E-Mail Security

Save to myBoK

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

Background

More and more people are using e-mail to communicate with friends, family, colleagues, and businesses. However, only a small percentage of physicians and healthcare providers regularly use e-mail to communicate with patients.

Advantages

The advantages of e-mail communication between providers and patients are numerous and include the elimination of telephone tag and voice mail messages; the ability to attach educational materials or test results; and improved documentation as compared to that traditionally associated with telephone calls and physician recollection of patient-provider discussion. When used in addition to, rather than as a substitute for, face-to-face communication, e-mail may also enhance the patient/provider relationship.

Risks

There are risks, however, associated with the use of e-mail by patients and providers to discuss health-related matters. The risks include information leakage, data integrity violations, repudiation, and others. Following is a brief overview of the major issues.

Information Leakage

- Employers and online services retain the right to archive and inspect messages transmitted through their systems.[1]
- Either party might accidentally send an e-mail to the wrong person.
- E-mail might be left visible on an unattended terminal.
- E-mail can be printed, circulated, forwarded, and stored in numerous paper and electronic files.
- E-mail is discoverable for legal purposes.
- A person authorized to access the information might use it for an unauthorized purpose or disclose it to an unauthorized party.
- Confidential health information might be obtained by an unauthorized entity from discarded media.
- E-mail may be vulnerable to computer hackers who could then transmit the information for illegitimate purposes.
- Phony e-mail could dupe legitimate users into voluntarily giving up sensitive information.

Data Integrity Violations

- E-mail is easily intercepted and altered without detection.[2]

- E-mail can be used to introduce viruses into computer systems.
- An impostor can forge e-mail.

Repudiation

- A party to the communication could falsely deny that the exchange of information ever took place.

Other Risks

- The sender may assume, but doesn't necessarily know, that his/her message was delivered.
- The recipient might not check his messages within the time frame the sender expects.
- The attachments embedded in the e-mail might be in a format the recipient's software can't read.
- E-mail can be misinterpreted. Without verbal and nonverbal feedback, the sender can't confirm that his/her messages are understood.

Safeguards can be devised and implemented against most threats. However, these are not without costs.

Legal and Regulatory Requirements

Federal statutes and regulations that address patients' right to privacy of health information include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Medicare Conditions of Participation, and the Code of Federal Regulations relative to Alcohol and Drug Abuse.

HIPAA contains requirements that health information be protected against threats to security, integrity, and unauthorized use. A notice of proposed rule making (45 CFR, Parts 160-164) published Nov. 3, 1999, proposed standards to protect the privacy of individually identifiable health information maintained or transmitted electronically in connection with certain administrative and financial transactions.

The Conditions of Participation with which healthcare facilities must comply to be eligible for Medicare funds vary based on the healthcare entity. The conditions are as follows:

- Hospitals: "The hospital must have a procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records."[3]
- Home health agencies: "Clinical record information is safeguarded against loss or unauthorized use."[4]
- States and long term care: "The resident has the right to personal privacy and confidentiality of his or her personal and clinical records."[5]
- Comprehensive outpatient rehabilitation facilities: "The facility must safeguard clinical record information against loss, destruction, or unauthorized use."[6]
- Critical access hospitals: "The facility must safeguard the clinical information against loss, destruction or unauthorized use."[7]
- Outpatient physical therapy services furnished by physical therapists in independent practice: "Clinical record information is recognized as confidential and is safeguarded against loss, destruction, or unauthorized use."[8]

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. Section 5 U.S.C. 552a (e) (10) of the act is very clear: federal systems must "establish appropriate administrative,

technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[9] Further, a HCFA Internet Security Policy issued in November 1998 states that "a complete Internet communications implementation must include adequate encryption, employment of authentication or identification of communications partners, and a management scheme to incorporate effective password/key management systems." The policy is meant to establish the basic security requirements that must be addressed to transmit HCFA Privacy Act protected and other sensitive HCFA information over the Internet.

Excerpt from HCFA Internet Security Policy

Acceptable Encryption Approaches

Note: As of November 1998, a level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (defined as 112-bit equivalent for symmetric encryption, 1024-bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve Systems) is recognized by HCFA as minimally acceptable. HCFA reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brut-force exhaustive search).

Hardware-based Encryption:

1. Hardware encryptors: While likely to be reserved for the largest traffic volumes to a very limited number of Internet sites, such symmetric password "private" key devices (such as link encryptors) are acceptable.

Software-based Encryption:

2. Secure Socket Layer (SSL) (sometimes referred to as Transport Layer Security-TLS) implementation: At minimum SSL level of Version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Socket Layer are acceptable.
3. S-MIME: Standard commercial implementations of encryption in the e-mail layer are acceptable.
4. In-stream: Encryption implementations in the transport layer, such as pre-agreed passwords, are acceptable.
5. Offline: Encryption/decryption of files at the user sites before entering the data communication process is acceptable. These encrypted files would then be attached to or enveloped (tunneled) within an encrypted header and/or transmission.

Acceptable Authentication Approaches:

Authentication (This function is accomplished over the Internet, and is referred to as an "in-band" process.)

1. Formal certificate authority-based use of digital certificates is acceptable.
2. Locally managed digital certificates are acceptable, providing all parties to the communication are covered by the certificates.
3. Self-authentication, as in internal control of symmetric "private" keys, is acceptable.
4. Tokens or "smart cards" are acceptable for authentication. In-band tokens involve overall network control of the token database for all parties.

Acceptable Identification Approaches:

Identification (The process of identification takes place outside of the Internet connection and is referred to as an "out-of-band" process.)

1. Telephonic identification of users and/or password exchange is acceptable. Exchange of passwords and identities by US Certified Mail is acceptable.
2. Exchange of passwords and identities by bonded messenger is acceptable.
3. Direct person contact exchange of passwords and identities between users is acceptable.
4. Tokens or smart cards are acceptable for identification. Out-of-band tokens involve local control of the token databases with the local authenticated server vouching for specific local users.[10]

While specific medical e-mail legislation has not emerged at the federal level, Congress has included e-mail within the definition of "telemedicine." Thus, any telemedicine interaction between a patient and provider requires informed consent, not only because medical information might be obtained, transmitted, or stored during the telemedicine consultation, but also because patients are engaging in a specific medical procedure.[11]

Because states determine policy on licensure to practice medicine within state boundaries, a practitioner with a license in one state may be at risk of violating another state's licensing laws when engaging in e-mail consultation, diagnosis, or treatment in another state. Prior to engaging in an electronic consultation with or about a patient, physicians should be aware of potential licensing issues, particularly when interacting across state lines.[12]

Most states prohibit physicians from disclosing information concerning the care and treatment of a patient. Many have statutes outlining specific requirements for the disclosure of patient information relative to mental health and sexually transmitted disease. Some state statutes address re-disclosure of health information.

Ethical Considerations

Even where the law does not specifically recognize a right to patient privacy, the medical profession has. The Hippocratic Oath declares "Whatever, in connection with my profession, or not in connection with it, I may see or hear in the lives of men which ought not be spoken abroad I will not divulge as reckoning that all should be kept." Further, the American Medical Association's Principles of Medical Ethics state "A physician may not reveal the confidence entrusted to him in the course of medical attendance, or the deficiencies he may observe in the character of patients, unless he is required to do so by law or unless it becomes necessary in order to protect the welfare of the individual or of the community."[13]

Accreditation Standards

The Joint Commission on Accreditation of Health Care Organizations' hospital, ambulatory care, and long term care standards IM.2 require that "confidentiality, security, and integrity of data and information are maintained."

Recommendations

Prior to establishing e-mail communication with patients, providers should:

1. Conduct a risk assessment that includes consideration of applicable laws and standards.

2. Establish a rigorous information security infrastructure that includes policies and procedures; training and awareness; and appropriate technology and architecture to protect health information against threats to security and integrity, unauthorized access, and repudiation.

3. Explain the inherent risks and benefits to patients, and obtain both an informed consent relative to the use of e-mail and telemedicine consultations.

4. Describe the types of individuals who may see patient e-mail messages, such as office staff, consultants, or those covering during physician absence.

5. Inform the patient that e-mail correspondence will be printed and placed in his or her paper record.
6. Inform the patient about intended response time.
7. Provide patients with e-mail guidelines for communicating with providers.
8. Configure an auto reply to acknowledge receipt of the patient's initial message, such as "Dr. Jones has received your e-mail and will attempt to process your request within one business day." Modify the auto reply if circumstances are such that no one will be responding to e-mail for an extended period of time.
9. Generate a new reply e-mail message upon completion of the patient's request.
10. Include footers that invite patients to escalate communication to a telephone call or office visit.
11. Print all messages, message replies, and confirmation receipts and place in the patient's paper record.
12. When composing e-mail, recognize that all e-mail is discoverable in legal proceedings.
13. Maintain a list of patients who communicate electronically in case it becomes necessary to notify a group of patients of an impending shutdown for network maintenance or technical difficulties.
14. When sending a group e-mail, address the e-mail to the sender with a blind copy to the intended recipients to keep recipients invisible to one another.
15. Avoid using patient e-mail addresses in marketing.
16. Never forward patient-identifiable data to a third party without the patient's express permission.

In communicating with providers, patients should:

1. Understand the risks associated with using electronic mail to discuss private health information with healthcare providers.
2. Understand the risks associated with telemedicine consultations.
3. Include the category of their question in the subject line, e.g., medical advice or billing question.
4. Include their full name and medical record number in the first line of the body of their message.
5. Use the auto reply feature to notify the provider that they received the provider's e-mail.
6. Print a hard copy for their personal records.

Both patients and providers should:

1. Limit personal e-mail communication to their homes.
2. Double-check the recipient's address.
3. Protect the security of their passwords.
4. Be careful about leaving programs operational and/or documents visible when computer terminals are unattended.

5. Make use of screen savers with private passwords or automatic sign-off.

6. Communicate via e-mail only those things they're comfortable having forwarded.

7. Avoid using e-mail for particularly sensitive matters.

8. Avoid using e-mail for time sensitive messages.

9. Take time to make sure the message is clear and concise, and cannot be misconstrued.

Note: The American Society for Testing and Materials (ASTM) Subcommittee E31.17 on Confidentiality is currently working on a new standard for e-mail transactions. Once finalized, the standard will be added to other confidentiality and security standards published by ASTM.

Prepared by

Gwen Hughes, RHIA
Professional Practice Division, AHIMA

Acknowledgments

Mary Brandt, MBA, RHIA, CHE
Gretchen Murphy, MEd, RHIA
Harry Rhodes, MBA, RHIA

Notes

1. Spielberg, Alissa. "Online Without a Net: Physician-Patient Communication by Electronic Mail." *American Journal of Law and Medicine*, 25 (1999): 282.

2. Spielberg, Alissa. "Online Without a Net." 270.

3. Health Care Financing Administration, Department of Health and Human Services. "Conditions of Participation for Hospitals." *Code of Federal Regulations*, 1998. 42 CFR, Chapter IV, Part 482.24.

4. "Conditions of Participation for Home Health Agencies." *Code of Federal Regulations*, 1998. HCFA, HHS, 42 CFR, Chapter IV, Part 484.48. Available online at http://www.access.gpo.gov/nara/cfr/cfr-table-search.html.

5. "Conditions of Participation for State and Long Term Care Facilities." *Code of Federal Regulations*, 1998. HCFA, HHS, 42 CFR, Chapter IV, Part 483.10.

6. "Conditions of Participation for Specialized Providers," *Code of Federal Regulations*, 1998. HFA, HHS, 42 CFR, Chapter IV, Part 485.60

7. "Conditions of Participation for Specialized Providers," *Code of Federal Regulations*, 1998. HCFA, HHS, 42 CFR, Chapter IV, Part 485.638.

8. "Conditions for Coverage of Specialized Services Furnished by Suppliers," *Code of Federal Regulations*, 1998. HCFA, HHS, 42 CFR, Chapter IV, Part 486.161.

9. "HCFA Internet Security Policy." Available online at www.hcfa.gov/security/isecplcy.htm.

10. *Ibid*.

11. Spielberg, Alissa. "Online Without a Net." 287-289.

12. *Ibid.* 291.

13. "Code of Medical Ethics: Current Opinions With Annotations." American Medical Association, Chicago, IL: 1996.

References

Ford, Warwick. *Computer Communications Security. Principles, Standard Protocols and Techniques*. New Jersey: Prentice Hall PTR, 1994.

Health Data Management. *Comprehensive Guide to Electronic Health Records*. New York: Faulkner and Gray, Inc., 1999.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Ambulatory Care: 1999*. Oakbrook Terrace, IL, 1999.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Hospitals: The Official Handbook. Refreshed Core January 1999*. Oakbrook Terrace, IL, 1999.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Long Term Care: 1998-99*. Oakbrook Terrace, IL, 1999.

Kane, Beverley, and Daniel Z. Sands. “Guidelines for the Clinical Use of Electronic Mail with Patients.” *Journal of the American Medical Informatics Association 5*, no. 1 (1998).

Sherman, Lynn, and Mark Adams. “Patients and E-Mail: Technology Means Increased Confidentiality Concerns.” *WMJ*, May/June 1999.

Issued February 2000
