E-Mail Security (1997)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Background

In the current work environment, there are many ways to communicate with peers and customers (e.g., telephone, facsimile, US mail, in-person meetings, and electronic mail). Of these modes of communication, electronic mail (e-mail) is becoming increasingly popular.

As Americans and as healthcare professionals, we are becoming more comfortable with this communication medium. One survey of computer users found that e-mail is the most popular online activity; 75 percent of surveyed users said they had used e-mail in the past month.[1] It is estimated that 15 percent of Americans (approximately 30 million adults 16 years of age and older) use e-mail, up from 2 percent in 1992. Nearly 50 percent of the US population, or 135 million people, will communicate via e-mail by 2001.[2]

Among integrated healthcare delivery systems (IHDSs), e-mail is the most common enterprise-wide application in place, with 44 percent of IHDSs reporting that they currently use e-mail and 12.4 percent planning to add an e-mail application in the near future.[3]

But our increasing comfort level contributes to the greatest security risk involved in the everyday use of e-mail. By its very nature, e-mail use gives us a false sense of security. We are often alone in our office or home when we are communicating via e-mail. Would we be willing to speak aloud our e-mail thoughts if we knew that they were accessible to our associates or employer? If we knew that our messages were being collected, stored, and reviewed by some third party? If we knew that the recipients of our e-mail massages were forwarding them to others or storing our messages in files outside our control?

In becoming too comfortable with e-mail, we run the risk of falsely believing that our communications are private. Nothing could be further from the truth. If you are using your employer's e-mail system, your employer has a right to review every document you send. And what becomes of those messages after you've sent them? Recipients of e-mail messages can easily forward them to someone else or store them in unsecured files. You may think you have deleted a sensitive message, but chances are your old e-mail is stored somewhere.

On the Internet your risks increase. An unencrypted message on the Internet is very much like a postcard; it may be read by numerous individuals and even stored in many different systems before it is actually delivered. Some Internet service providers save e-mail messages in their databases, and at least one provider sells information about its users to third parties.

Legal and Regulatory Requirements

Laws that specifically address online privacy are still evolving. In the absence of specific laws addressing online confidentiality, it is important to remember that existing laws and regulations that apply to health information in paper form also apply to electronic health information.

Healthcare facilities operated by, or under contract with, the federal government are bound by the Privacy Act of 1974. Many individuals believe that the Privacy Act of 1974 provides privacy protection for all health records. In fact, the act provides limited control over the disclosure of information to other parties and only applies to information collected by the federal government and its agencies. The primary intent of the act is to allow individuals to discover, obtain, and correct or amend information collected about them by the federal government.

Public Law 104-191, the Health Insurance Portability and Accessibility Act signed into law in August 1996, may pave the way to federal guidelines for electronic health information. The law requires that the secretary of Health and Human Services (HHS) submit recommendations to Congress within 12 months on standards with respect to the privacy of individually identifiable health information. The law also mandates Congress to enact legislation within 36 months of enactment of the act. Should Congress fail to enact legislation, the secretary of HHS is required to publish final regulations within six months of Congress's deadline.

Laws regarding health information are in place in many states. Healthcare organizations considering the use of e-mail should take these laws into consideration.

Security Considerations

The most successful security measures combine effective policies with proven security hardware and software tools. A process-driven, enterprise-wide security plan should be in place before an organization decides to begin using e-mail to communicate sensitive information. The organization should have a clear understanding of its business process, so as not to introduce security measures that have a negative impact. In some ways, e-mail is similar to other types of communication tools. It would be wise to use existing communication policies, perhaps for the use of fax machines or the telephone, as guides when developing an e-mail security policy.

Among the most important issues related to e-mail security are encryption, storage, and disclosure and redisclosure.

Encryption

Encryption, one of the oldest forms of security, should be taken into consideration when an organization is preparing to purchase an e-mail system. When encryption is used, a mathematical algorithm is employed to prevent unauthorized individuals from seeing information they shouldn't see.

There are many types of encryption algorithms in use today, but the two forms that seem to be best suited for use in healthcare are the Data Encryption Standard (DES) and Rivest, Shamir, and Adleman (RSA). DES was developed by the federal government and is defined in Federal Information Processing Standards Publication 46. RSA, named for its inventors, is a patented algorithm.

The DES algorithm uses the same private key to both encrypt and decrypt information. The protection of the information is dependent on the secrecy of the key. RSA is a public key algorithm, using separate keys to encrypt and decrypt. An organization can choose to keep both key values secret or publish the value of one key and keep the second secret.

In the DES algorithm, both the sender and the recipient of the message know the same key value. In the RSA algorithm, system users have three choices:

1. Both keys can be kept private
2. The sender can send to a recipient using the recipient's public key. The recipient would use the private key value to decode the information. Using this arrangement would guarantee that only the recipient would view the document
3. .The sender utilizes the private key and the recipient utilizes the public key. This arrangement guarantees to the intended recipient that the message received was sent by only the sender[4]

The point at which encryption occurs will have an effect on the security of your organization's messages. Use of encryption for messages sent via the Internet will not protect messages within an organization. Messages stored and transmitted in clear text within an organization and encrypted just prior to leaving the internal network are open to internal security breaches.

Remember that even if your organization has a solid information security program, not all organizations do. In some places systems and network personnel are routinely assigned privileges that permit them to read e-mail or perhaps impersonate other senders. In this case it is not always reasonable to trust the validity of incoming messages. Procedures for determining when to confirm the source of incoming messages by another means should be provided.

Storage Issues

If e-mail is used to communicate confidential patient health information to patients or other providers, the e-mail documents containing the confidential health information must comply with existing laws and regulations with regard to record retention and security. The enterprise will need to develop a process to incorporate e-mail messages into the existing medical record. For facilities with paper records, the e-mail messages should be printed and filed in the paper record. And in facilities with computer-based patient records (CPR), applications that integrate e-mail files should be incorporated into the CPR. Furthermore, the enterprise should ensure that policies and procedures address the retention and storage of e-mail archive files, as directed by state and federal laws.

An enterprise should also consider developing procedures to address e-mail messages stored by a person who has left the organization. Should those stored messages be deleted or reviewed? These questions should be resolved.

Disclosure and Redisclosure

By design, e-mail provides users with a multitude of ways to move information through a network quickly and easily. The same features that make e-mail a powerful communication tool also prevent it from being used as a secure system. Encryption and other security measures may protect the information in transit and prevent unauthorized users from entering your system, but once your e-mail message reaches its destination, you have lost all control over it.A recipient of your e-mail message can:

- Forward the message to an unlimited number of people
- Print out the message an unlimited number of times
- Leave the message on the screen for anyone in the area to view
- Store the message in an unsecured file
- Forward the message to a mailing list or bulletin board service
- Alter the original message

What's more, if the recipient of an e-mail message is using his or her employer's e-mail system, that employer has a right to view any message in the system.

A security policy and signed user confidentiality agreements will raise awareness and ensure compliance by most users. Policies should clearly delineate circumstances under which e-mail should be forwarded and distributed to multiple recipients. However, policies and procedures cannot guarantee that security breaches -- accidental or deliberate -- will never occur.

Recommendations

Ideally, before an enterprise decides to use e-mail it should develop a security policy. The enterprise should begin by conducting a comprehensive information security assessment. This risk assessment should indicate the value of the information in question, the risks to which this information might be subject if sent in an e-mail message, and the possible controls that might be put in place to protect this information. The enterprise should consider developing a centralized security mission statement.

To ensure that information security is woven into the fabric of an organization, employees could be asked to sign security agreements. Job descriptions and procedures should be updated to include information security requirements. The organization should attempt to clearly delineate confidential and nonconfidential information.

Ultimately, every e-mail user must know what information should never be included in an e-mail message. Security risks can be reduced by providing training, policies, and procedures that focus on ethics and information security before any new computer application is introduced. Policies and procedures should be coordinated with appropriate security software and hardware.

It is only by fully understanding the issues and risks of using e-mail that healthcare organizations will be able to successfully master the technology without compromising patient privacy.

Notes

1. Intelligent Information Group. Worldwide Internet/On-line Tracking Service. Austin, TX: Intelligent Infor-mation Group, 1997.
2. Delhagen, Kate. "E-mail Explodes." Cambridge, MA: Forrester Research, 1997.
3. Miller, Dale W. "Using Encryption to Protect Health Information." *In Confidence*, 3 no. 6 (1995): 7-8.
4. Siwicki, Bill. "Enterprise Networks-Strategies for Integrated Delivery Systems." *Health Data Management*, 5 no. 2 (1997): 56.

References

Borzo, Greg. "The ABCs of e-mailing patients." *American Medical News* 38, no. 34 (1995): 5.

Brandt, Mary. "On the Line: Professional Practice Solutions." *Journal of AHIMA* 67, no. 4 (1996): 31.

Ernst & Young LLP. "Healthcare Cybervison: The Role of the Internet in Healthcare." New York: Ernst & Young LLP, 1996.

Miller, Dale W. "Internet Security: What Health Information Managers Should Know." *Journal of AHIMA* 67, no. 8 (1996): 56-58.

Miller, Dale W. "Preserving the Confidentiality of E-mail Communications." *In Confidence* 4, no. 5 (1996): 4-6.

Moody, Gibbs. "Electronic Information Security Software." New York: UBS Securities, Equity Research, 1996.

Morrissey, John. "Securing the Internet Frontier." *Modern Healthcare* 26, no. 43 (1996): 56-64.

Shiver, Art. "Peeping Toms in Cyperspace: If You Think You Are Alone, Think Again." *Computer Currents* 5, no. 3 (1997): 14-18.

Wood, Charles C. "Policies from the Ground Up." *Information Security News* 8, no. 2 (1997): 24-29.

Prepared by

Harry B. Rhodes, MBA, RRA, Professional Practice Division

Acknowledgements

Assistance from the following individuals is gratefully acknowledged:

Mary Brandt, MBA, RRA, CHE
Donna Fletcher, MPA, RRA
Dale W. Miller
Jill Callahan Dennis, JD, RRA
Jim Braden
Carl Uhla
Julie King, RRA
Donald Kellogg, RRA
Patrice Spath, ART

Issued June 1997

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.