Metanoia Communications
info@metanoia.org
http://www.metanoia.org

Safeguarding Patient Confidentiality in E-Mail

If you allow your e-mail address to be known – if it is published on any web page, or printed in any directory, or on your business card or letterhead – then you are available to your patients by e-mail, as surely as if you give them your phone number. In which case:

1. You are responsible for your e-mail communications in the same way you are responsible for your telephone communications.
2. You must take responsibility to check your e-mail as you do your answering machine or voice mail.
3. You must explain to patients the limitations of e-mail communication, especially with regard to:
   a. Availability (make sure patients know e-mail is probably not a good way to reach you in an emergency)
   b. Confidentiality (both you and the patient must take precautions)

The two problems:

A. Internet e-mail in transit is vulnerable. Although it's unlikely, e-mail in transit can easily be read by technicians at any intermediate computers between you and your patient (including AOL or your ISP); by NSA security programs; and by system administrators on a workplace network.

B. Unless you take precautions, e-mail and files on your computer, or your patient's computer, are vulnerable. They may easily be read by other persons for whom they were not intended.

The solutions:

A. The safest solution is abstinence: completely avoid communicating with patients via e-mail.
   1. *Do not allow patients to know your e-mail address.*
   2. *Never communicate anything via e-mail that you would not want printed in the newspaper.*

B. However, to be honest, most therapists do use e-mail to communicate with patients.

continue next page...

Metanoia Communications
info@metanoia.org
http://www.metanoia.org

If you (like most therapists) do communicate with patients via e-mail, use adequate precautions:

A. Protect e-mail in transit by using encryption.

1. Option 1: install and use an encryption program. They are inexpensive and reasonably easy to use.
   a. **ZixMail** http://www.zixmail.com/ (free download then $24 per year)
   b. **PGP** http://mcafeestore.beyond.com/ ($30 for business use, works with any existing e-mail program, plug-ins for Outlook and Eudora, encrypts files and disks too)
2. Option 2: instead of e-mail, use secure web-based messaging. Messages never leave the server and so cannot be intercepted, and nothing is stored on your computer or your patient's.
   a. **ZipLip** http://www.ziplip.com (free)
   b. **HushMail** http://www.hushmail.com (free)

B. Protect e-mail and files from being seen by others.

1. Never leave your computer unattended while it is running – especially while connected to the Internet. If you walk away, use a password-protected screen saver, or lockout program.
2. Make sure other persons ***cannot*** sit down at your computer and send or receive e-mail. (Do not and would not are not adequate; go for cannot.) Do not store your e-mail password in your e-mail program; set up your e-mail so that you must type your password every time to send or receive e-mail.
3. Password-protect your computer. If you share your computer with anyone else (including family members or other therapists), password-protect files containing patient communications. Move old e-mail onto diskettes, encrypt them, and store under lock and key.
4. For passwords, select a meaningless string of characters, not a word. Use punctuation characters if possible. A good password looks like this: j47!K4%u
5. Double-check every e-mail before sending it, to make sure it is correctly addressed.
6. If you print e-mail on paper, safeguard the paper adequately.
7. If you use a laptop, be very careful to avoid its theft.
8. If you employ system administrators with access to your computers, make them sign a legal agreement that they will not read e-mail. Otherwise they probably will, because they can.
9. Tell your patients to follow similar precautions.