Email security in clinical practice: ensuring patient confidentiality

David M. Kreindler

David M. Kreindler, BSc, MD, FRCP(C), is with the Division of Youth Psychiatry, Department of Psychiatry, Sunnybrook Health Sciences Centre, and the Mood and Anxiety Program, Department of Psychiatry, University of Toronto.

Competing interests: None declared.

Correspondence: Dr. David Kreindler, Department of Psychiatry, Sunnybrook Health Sciences Centre, 2075 Bayview Avenue, Room FG-62, Toronto ON M4N 3M5; david.kreindler@utoronto.ca

Note: Elements of this article were presented as a part of a workshop at the annual meeting of the Canadian Psychiatric Association (CPA) in Vancouver in November 2005 and at a CPA continuing medical education online forum in 2006.

Electronic mail (email) enjoys wide acceptance among the general public but has more limited acceptance among physicians. A 2005 survey found that 46% of Canadian physicians used email to communicate with colleagues for clinical purposes. Although email can be extremely useful, physicians need to appreciate the potential hazards of using email in clinical practice. The College of Physicians and Surgeons of Ontario (CPSO) has noted that “e-mailing or faxing unencrypted patient health information is really no more secure than sending that information on a postcard,” and that “those physicians who wish to send personal health information by email should use an encrypted or otherwise secure system.” The American Medical Informatics Association has offered similar guidance.

This article outlines how email works, introduces the basics of encryption, and highlights the important role that encryption has to play in the clinical use of email. It does not recommend specific pieces of commercial software, since both software and encryption technology are constantly evolving.

Clinical vignette

A specialist visits a clinic in a remote city to provide consultations. While there, the physician dictates consultation notes that are transcribed by the clinic staff. The transcribed notes are sent at a later time by email to the consultant for review and editing; they are then returned to the remote clinic by email for distribution and inclusion in the patient record.

Question 1: Does the use of email in this scenario result in risks to confidentiality?

Yes, there are definite potential risks. To understand why, it is essential to first understand how email works.

How email works

Email is not sent; it is copied. In contrast to a regular letter sent via the postal service, an email message is not carried from one computer to another; rather, the original message is copied to the remote location, while the original copy remains at the sending location, in a manner similar to what happens in the transmission of a facsimile (fax).

Copies of email are generated on multiple computers. Email is relayed via a network of client and server computers, such that one copy is generated at each computer participating along the way (Fig. 1). This process is documented in the header of each email message and can be inspected if the header is viewed (Fig. 2). In principle, a copy of the original message could be accessed by anyone with computer expertise, physical or network access to any one of these computers, and the necessary passwords. Typically, servers retain copies of emails that they relay only temporarily, in order to conserve storage space; however, these copies are not necessarily deleted immediately. Moreover, servers are typically backed up from time to time, so there is no guarantee that copies of email in temporary storage on a server will not be preserved indefinitely as part of a backup.

Can you be sure that the sender’s and receiver’s computers are secure? Many personal computers (PCs) are used by more than one person — for example, by family members at home or colleagues at work. Moreover, some operating systems — notably, most versions of Windows — are not configured by default to
Figure 1: Email transmission. Email is relayed via a network of client and server computers. An email client — typically a personal computer (PC) running an email program such as Microsoft Outlook, Mozilla Thunderbird, Netscape Mail, or Qualcomm Eudora — does two things: it lets you compose an email message, then it transmits the message to an email server. A server, typically a corporate computer connected to the Internet (shown in grey), inspects the destination address of each incoming email and checks if it knows where to find the computer belonging to the addressee. If it does, it copies the message to the destination computer; if it does not, it copies the email message to another mail server that should have information about how to connect with the addressee’s computer. If email is transmitted via an intranet — a network of clients (“A” and “B”) and servers (shown in green) exclusively owned and operated by a single organization, such as with some hospitals — copies of the email (also shown in green) will not be generated outside this intranet. This will be more secure to the extent that only employees of the organization have access to the computers that make up this network. In contrast, email transmitted in whole or in part via the Internet (e.g., from client “A” to client “C”) will generate a trail of copies (shown in orange) on one or more servers. In general, it is difficult to ascertain the security of the Internet servers (shown in grey) that are part of this trail.

restrict one user's ability to access other users' files. Thus, it is possible that persons other than the sender or the intended recipient may be able to access email messages not intended for them on the sender's or recipient's computer. Also, it is possible for unauthorized users to impersonate physicians if the computer is not properly configured.

Summary. In this vignette, email is sent from clinic to consultant via mail servers on the Internet; the owners and operators of the servers are unknown. There are three loci at which someone could intercept and potentially read the clinic notes: the sender’s computer; any of the mail servers that relayed the email; and the recipient’s computer. Even if one demands that the sender and the recipient be responsible for securing access to their computers, copies of the email are generated at each of the servers; confidentiality could be breached at any one of them.

Question 2: What reasonable steps could be taken to decrease the risk to patient confidentiality?

In practice, there are two straightforward solutions.

1. Strip the consultation note of all identifying patient information. However, this is typically inconvenient and time-consuming.
2. Encrypt the email. If an email is the Internet equivalent of a postcard, the encryption process acts as an envelope.

How encryption works

Cryptography, encryption and decryption. Cryptography refers to processes for converting text from a readable to an unreadable format (“encryption”) and back again (“decryption”). Modern cryptographic systems generate a set of random digits that are then protected using a password or passphrase selected by the user, creating the key. The key is used to scramble (i.e., encrypt) the text. If viewed while encrypted, the text appears to be a string of random incomprehensible characters. Only when provided with the proper key can the original text be unscrambled (i.e., decrypted) into the original text.

Modern cryptographic systems can be divided into two broad classes,\(^\text{13}\) based on how keys are handled: secret key (or symmetric key) systems, and public key systems. These are summarized in Table 1.\(^\text{13-29}\)

How secure is an encrypted document? An encrypted document’s security — its ability to resist being read by unauthorized third parties — depends on (i) the strength of the encryption system that is being used, and (ii) the strength and confidentiality of the key. If a password protecting either the sender’s or the
recipient's key is intercepted by a third party (e.g., by being overheard, stolen, inadvertently disclosed, etc.) or the key is discovered, the document is no longer secure. Broadly speaking, there are three ways by which an unauthorized third party can decrypt and read (“crack”) an encrypted message when the sender's or recipient's computer is secure:

1. **Guessing the password.** A thorough discussion of password selection is beyond the scope of this article. Briefly, if a cryptosystem’s key is protected by a user-supplied password, the key is vulnerable to anyone with access to the system. The degree of vulnerability depends on the strength of the user-supplied password. Words found in a dictionary are poor (“weak”) choices, since they are relatively easy to guess, as are birth dates, phone numbers, maiden names, etc., or any minor variations of these. Unusual combinations of letters, numbers, and punctuation are better choices, as are long multi-word combinations with interspersed numbers or punctuation. Long random character sequences are “strongest,” i.e., hardest to guess, but these can be difficult to remember.*

*One way to remember multiple passwords is to use password management software. Password management software lets you record all your passwords in a single database, which is then encrypted with a single master password using high-level computer security, such as public key systems. One popular system is PGP. These systems have several advantages:

- **Password reuse** is avoided, so if you lose your password you must contact the recipient to change it.
- **Advantages:** Less computer-intensive (i.e., requires fewer calculations) but has comparable security to public key systems.
- **Disadvantages:** Requires prior communication to agree on encryption software and a password. Moreover, if you are concerned about the security of email, using email to discuss which password will be used is senseless!
- **Examples:** Most commercial word-processing, spreadsheet, or compression software that allows documents to be saved with a password. Simple mail transfer protocol (SMTP) for sending plain text, or any mail client.
- **Revocation of keys:** If compromised, every person using the same password must be contacted to change the password.

Public key cryptosystems‡

- **Encryption / decryption:** Text is encrypted by the sender using the recipient’s public key and decrypted by the recipient using the recipient’s private key.
- **Examples:** S/MIME, PGP. Web browsers’ mechanisms for establishing secure connections to websites.
- **Advantages:** Requires no prior communication between recipients (if using compatible cryptosystems and digital certificates from a Certificate Authority).
- **Disadvantages:** Requires each correspondent to have published his or her public key (see “Getting started with encrypted mail”)
- **Examples:** Not all email client software (e.g., some webmail clients) is compatible.

‡ In practice, most “public key” cryptosystems are in fact hybrid public/secret key systems. Public key systems result in encrypted messages that are both substantially longer and require more computer time to create than a comparably strong secret key system. Therefore, most popular implementations of public key systems (such as S/MIME or PGP) (1) generate a random, one-time use session key, (2) use a public key system to securely transmit this session key between the sender and the recipient, and then (3) transmit the body of the message encrypted using this session key and a specified secret key cryptosystem.

---

| Table 1: Cryptosystem characteristics |
|---------------------------------------|
| **Class** | **Secret key cryptosystems** | **Public key cryptosystems‡** |
| Prerequisites | Sender and recipient must communicate with each other to agree on (i) encryption software and (ii) a key or password that will be used to encrypt and decrypt the message. | Sender and recipient must each (i) create a public / private key pair and (ii) publish the public key. (The private key is kept strictly confidential. (iii) Sender and recipient may need to communicate with each other to agree on encryption software if using incompatible software. |
| Encryption / decryption | Text is both encrypted and decrypted with the agreed-upon key or password. | Text is encrypted by the sender using the recipient’s public key and decrypted by the recipient using the recipient’s private key. |
| Password reuse | Avoid re-using passwords with different correspondents. If you mistakenly send an encrypted document to the wrong recipient, it will be protected against decryption only if that recipient does not know or cannot guess the password. | Your public/private key pair can be re-used with any number of correspondents. |
| Advantages | Less computer-intensive (i.e., requires fewer calculations) but has comparable security to public key systems. | Requires no prior communication between recipients (if using compatible cryptosystems and digital certificates from a Certificate Authority). |
| Disadvantages | Requires prior communication to choose encryption software and a password. Moreover, if you are concerned about the security of email, using email to discuss which password will be used is senseless! | Requires each correspondent to have published his or her public key (see “Getting started with encrypted mail”)
| Examples | Most commercial word-processing, spreadsheet, or compression software that allows documents to be saved with a password. | S/MIME, PGP. Web browsers’ mechanisms for establishing secure connections to websites. |
| Revocation of keys | If compromised, every person using the same password must be contacted to change the password. | PGP and certificate-based systems have ways of revoking a public key without a communication to each person using it. |

---

1. Analysis and Comment

Kreindler

Open Medicine 2008;2(2):e29–34
2. **Guessing the key.** It is theoretically possible to decrypt an encrypted message by guessing the key that was used to encrypt it. The advantage of this method is that it does not depend on access to the sender’s or receiver’s computer. The disadvantage is that the attack — referred to as a brute force attack — is extremely resource- and time-consuming. One example of successful brute force attacks is against the widely available but poorly implemented RC-4 encryption system\(^{13,17}\) included with Microsoft Word 2000.\(^{18}\) In principal, RC-4 is a good encryption system\(^{19}\); however, to comply with United States export laws,\(^{17,20,21}\) the implementation of RC-4 in Word 2000 is limited to \(2^{40}\) or \(1\,099\,511\,627\,776\) possible passwords (technically, a “40 bit key”).\(^{22}\) Although this may seem like a huge number, a modern computer capable of testing 100 million potential passwords per minute can exhaust all possible alternatives in approximately 10 days. Many inexpensive software tools and services for doing exactly this are available for purchase, e.g., by searching the Internet via www.google.com using keywords, “Word password decryption crack.” In contrast, one study estimated that, on average, it would take a dedicated 2001-vintage \$10 million computer longer than the lifetime of the universe to break a document encrypted using symmetric encryption and a random 128-bit key.\(^{23}\)

3. **“Breaking” the encryption system,** by finding a flaw in the math underlying the encryption system’s algorithm that can be exploited to decrypt the message. One may think of this type of attack as using an unplanned “shortcut” to a cryptosystem’s complex math problem. These kinds of shortcuts can appear in any cryptosystem, but have historically been found in cryptosystems that have been deployed with little or no peer review. One such example is the wireless encryption system used in many commercial and consumer wireless routers.

Any document encrypted with a weak key is vulnerable to guessing attacks.\(^{17}\) To defend against the possibility of poor key choice, some encryption systems (such as PGP, described below) automatically generate random keys. In general, if a strong key is paired with a robust encryption system — that is, one based on Triple-DES,\(^{13,17}\) AES/Rijndael,\(^{25}\) Blowfish,\(^{17,26}\) ECC,\(^{17,27}\) RSA,\(^{13,17}\) or one of the others that have survived peer review and/or public contests\(^{28}\) and thus can be considered reliable — the chance of unauthorized decryption is very small.

**Getting started with encrypted email**

In general, by default, most email programs transmit email *without* encryption. Although encryption is increasingly being incorporated into widely available software, no single standard for encrypted email presently exists. The closest to a single standard for public-key encrypted email, S/MIME,\(^{13,28}\) has been incorporated into many but not all popular email software packages, although it requires some infrastructure to work. Another popular implementation is PGP (“Pretty Good Privacy”).\(^{17,29}\) The following steps are key for those wishing to start using encrypted email with colleagues, patients, or others:

1. Select cryptographic software compatible with that of your correspondents.
2. Become proficient with your email and encryption software.
3. Ensure that you are using strong passwords and keys, and keep them confidential.
4. For secret key cryptosystems, decide on a shared password and communicate it to your correspondent securely.

For public key cryptosystems, each correspondent will need to publish his or her public key. How this happens depends on the specific implementation chosen. S/MIME users require a digital certificate (also known as a public key certificate) from a certificate authority.\(^{17,30}\) A certificate authority is deemed to be implicitly trustworthy; it verifies an applicant’s identity, then issues a digital certificate. The digital certificate specifies the applicant’s email and certifies that the public key, which is included in the certificate, belongs to the applicant. Anyone wishing to send email to a user looks up the user’s public key in the certificate.
authority's database online. In contrast, every PGP user generates and distributes his or her own public key. Rather than relying on the certificate authority to verify identities, PGP uses other users to vouch for the validity of each others' public keys, thereby creating an interconnected “web of trust.”

Keys and trust signatures can be hosted on PGP key servers, further simplifying this process.

Acknowledgements: The author thanks Deborah Fenichel, PhD, and Dr. Tarek Loubani, MD, for their careful reading and detailed critique during the preparation of this manuscript.

REFERENCES

1. Dryburgh H. Changing our ways: Why and how Canadians use the Internet. Ottawa: Statistics Canada; 2000 (accessed 2006 Aug 16). [Full Text]
2. U.S. Census Bureau. Purpose of computer use at home for people 18 years and over using a computer at home, by selected characteristics. Current Population Survey, October 2003. Washington, DC: United States Census Bureau; 2003 (accessed 2006 Aug 16). [Full Text]
3. Sands DZ. Help for physicians contemplating use of e-mail with patients. J Am Med Inform Assoc 2004;11(4):268–9. [PubMed] [Full Text]
4. Canadian Medical Association and Canada Health Infoway. Physician Technology Usage and Attitudes Survey. Ottawa: Canadian Medical Association; 2005. [Full Text]
5. Mandl KD, Kohane IS, Brandt AM. Electronic patient-physician communication: problems and promise. Ann Intern Med 1998;129(6):495–500. [PubMed] [Full Text]
6. College of Physicians and Surgeons of Ontario. Privacy Legislation. Members’ Dialogue. Toronto: The College; 2004 (accessed 2006 Aug 16).
7. College of Physicians and Surgeons of Ontario. Medical Records Policy #5-05-2. Overview and Organization of Medical Records. Toronto: The College; 2005 (accessed 2006 Aug 16). [Full Text]
8. Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail. J Am Med Inform Assoc 1998;5(1):104–11. [PubMed] [Full Text]
9. Klenins J. AT&T Laboratories; 2001 (accessed 2006 Nov 20). [Full Text]
10. Freed N, Borenstein N. Base64 content-transfer-encoding. Network Working Group Request for Comments: 2045 — Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. First Virtual; 1996 (accessed 2006 Aug 16). [Full Text]
11. Tugend T. UCLA to be first station in nationwide computer network. In: Kleinrock L, Norman JM. editors. From Gutenberg to the Internet: A Sourcebook on the History of Information Technology. HistoryofScience.com; Novato, CA: 2005. p 869–70. (accessed 2008 June 16). [Full Text]
12. Schneier B. Desktop Google finds holes. EWeek. 2004 (accessed 2006 Feb 12). [Full Text]
13. RSA Laboratories. RSA Laboratories’ frequently asked questions about today’s cryptography, version 4.1. Bedford, MA: RSA Security, Inc; 2004 (accessed 2006 May 30). [Full Text]
14. Schneier B. MySpace passwords aren’t so dumb. 2006. [Full Text]
15. Schneier B. Choosing Secure Passwords. 2007 (accessed 2007 Feb 20). [Full Text]
16. Microsoft Corporation. Strong passwords: How to create and use them. 2006 (accessed 2007 Feb 20). [Full Text]
17. Schneier B. Applied Cryptography: protocols, algorithms, and source code in C. Mississauga, ON: John Wiley & Sons; 1995.
18. Microsoft Corporation. Word 2000 9.0.6926 SP-3. Redmond, WA: Microsoft Corporation; 1999.
19. Schneier B. Microsoft RC4 Flaw. 2005 (accessed 2006 Feb 14). [Full Text]
20. Levy S. Crypto. New York: Penguin; 2001.
21. Wikipedia contributors. Export of cryptography. Wikipedia. The Free Encyclopedia. 2006 (accessed 2006 Nov 20). [Full Text]
22. Microsoft Support. Changes in encryption file properties in Office 2003 and Office 2002. Redmond, WA: Microsoft Corporation; 2006 (accessed 2006 Aug 16). [Full Text]
23. RSA Laboratories. Bulletin 13: A cost-based security analysis of symmetric and asymmetric key lengths. Bedford, MA: RSA Security Inc; 2001 (accessed 2006 May 30). [Full Text]
24. RSA Laboratories. Cryptographic Challenges. Bedford, MA: RSA Security Inc; 2004 (accessed 2006 May 30). [Full Text]
25. Technology Administration, US Department of Commerce. AES–FIPS–197. Washington, DC: 2001. May 21, 2006 [Full Text]
26. Schneier B. The Blowfish encryption algorithm. (accessed 2006 May 30). [Full Text]
27. Certicom. Introduction to ECC. Mississauga, ON: Certicom Inc; 2006 (accessed 2006 May 30). [Full Text]
28. Ramsdell B. Network working group request for comments: 2033: S/MIME version 3 message specification. Worldtalk; 1999 (accessed 2006 Nov 20). [Full Text]
29. Network Associates, Inc. An Introduction to Cryptography. Santa Clara, CA: Network Associates Inc; 1999. [Full Text]
30. Netscape Communications Corp. Glossary: Certificate Authority (CA). 2001 (accessed 2007 Feb 23). [Full Text]

Citation: Kreindler DM. Email security in clinical practice: ensuring patient confidentiality. Open Med 2008;2(1):e29–34.

Published: 8 July 2008

Copyright: This article is licenced under the Creative Commons Attribution ShareAlike 2.5 Canada License, which means that anyone is able to freely copy, download, reprint, reuse, distribute, display or perform this work and that the authors retain copyright of their work. Any derivative use of this work must be distributed only under a license identical to this one and must be attributed to the authors. Any of these conditions can be waived with permission from the copyright holder. These conditions do not negate or supersede Fair Use laws in any country. For further information see http://creativecommons.org/licenses/by-sa/2.5/ca/.

Further reading

Email Security [web page on the Internet]. Toronto: Computing and Networking Services, University of Toronto; c2004 [cited 2006 May 30]. Available from: www.utoronto.ca/security/UTORprotect/email.htm

RSA Laboratories’ Frequently Asked Questions About Today’s Cryptography, Version 4.1 [monograph on the Internet]. Bedford, MA (USA): RSA Security Inc; c2000 [cited 2006 May 30]. Available from: www.rsasecurity.com/rsalabs/faq/files/rsalabs_faq41.pdf

Bruce Schneier: Crypto-Gram [newsletter on the Internet]. A free monthly newsletter commenting on security issues and security technology. Available from: www.schneier.com/crypto-gram.html

Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons; 1996. An introductory text for anyone interested in the details of modern applied cryptography. Technical yet very readable.