients in advance when e-mails may be forwarded to other clinics/providers (e. g. referrals or consults).

HIM Managers Tasks and Skills with Regard to Electronic Document Management

Level	Skill/Task	
Analysis	**Task**	Identify existing, enterprise-wide repositories that securely store (or should store) e-mail records and attachments that merit evidentiary handling.
Analysis	**Task**	Select an e-mail management system that (1) includes a centralized archive, (2) has dependable search capabilities as well as fast and efficient access to the archive, (3) has an open architecture allowing for compatibility with the popular e-mail systems, and (4) the system enforces e-mail archiving policies.
Analysis	**Task**	Create appropriate rules, policies, and procedures upon system deployment to eliminate the risk of purging e-mail attachments in a storage crisis when elimination of carbon and blind copies would be a more prudent step in the purging process.
Analysis	**Task**	Establish a methodology to meet the HIPAA requirement for providing an accounting of disclosures.

Clinical and Medical Staff Tasks/Skills

Level	Skill/Task	
Understanding	**Skill**	Knowledge of electronic messaging software and hardware.
Understanding	**Skill**	Knowledge of HIPAA security regulations.
Understanding	**Skill**	Risk management training on the use of patient e-mail (security, e-mail etiquette, medical record documentation, appropriate situations for e-mail).
Analysis	**Task**	Develop clinical guidelines for conditions and situations where electronic communication is appropriate.

Application	**Task**	Triage e-mail to appropriate staff member or physician (medical questions, refills, scheduling, etc.).
Application	**Task**	Knowledge and compliance with state licensure requirements regarding online communication with patients outside state of licensure.
Application	**Task**	Knowledge and compliance with facility policies and procedures on e-mail.
Application	**Task**	Follow policies and procedures for storing e-mails in the patient's medical record.
Understanding	**Task**	Verify patient identity on e-mail when received, and use the reply (not reply all) feature with responding to patient's e-mail.
Understanding	**Task**	Verify e-mail address of patient prior to initiating an e-mail. Follow office policy on patient identifiers for e-mail. Verify that the e-mail address is typed accurately.

Clerical Staff Tasks/Skills

Level	**Skill/Task**	
Understanding	**Skill**	Knowledge of electronic messaging software; how to send a secure message and how to open a secure message.
Understanding	**Skill**	Understanding of good e-mail to include etiquette and concise and clear wording.
Understanding	**Skill**	Knowledge of HIPAA security regulations.
Understanding	**Skill**	Knowledge and compliance with facility policies and procedures on e-mail.
Application	**Task**	Follow policies and procedures for storing e-mails in the patient's medical record.
Understanding	**Task**	Risk management training on the use of patient e-mail.
Understanding	**Task**	Verify patient identity on e-mail when received, and use the reply (not reply all) feature with responding to patient's e-mail.
Understanding	**Task**	Verify e-mail address of patient prior to initiating an e-mail. Follow office policy on patient identifiers for e-mail. Verify that the e-mail address is typed accurately.

Explanation of Skill/Task Levels

Understanding	Definition: Recall, recognition, knowledge of framework and content (basic)
	Description: Requires only the recall or recognition of specific factual information, which generally does not vary relative to the situation. Memory alone is required at this level.
Application	Definition: Comprehension, translation, extrapolation, and interpretation of meaning (intermediate)
	Description: Requires the comprehension, interpretation, or manipulation of concepts or data, in which the response or outcome is situationally dependent, but not overly complex (i. e. knowledge that varies based on a situation). Examples of application questions may include basic calculations (applying a formula), recognition of a pattern, finding relationships between concepts (e. g., how does x relate to y? or compare and contrast x and y, or if-then questions).
Analysis	Definition: Appropriate application of knowledge using analysis, synthesis, and evaluation in new situations (advanced).
	Description: Requires integration or synthesis of a variety of concepts or elements to solve a specific problem (i. e. evaluating and rendering judgments on complex problems with many situational variables). Frequently, several steps are needed to select the correct answer.

Appendix B

Documentation of Authorization to E-mail Discussion

Date _____

I wish to communicate with my provider via e-mail. I have received patient education that included a review of the benefits, risks, and appropriate use of e-mail communication. I have been given the opportunity to ask questions.

I understand the benefits, risks, and appropriate use of e-mail communication.

I have received a copy of the e-mail guidelines and agree to abide by them.

Patient signature _____

Patient's e-mail address _____

Witness _____

File in EHR or paper record.

Patient's e-mail address can be permanently posted in a database when signed to e-mail authorization is received.

For discussion purpose only. Not for use without advice of legal counsel.

Appendix C

Patient Authorization for E-mail Communication

Patient should initial next to each statement.

- I would like to communicate via e-mail with my provider.
- I have been given an information sheet with guidelines for e-mail with my provider and have been given the opportunity to ask questions.
- I understand that all e-mail communication, this authorization, and a copy of the e-mail guidelines I have received will be filed in my permanent medical record.
- I agree to follow the guidelines for e-mail communication with my provider and will use e-mail for nonemergency purposes only.
- I agree to inform this office in writing if my e-mail address changes.

My current e-mail address _____

Signature _____

Print full name _____

Witness _____ Date _____

Change of e-mail address. This is to inform you that my e-mail address has changed.

My e-mail address has changed FROM: _____

My e-mail address has changed TO: _____

Signature _____

Print Name _____

Witness _____ Date _____

For discussion purpose only. Not for use without advice of legal counsel.

Appendix D: Summary of Best Practices for Provider-Patient E-mail Communication

Most patient-provider electronic communications, in-cluding all containing protected health information, are subject to the same storage, retention, retrieval, medicolegal, privacy, security, and confidentiality provisions as any other patient-identifiable health information.

Security

- E-mail system security must be sufficient to ensure the following to the highest degree possible
    - Nonrepudiation
    - Messages are read only by their intended recipients
    - Verification of delivery/ receipt
    - Labeling of sensitive material
    - Control of access by those other than the provider
    - Security of computer hardware
    - Completeness
    - Trustworthiness
- Strive to retain the integrity of the message and authentication of source.
- Configuration management is essential. Software must be monitored even after installation for upgrades and correct versus default settings, especially after a server crash.
- A secure Web server is purchased and managed by system security professionals.
    - Extensive network infrastructure (firewalls, routers, intrusion detection system).
    - Encryption software is available for wired and wireless communication.
    - Follow guidelines for transmission security in the HIPAA security rule.
- Establish and enforce procedures for cleaning hard drives.

Privacy

- Establish a policy and educate patients about appropriate types of e-mail (e. g., prescription refills, appointment scheduling, lab results) and queries that will not be responded to via e-mail (e. g., HIV, mental health).
- Electronically copy and paste e-mail addresses and/ or use the reply button to minimize mistyped e-mail addresses.
- Answering e-mail messages from home requires the clinician to have a private e-mail address with privacy and security procedures in place.
- The clinician must not communicate with patients in the context of their professional relationship using personal e-mail accounts such as America Online, Earthlink, or any other nonemployer e-mail system.
- Requests from patients to discuss subject matter that is not appropriate for the electronic medium should be resolved via telephone or in person. The following topics should not be discussed in e-mail transactions

- Protected diagnosis (e. g., mental health, substance abuse)
- Communication related to a diagnosis of HIV/AIDS
- Workers' compensation injuries and disability
- Confusing or abnormal test results
- New diagnoses
- Bad news
- Anything urgent

- When communicating confidential medical information via e-mail, a banner similar to the one below should be displayed prominently at the beginning of the e-mail message:
  THIS CONFIDENTIAL COMMUNICATION CONTAINS INFORMATION PROTECTED BY PROVIDER-PATIENT PRIVILEGE.

Administrative and Medicolegal

- Policies should be in place to establish criteria for e-mail communication with patients.
  - The physician and patient should have a prior established relationship.
  - Develop criteria to determine a patient's health literacy level and ability to use an e-mail application.
  - There should be a patient-clinician agreement for informed consent to use e-mail as a communication medium.
  - The patient must agree to indemnify the provider for information loss due to technical failures.
  - Patients must register e-mail addresses and provide identifying information.
- Develop procedures for the patient-clinician authorization/ agreement
  - Where the authorization will be filed
  - How it will be retrieved
  - What indicator/ flag shows that an authorization is on file
- Develop and enforce policies defining and prohibiting emergency e-mail messages.
- A workable documentation mechanism should be in place for responding to e-mail via telephone call and responding to a telephone call via e-mail.
- Use the signature line for all outgoing messages to communicate important guidelines and information, such as
  - Physician's full name and contact information
  - Response time
  - Instructions for when response time is not met
  - Instructions for urgent communication and patient emergencies
  - Other abbreviated guidelines as needed
- Web pages used as links or given to patients should reflect active links and credible Web sites.
- Maintain an archive of referenced Web sites, patient education materials, and other information that may be communicated electronically.
- The patient should initiate e-mail messages. Providers should respond to patients by using the reply button.
- Include the patient's original message in any reply.
- The original e-mail, with reply, should be filed in the electronic record or printed for the paper record. The provider should initial and date the paper copy for the paper record.
- Develop policies and procedures for retention and storing (filing) e-mail messages in the paper medical record or electronic health record.
- Use e-mail system functionality (e. g., automatic reply to acknowledge receipt or notify senders that the physician is out of the office, return receipt to confirm patient receipt).
- Develop policies and procedures to guide the use of group e-mail messages. For example, patients should not see names of all intended receivers.
- Establish a central patient registration database that will serve as a systemwide directory to prevent duplications and errors in the patient's e-mail information
- Verify/ update patient e-mail addresses in the database when notified of changes.

- Patient name without other identifiers is not appropriate. Medical record numbers will not be a relevant identifier if e-mail is being forwarded to another healthcare facility (e. g., for a referral). Suggested patient identifiers are
    - Date of birth
    - Last six digits of social security number
    - Phone number
- A healthcare entity should have a standardized template for e-mail in place to ensure the appropriate information is communicated and captured.
- Lengthy e-mail messages or prolonged correspondence with a patient may necessitate scheduling an appointment with the patient or calling the patient.
- Establish a policy for e-mail turnaround time. It should include
    - Priority for different types of messages
    - Identification of what may require urgent, emergent handling
    - Instructions for when the turnaround time is not met
- Audit e-mail correspondence for
    - Appropriate customer service
    - Quality of care provided
    - Quality of the response provided
    - Potential legal liability or medicolegal risk
    - Patient privacy and confidentiality
    - Adherence to applicable guidelines
    - Follow-up on e-mail messages returned due to incorrect addresses
- Educate staff in the use of electronic communication:
    - Avoid anger, sarcasm, harsh criticism, and libelous references to third parties
    - General e-mail etiquette
    - Risk management training

Patient Education

- Instruct patients on what information must be included in the e-mail message
    - Patient name and identification
    - Name of the healthcare provider
    - Appropriate use of the subject line to identify the type of message in order to facilitate response time (e. g., prescription refill, appointment, billing question)
- Inform patients on the hours of e-mail operations and expected response time.
- Instruct patients to contact the office by phone if they do not receive a response to an e-mail within the expected time frame.
- Instruct patients to acknowledge receipt of e-mail.
- Inform patients of the privacy/ security risks associated with the use of e-mail
    - Forwarding, interception, and unintended receipt of e-mail
    - Loss of confidentiality when using employer's e-mail or shared computers
- Inform patients that e-mail correspondence will be terminated for patients who repeatedly do not adhere to the written e-mail guidelines.
- Inform patients of general e-mail practices, such as
    - E-mail messages may be forwarded to other clinics or clinicians (e. g., referrals).
    - E-mail messages become part of the patient's permanent medical record and are discoverable for legal purposes.

    - Office personnel will be screening e-mail messages.

- Patients should be educated about the appropriate types of transactions for e-mail communications. Examples of when e-mail is appropriate include

    - Prescription renewals
    - Nonurgent medical advice
    - Test results, based on professional judgment
    - Insurance inquiries
    - Benefit information
    - Provider network information
    - Billing information
    - Scheduling/ canceling/ rescheduling appointments
    - Clinic/ provider changes
    - Other nonurgent communication

- Document training in the patient's medical record and reference training materials given to the patient.
- Clarify the guidelines; remind patients of their responsibilities. Document such discussions in the patient's health record.

Electronic Document Management

- Identify existing, enterprise-wide repositories that securely store (or should store) e-mail records and attachments that merit evidentiary handling.
- Develop or acquire an easy-to-use e-mail management system that includes a centralized archive.
- The system should have

    - Intuitive methods for identifying e-mail classification (e. g., patient medical information versus business communications)
    - Retention rules
    - Dependable search capabilities
    - Fast and efficient access to archives
    - Open architecture allowing for compatibility with popular e-mail systems
    - Retention rules triggered automatically by actions
    - A method to enforce e-mail archiving policies

- Create appropriate rules, policies, and procedures upon system deployment to eliminate the risk of purging e-mail attachments in a storage crisis.
- Establish a methodology for providing an accounting of disclosures (as required by HIPAA).
- Word documents sent as attachments stay on the hard drive.

Prepared by

This practice brief was developed by the following AHIMA e-HIM work group:

Marti Adkins, RHIA
Nancy Russell Cardamone, RHIA
Ray Chien, MS
Angela Clark, RHIA
Lynn Crothers, RHIT
Carmella Jackson, MS, RHIA, NMCC
Stephanie John, RHIA
Bassam Kawwass, RHIA
Sandra Kersten, RHIA
Gail Kraft, RHIA
Catherine Krawetz, RHIT, CCS
Lynda Mitchell, RHIA, CPHQ

David Mozie, PhD, RHIA
Deborah Nieves, RHIA
Harry Rhodes, MBA, RHIA, CHP (staff)
David Sweet (staff)
Mary Stanfill, RHIA, CCS, CCS-P (staff)

Acknowledgements

For assistance in the development of this practice brief:
Deborah Kohn, MPH, RHIA, CHE, CPHIMS, FHIMSS

Source: AHIMA e-HIM Work Group on E-mail as a Provider-Patient Electronic Communication Medium and its Impact on the Electronic Health Record (October 2003)
