Many forensic mental health practitioners, including psychologists, psychiatrists, counselors, and social workers, use technology on a daily basis. Forensic mental health professionals should become familiar with ethical and legal responsibilities concerning confidentiality and the use of technologies such as telephones, cell phones, fax, e-mail, and chat. Becoming cognizant of the benefits and hazards in using technology will enhance the forensic practitioner's ability to practice risk management within his or her particular work setting.

Discussion

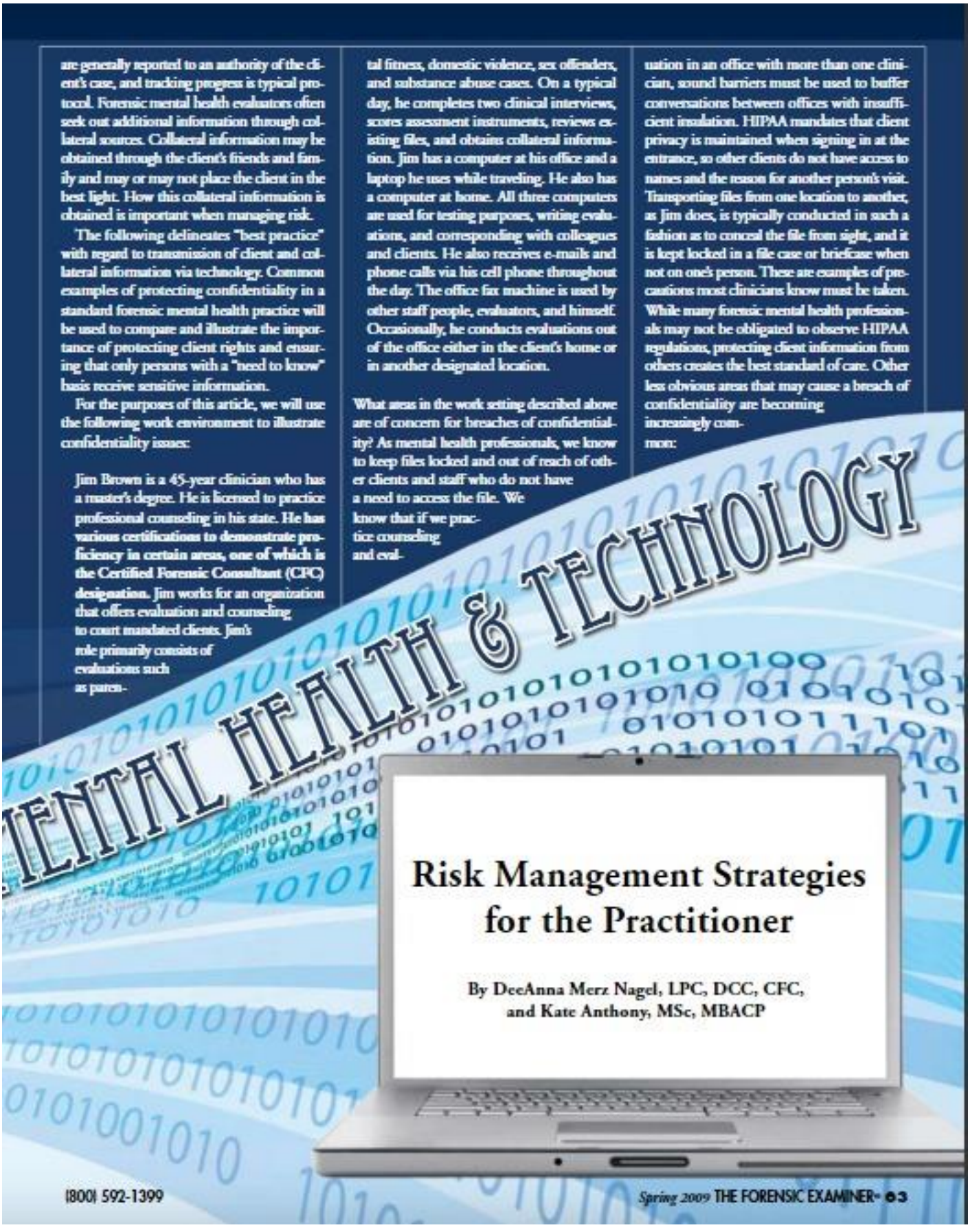
Technology is a common part of our work and personal lives. Using the computer to create documents, read and send e-mail, "Google" for information, and enter data to generate reports is a mainstream activity. Fax machines have become almost passé, but they are still used. Carrying a cell phone has become almost as commonplace as carrying a wallet or purse.

The use of this technology assumes certain risks for the forensic mental health practitioner that should be considered.

All mental health professionals, regardless of education and work setting, are familiar with the basic principles of confidentiality. During the informed consent process, forensic mental health professionals educate clients about the possible circumstances in which the information shared during a session might be shared with others. If the service is mandated by the courts, all of the information may be available to the courts. Otherwise, precautions are taken to ensure that the client's information remains confidential, following the dictates of laws such as HIPAA (Health Insurance Portability and Accountability Act), state licensing rules, and ethical code(s) of various mental health organizations (International Society for Mental Health Online, 2000).

However, many professionals do not consider the basic tasks performed every day as areas of practice that involve any particular risk. For example, many professionals rely on e-mail to make contact with clients or to set up appointments. Some professionals, after receiving the appropriate release of information, may use e-mail to send a report or summary to another mental health professional or a lawyer. Others encourage collateral sources to send information regarding a client via e-mail. The collateral information, sometimes regarded by the court as heresay, is used in writing certain forensic evaluations such as custody and parental fitness. This information may be flattering of the client's character or may contain inflammatory remarks and other negative information that may or may not be accurate.

In most cases, forensic mental health clients are court-ordered to obtain an evaluation and/or treatment. Because of the court order, the "client-therapist" privilege is not always pertinent. Results of the evaluation or treatment



are generally reported to an authority of the client's case, and tracking progress is typical protocol. Forensic mental health evaluators often seek out additional information through collateral sources. Collateral information may be obtained through the client's friends and family and may or may not place the client in the best light. How this collateral information is obtained is important when managing risk.

The following delineates "best practice" with regard to transmission of client and collateral information via technology. Common examples of protecting confidentiality in a standard forensic mental health practice will be used to compare and illustrate the importance of protecting client rights and ensuring that only persons with a "need to know" basis receive sensitive information.

For the purposes of this article, we will use the following work environment to illustrate confidentiality issues:

Jim Brown is a 45-year clinician who has a master's degree. He is licensed to practice professional counseling in his state. He has various certifications to demonstrate proficiency in certain areas, one of which is the Certified Forensic Consultant (CFC) designation. Jim works for an organization that offers evaluation and counseling to court mandated clients. Jim's role primarily consists of evaluations such as parental fitness, domestic violence, sex offenders, and substance abuse cases. On a typical day, he completes two clinical interviews, scores assessment instruments, reviews existing files, and obtains collateral information. Jim has a computer at his office and a laptop he uses while traveling. He also has a computer at home. All three computers are used for testing purposes, writing evaluations, and corresponding with colleagues and clients. He also receives e-mails and phone calls via his cell phone throughout the day. The office fax machine is used by other staff people, evaluators, and himself. Occasionally, he conducts evaluations out of the office either in the client's home or in another designated location.

What areas in the work setting described above are of concern for breaches of confidentiality? As mental health professionals, we know to keep files locked and out of reach of other clients and staff who do not have a need to access the file. We know that if we practice counseling and evaluation in an office with more than one clinician, sound barriers must be used to buffer conversations between offices with insufficient insulation. HIPAA mandates that client privacy is maintained when signing in at the entrance, so other clients do not have access to names and the reason for another person's visit. Transporting files from one location to another, as Jim does, is typically conducted in such a fashion as to conceal the file from sight, and it is kept locked in a file case or briefcase when not on one's person. These are examples of precautions most clinicians know must be taken. While many forensic mental health professionals may not be obligated to observe HIPAA regulations, protecting client information from others creates the best standard of care. Other less obvious areas that may cause a breach of confidentiality are becoming increasingly common:

Are computer screens in the office or at home visible to clients, staff, or others who do not have a need to know? Staff whose tasks involve data entry about clients should tilt the screen away from view, and a screen shield should be used. When using a laptop during travel, a screen shield should also be used to avoid intentional eavesdropping by others and to protect client names from the public.

Are computers password protected? One's home computer should be password-protected from family, friends, and guests. This concept applies to the work setting as well, and using the "need to know" principle can be helpful in gauging who should have access to the work computer. At the very least, the computer should be password-protected to prevent easy access to confidential information, particularly if the laptop or PDA is one's main personal computer, because it is at higher risk of being stolen. Additional precautions can include password-protecting document files and/or placing the files in encrypted storage that may be on the hard drive or hosted on the Internet via a third-party server. HIPAA-compliant file storage service is available at minimal cost.

Is the facsimile machine in an area of the office or home that offers confidential receipt of documents? Staff who do not have a need-to-know basis should not have access to incoming fax documents. If the practitioner works from home, the fax machine should be in a locked office. The fax can often be set not to print until activated by the recipient. These are important factors to consider when designing work flow in the work and home office setting.

Is the practitioner discussing confidential client information via a cell phone? Cell phone conversations are not a secure and confidential mode of communication. If a client calls with confidential information, or a collateral source returns a phone call, the caller should be advised of this, and every effort should be made to communicate in an alternative secure fashion. Landline phones are secure and VoIP (Voice over Internet Protocol) phone conversations via services such as Skype are secure and encrypted.

Does the practitioner use e-mail to confirm appointments and disseminate/receive information? Forensic evaluators may receive initial enquiries through e-mail. When responding, the evaluator should consider whether they are encouraging an open line of communication that is not secure. Standard e-mail is not secure or encrypted. Evaluators should make every effort to use encrypted e-mail with clients or collateral sources to protect the confidentiality of all parties ("Advice on Group Coverage", 2003). Intake forms, contractual agreements, and other seemingly innocuous documented information should not be passed through unencrypted e-mail (National Board for Certified Counselors, 2005). Many may think it unlikely that an e-mail will be intercepted, but the likelihood of someone breaking into one's office and stealing files is slim as well. Still, as professionals, we generally take certain precautions and keep files in locked file cabinets.

Is the practitioner using instant messaging (IM) or chat programs such as AOL or Yahoo? Although these IM or chat programs offer a convenient way to communicate, the service is not secure and encrypted (American Counseling Association, 2005). Best practice standards regarding e-mail are applicable to IM chat as well. Because we now know that e-mails can be traced and that chat room participants can be found (Manes, 2007), encryption is the electronic equivalent of the locked filing cabinet.

Has the practitioner incorporated these communication and confidentiality issues into the informed consent process? Allowing the client to understand the limitations of certain forms of communication encourages best practice, protects the client, and minimizes risk to the forensic mental health professional.

Conclusion

Forensic mental health practitioners work in different settings under different guidelines and authorities, including codes of ethics, licensing scopes of practice, and HIPAA regulations. Although one practitioner may not be mandated to comply with certain ethics or laws, all mental health practitioners should use guidelines and laws as formulation for "best practice." In doing so, forensic mental health practitioners avoid risks in the form of libel, slander, and breach of confidentiality.

References

Advice on group coverage, email us. (2003, May 16). *Psychiatric News*, 38(10), 36.

American Counseling Association. (2005). ACA code of ethics. Retrieved September 10, 2007, from http://www.counseling.org/Resources/CodeOfEthics/TP/Home/CT2.aspx

International Society for Mental Health Online. (2000). Suggested principles for the online provision of mental health services. Retrieved September 10, 2007, from http://www.ismho.org/builder/?p_page&id_214

Manes, G. (2007). Digital forensics in the twenty-first century. *The Forensic Examiner, 16*(4), 17.

National Board for Certified Counselors and Center for Credentialing and Education. (2005). *The practice of Internet counseling*. Retrieved September 10, 2007, from http://www.nbcc.org/assetmanager/files/ethics/internet-counseling.pdf

Earn CE Credit
To earn CE credit, complete the exam for this article on page 65 or complete the exam online at www.acfei.com (select "Online CE").

About the Author

DeeAnna Merz Nagel, LPC, DCC, CFC, is a psychotherapist, educator, and consultant. She maintains a private practice in Rumson, NJ. As a member of the ACFEI Forensic Counseling Advisory Board and past president of the International Society for Mental Health Online, she is keenly aware of the forensic mental health professional's responsibilities with regard to technology. Her specialties include the impact of technology on mental health including Internet addictions and social media.

Kate Anthony, MSc, FBACP, is CEO of OnlineCounsellors.co.uk, offering consultancy, training, and research on online counseling, psychotherapy, and the use of technology in mental health. She is past president of the International Society for Mental Health Online and ambassador for technology for the British Association for Counselling and Psychotherapy. She is co-editor of "Technology in Counselling and Psychotherapy: A Practitioner's Guide" with Dr. Stephen Goss (Palgrave 2003).

DeeAnna and Kate are co-founders of the Online Therapy Institute, which can be accessed at www.onlinetherapyinstitute.com.