Provider-Patient E-Mail Security (2003 update)

Save to myBoK

Editor's note: The following information replaces information contained in the February 2000 "E-mail Security" Practice Brief.

E-mail communication has become "as common as the fax machine in business settings."[1] In fact, the American Medical Association reports that 96 percent of physicians send or receive e-mail, and 25 percent of those physicians use e-mail to communicate with patients.[2] Clearly, e-mail is becoming another communication tool in healthcare.

Advantages

The advantages of e-mail communication between providers and patients are numerous. For example, e-mail:

- is an efficient way to respond to multiple non-urgent messages
- is retrievable at any site (for more mobile physicians)
- eliminates the "telephone-tag" problem
- is communication that may be saved and stored in a way that telephone and face-to-face communications cannot
- can be used to send test results with interpretations and treatment recommendations
- can be used to clarify treatment instructions or medication administration
- may be used to direct a patient to a specific Web site for more information

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

In addition to the benefits, there are risks associated with the use of e-mail by patients and providers to discuss health-related matters, including privacy breaches, data integrity violations, repudiation, and others. Following is a brief overview of the major issues:

Confidentiality Concerns

- Employers and online services retain the right to archive and inspect messages transmitted through their systems.[3] Personal messages between patient and physician would not be considered confidential.
- E-mail, because it is usually unencrypted, can be intercepted.[4] Although the probability of interception is low, the results of such interception can be harmful.
- An individual might accidentally send e-mail to the wrong person because addresses are not always intuitive and frequently change.
- 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 may be 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 transmit information for illegitimate purposes.
- Phony e-mail could dupe legitimate users into voluntarily giving up sensitive information or receiving incorrect or maliciously generated information.

Data Integrity Violations

- E-mail can be used to introduce malicious software into computer systems.

- An impostor can forge e-mail.
- E-mail can be altered, forwarded, and stored without detection.

Repudiation

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

Other Risks

- The sender may assume, but doesn't necessarily know, that his or her message was delivered.
- The recipient might not check his or her 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 or 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' rights to privacy of health information include 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 authorized use. The final privacy rule, published August 14, 2002, mandates standards to protect the privacy of individually identifiable health information maintained or transmitted electronically in connection with certain administrative and financial transactions.

The final security rule, published February 20, 2003, also mandates standards to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, or transmits.[5] The security rule indicates that covered entities must perform a risk analysis and then determine the level of e-mail security that is needed.

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."[6]
- Home health agencies: "Clinical record information is safeguarded against loss or unauthorized use."[7]
- State and long-term care: "The resident has the right to personal privacy and confidentiality of his or her personal and clinical records."[8]
- Comprehensive outpatient rehabilitation facilities: "The facility must safeguard clinical record information against loss, destruction, or unauthorized use."[9]
- Critical access hospitals (CAHs): "The CAH maintains the confidentiality of record information and provides safeguards against loss, destruction, or unauthorized use."[10]
- 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."[11]

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. Section 5 USC 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."[12]

Further, a Department of Health and Human Services (HHS) policy (still referred to as the 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."[13] The policy is meant to establish the basic security requirements that must be addressed to transmit HIPAA-protected 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.
2. Exchange of passwords and identities by US Certified Mail is acceptable.
3. Exchange of passwords and identities by bonded messenger is acceptable.
4. Direct person contact exchange of passwords and identities between users is acceptable.
5. 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.[14]

While specific medical e-mail legislation, other than previously mentioned in the security rule, 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.[15]

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.[16]

The HIPAA privacy rule addresses disclosure of information concerning the care and treatment of a patient. Many states have additional protections outlining the disclosure of patient information relative to mental health, substance abuse, and sexually transmitted disease.

Ethical Considerations

The medical profession recognizes the ethical necessity of patient privacy. 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 Report of the Council On Ethical and Judicial Affairs addresses e-mail as follows: "When using e-mail communication, physicians hold the same ethical responsibilities to their patients as they do during other encounters."[17]

Accreditation Standards

The Joint Commission on Accreditation of Healthcare Organizations' hospital, ambulatory care, behavioral health, home health, networks, critical care hospital, 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 an informed consent relative to both 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 maintained in the individual health record
6. Inform the patient about intended response time
7. Provide patients with e-mail guidelines for communicating with providers
8. Consider using an automatic reply to acknowledge receipt of the patient's initial message. 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 telephone calls or office visits if the patient would like further contact
11. Maintain all messages, message replies, and confirmation receipts electronically or in hard copy in the patient's healthcare record
12. Recognize that all e-mail is discoverable in legal proceedings
13. When sending group e-mail, address the e-mail to the sender in the blind copy section of the email address in order to keep recipients invisible to one another
14. Do not use patient e-mail addresses in marketing without the patient's consent
15. 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 their full name in the first line of the body of their message
4. Maintain a copy for their personal records

Both patients and providers should:

1. Double-check the recipient's address
2. Protect the security of their passwords
3. Be careful about leaving programs operational and/or documents visible when computer terminals are unattended
4. Make use of screen savers with private passwords or automatic sign-off
5. Communicate via e-mail only information they're comfortable having forwarded
6. Avoid using e-mail for particularly sensitive matters
7. Avoid using e-mail for time sensitive messages
8. Take time to make sure the message is clear and concise and cannot be misconstrued

Notes

1. Sands, Daniel Z. "Guidelines For the Use of Patient-centered E-mail." Massachusetts Health Data Consortium, Inc., 1999. Available at www.mahealthdata.org. (accessed July 2, 2003)

2. Mindy Schneiderman, director of market research and analysis, American Medical Association, telephone interview by author, March 2003.

3. Spielberg, Alissa. "Online Without a Net: Physician-Patient Communication by Electronic Mail." *American Journal of Law and Medicine* 25, no. 2/3 (1999): 282. Available online at www.acpenet.org/Forums/Positional/SmallPractice/Resources/Spielberg.pdf. (accessed July 2, 2003)

4. Ibid. 270.

5. "Health Insurance Reform: Security Standards Final Rule." 45 CFR, Part 164.306(a)(1). *Federal Register* 68, no. 34 (February 20, 2003). Available online at www.access.gpo.gov/su_docs/fedreg/a030220c.html.

6. Centers for Medicare & Medicaid Services, Department of Health and Human Services. "Conditions of Participation for Hospitals." *Code of Federal Regulations*, 2002. 42 CFR, Chapter IV, Part 482.24. Available online at www.access.gpo.gov/nara/cfr/cfr-table-search.html.

7. Centers for Medicare & Medicaid Services, Department of Health and Human Services. "Conditions of Participation for Home Health Agencies." *Code of Federal Regulations*, 2002. 42 CFR, Chapter IV, Part 484.48.

8. Centers for Medicare & Medicaid Services, Department of Health and Human Services. "Conditions of Participation for State and Long Term Care Facilities." *Code of Federal Regulations*, 2002. 42 CFR, Chapter IV, Part 483.10.

9. Centers for Medicare & Medicaid Services, Department of Health and Human Services. "Conditions of Participation for Specialized Providers." *Code of Federal Regulations*, 2002. 42 CFR, Chapter IV, Part 485.60.

10. Centers for Medicare & Medicaid Services, Department of Health and Human Services. "Conditions of Participation for Specialized Providers." *Code of Federal Regulations*, 2002. 42 CFR, Chapter IV, Part 485.638.

11. Centers for Medicare & Medicaid Services, Department of Health and Human Services. "Conditions for Coverage of Specialized Services Furnished by Suppliers." *Code of Federal Regulations*, 2002. 42 CFR, Chapter IV, Part 486.161.

12. The Privacy Act of 1974, Section 5 U.S.C. 552a. Available online at www.usdoj.gov/foia/privstat.htm. (accessed July 2, 2003)

13. "HCFA Internet Security Policy." Issued November 24, 1998. Available online at www.cms.hhs.gov/it/security/docs/internet_policy.pdf. (accessed July 2, 2003)

14. Ibid.

15. "Online Without a Net," 287-289.

16. Ibid. 291.

17. American Medical Association. "Guidelines for Physician-Patient Electronic Communications" (2002). Available online at www.ama-assn.org/ama/pub/category/2386.html (accessed July 2, 2003).

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: 2002. Oakbrook Terrace, IL: Joint Commission, 2002.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Hospitals: The Official Handbook. Refreshed Core January 2002*. Oakbrook Terrace, IL: Joint Commission, 2002.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Long Term Care: 2002*. Oakbrook Terrace, IL: Joint Commission, 2002.

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.

Revised By

Jill Burrington-Brown, MS, RHIA

Originally prepared by Gwen Hughes, RHIA

Acknowledgments

Mary Brandt, MBA, RHIA, CHE, CHP
Michelle Dougherty, RHIA
Beth Hjort, RHIA, CHP
Carol Quinsey, RHIA
Harry Rhodes, MBA, RHIA, CHP

Source: Burrington-Brown, Jill, and Gwen Hughes. "AHIMA Practice Brief: Provider-Patient E-mail Security" (Updated June 2003)