

# Addressing NASW Standard 1.07m Privacy and Confidentiality

Contributed by Stephen M. Marson, Ph.D., ACSW, and Ollie Bishop, MBA

Unlike most NASW ethical standards, 1.07m Privacy and Confidentiality operates under an implicit assumption that social workers must be aware of customary technological precautions necessary for privacy and confidentiality. Social work education has no formal accreditation standard to assure this assumption is being met. Although much is written on social work ethics and some about ethics related to technology, we continue to witness social workers mishandling and misinformed about technology in general and password protection/encryption specifically. The ethical implications related to password and encryption security are outlined in this article. Here, we introduce specific strategies for compliance with NASW Standard 1.07m.

NASW's Standard 1.07m Privacy and Confidentiality states:

Social workers should take precautions to ensure and maintain the confidentiality of information transmitted to other parties through the use of computers, electronic mail, facsimile machines, telephones and telephone answering machines, and other electronic or computer technology. Disclosure of identifying information should be avoided whenever possible.

This standard requires social workers to understand the technological aspect of information transmission over the Internet. Two dimensions for compliance exist for this standard:

password construction conventions and standards  
encryption protocols

First, social workers need to understand that NO password or encryption is totally secure. However, some are more secure than others.

## E-Mail Ethical Fundamentals

The traditional analogy for explaining the transmission of e-mail is "it is like sending a postcard through the U.S. mail." As soon as a postcard is mailed anyone can read it, make a copy, and make the contents available for anyone who wants the information. Like the postcard, the sender has no method of knowing if the e-mail has been captured, copied, and distributed. Analyzing e-mail, in fact, is more complex than postcards. If a postcard is delayed, one might suspect foul play. When e-mail is captured, copied, and distributed, no delay can be detected—even if one tracked the time it took to transmit the e-mail!

According to NASW Standard 1.07m Privacy and Confidentiality, social workers who employ e-mail with clients have an ethical obligation to understand the level of confidentiality for the type of e-mail being sent. Figure 1 illustrates the current levels of security of transmitted e-mail. The higher the level, the more secure the transmission is.

Figure 1  
Confidentiality Levels

LEVEL 1: Sending e-mail with confidential information as an attachment with no password protection.  
Clear non-compliance with Standard 1.07m Privacy and Confidentiality

LEVEL 2: Sending e-mail with confidential information as an attachment with password protection, but the password does not comply with the conventional standard for password selection.  
Non-compliance with Standard 1.07m Privacy and Confidentiality

LEVEL 3: Sending e-mail with confidential information as an attachment with password protection, but the password complies with the conventional standard for password selection.  
Compliance with Standard 1.07m Privacy and Confidentiality

LEVEL 4: Sending e-mail with confidential information as an encrypted attachment.  
Clear compliance with Standard 1.07m Privacy and Confidentiality

LEVEL 5: Sending e-mail with confidential information as an encrypted attachment with a password.  
Best compliance with Standard 1.07m Privacy and Confidentiality

The question becomes: what must a social worker do in order to comply with Standard 1.07m Privacy and Confidentiality? Rules for Password Construction

Some methods of password creation are better than others. The level of confidentiality dictates the level of security. For protecting client information, NASW Standard 1.07m Privacy and Confidentiality requires the highest level of protection. Figure 2 includes the current standards for password creation.

If confidentiality is breached, failure to comply with standards of password creation rules can be grounds for a malpractice suit. Although these are the standard rules for password construction, the safest construction method is to employ software that randomly generates a password. When a social worker is transmitting confidential client information, a randomly generated password (which will never be used again) is the best compliance for Standard 1.07m.

Figure 2  
Password Creation Rules

- Password must have at least eight characters.
- Include punctuations, digits, and letters.
- Use a combination of upper and lower case letters.
- Do NOT write the password anywhere—memorize it.
- Use combination that makes the password easy to remember.
- Do not use any combination that can be found in any dictionary.
- Do not use a keyboard pattern such as qwertyui or oeuidhtn.
- Do not repeat any character more than once in a row.
- Do not use: phone numbers; friends', relatives', or dogs' names; any proper noun; dates.
- Use different passwords for each machine.
- Change the password every three months.
- Do not reuse passwords.
- Do not reverse words.

### Encryption

Whereas password protecting a file may be adequate for some file transfers, a higher level of security is required for others. Implicit within Standard 1.07m is the assumption that a social worker will know the difference between high and low security. Encrypting a file offers a much greater level of security. When a file is encrypted, the text of the file is scrambled in patterns that can only be unscrambled with the password or encryption key used to encrypt the file. Anyone intercepting and hacking the file will see what appears to be random text.

Many free and commercial programs exist that will encrypt/decrypt a file using password encryption/decryption or public/private key encryption/decryption. A public key and private key is a series of letters, numbers, and symbols used to encrypt/decrypt a file. Files encrypted with the AES algorithm or the Blowfish algorithm and e-mailed using a public/private key are virtually unbreakable. As the term implies, a public key is made available to the individuals to whom you wish to send sensitive files, and the private key is not disclosed. Each individual in the communication chain must have both a public key and private key and the software necessary to encrypt/decrypt the file. The public key and private key are a matched pair, and both are needed to encrypt/decrypt a file. To send encrypted information to an individual, you must know their public key.

To read an encrypted file that is received, the encryption/decryption program will match the receiver's public key in the encrypted file with the receiver's private key, which is stored on the receiver's computer. Once the two keys are matched, the receiver's private key will decrypt the file. The graphic in Figure 3 illustrates the process when Individual A sends Individual B an encrypted file.

Figure 3  
Individual A encrypts the clear text file before transmitting it to Individual B.

Generally, the sender of the file and the receiver of the file must use the same encryption/decryption software product. Although we recommend no particular software product, PGP Desktop Professional is a widely used comprehensive encryption/decryption software product that will, among other things, perform full disk encryption and e-mail encryption. It is available in a freeware version and a reasonably priced commercial version. Information on using the software product is available at [http://na.store.pgp.com/desktop\\_pro.html](http://na.store.pgp.com/desktop_pro.html). In our opinion, it would be imprudent to e-mail a highly sensitive file without encrypting it.

### Summary and Conclusion

The NASW Code of Ethics provides a general overview for the ethical expectations of all social workers. The standards do not offer guidance or technical support to comply with the individual ethical codes. Social workers are ethically responsible to keep abreast of changing technologies and the best methods to secure confidentiality.

### For Further Reading

Electronic Frontier Foundation. (1998). *Cracking DES*. Sebastopol, CA: O'Reilly & Associates.

Marson, S. M. (2000). Internet ethics. *The New Social Worker*, 7 (3), 19-20.

Marson, S. M., & Brackin, S. (2000). Ethical interaction in cyberspace for social work practice. *Advances in Social Work*, 1 (1), 27-42.

Marson, S. M., & Brackin, S. (1996). Therapy on the Internet: Confidentiality as a misnomer, Part II. *North Carolina Social Worker Newsletter*, 21 (6), 2, 6-7.

Stephen Marson, PhD., ACSW, is the Senior Editor and Ollie Bishop, MBA, is the Technical Advisor for the *Journal of Social Work Values and Ethics*. Both are professors at the University of North Carolina at Pembroke.