VISTAS Online
ACA Knowledge Center
counseling.org/knowledge-center/vistas
703-823-9800 x281 | 800-347-6647 x281
By Drs. Garry R. Walz and Jeanne C. Bleuer of Counseling Outfitters, LLC | *Sponsored by the American Counseling Association*

Article 55

The ACA 2014 Code of Ethics and Technology: New Solutions to Emerging Problems

Timothy D. Baker and Juliana Delgado

Baker, Timothy D., is an associate professor in the School Counseling program at St. Cloud State University in St. Cloud, Minnesota.

Delgado, Juliana, is a graduate student in the School Counseling program at St. Cloud State University, Minnesota.

Abstract

The ACA 2014 Code of Ethics addresses counselors' responsibilities to changing technology and the obligation to keep client data confidential. For counselors who work in non-clinical settings, lack of access to HIPAA-compliant tools can present a bewildering set of choices. This document describes state-of-the-art tools that can be used by counselors in any setting to protect the integrity of face-to-face counseling sessions, confidentially maintain sole-possession notes, and practice discretion when searching the Internet for information resources pertaining to client's needs. Recommendations for ongoing training and awareness are presented.

The American Counseling Association's (ACA) Code of Ethics (2014) provides new directives to counselors who use technology. Counselors educate and inform their clients regarding the benefits and risks of social media use (ACA, 2014, section H.6.b); keep their clients' information confidential, informing them who will have access to these records (B.6.b, H.2.b); take all reasonable precautions including the use of electronic encryption technologies, where appropriate (H.2.d); and, when ordered by a court, narrowly limit the scope of information released in order to minimize harm to the client (B.2.d). Counselors who work in clinical settings may use HIPAA-compliant software that provides a mechanism to accomplish these goals, but other counselors may not, for reasons of cost and other factors. This latter group may include school counselors, graduate students, and counselors with non-clinical duties (such as advocates and trainers) who do not bill third parties for services. For these counselors, failure to keep adequate records and documentation of services may not be an ethical option (ACA, 2014, section A.1.b).

Composite Case Analysis

If you are a counselor who does not have access to software designed specifically for keeping medical records, would you know how to manage your ethical responsibilities if you were caught in either of these scenarios?

Scenario A. Carmen is returning from an international conference. On her laptop computer are several of her clients' case files; she has been using "down time" in the airport to discreetly finish typing several diagnostic assessments. On the last leg she must pass through security. Her laptop computer is completely encrypted, so Carmen believes these records are private. Several uniformed officials approach her and explain she has been selected for enhanced screening in accordance with anti-terrorism laws. She is ordered to turn on the laptop, log in, and thus demonstrate it does not pose a threat; if she refuses, she will be detained up to 15 hours and may be denied boarding the airplane. Carmen suddenly feels trapped in this foreign country. She complies with officials and logs in to her laptop. Powered up, her laptop is confiscated for several hours and returned. She is notified that officials made a complete copy of the hard drive for analysis by an anti-terror unit.

Scenario B. Greg is a counselor at the end of a long work day. His children are in the car as he has picked them up from an after-school program. Distracted, he runs a red light, and is almost immediately pulled over by city police. The officer explains that state law prohibits text-messaging while driving, and therefore he has cause to demand his cellular telephone to verify Greg was not texting. Greg is concerned that the officer may look at more than text-messaging, and asks if the officer has a warrant. The officer replies that if Greg does not cooperate, he will arrest him on the spot while a warrant is pending. Greg's wife is out of town; he realizes that if he is taken to jail, his children will be taken into emergency foster care, and his car towed. Fearing this impact on his family, Greg complies under duress. The officer checks Greg's text message history, which is clear. The officer then browses Greg's Facebook wall. A former client of Greg's employer, an addictions recovery center, has posted something (meant to be humorous) about her recent drinking escapades. The police officer takes a photo of the screen, and forwards it to the former client's current probation officer. Greg's former client is remanded to custody, and sentenced to additional time for violating the terms of her parole.

Could these scenarios occur in real life? In fact, they are composites of real events. Only one involved a helping professional, a psychologist, whose work laptop containing client case files was scrutinized while clearing security at Boston airport (Schmidt & Lichtblau, 2012). And many states now allow troopers to demand a driver's cellular telephone, including cases where search of the phone resulted in the arrest of a third party unrelated to the traffic stop. New guidelines at the U.S. Department of Justice allow prosecutors to use evidence obtained from a warrantless source if a judge can be presented with a plausible explanation why a warrant could have been justified on other grounds, a process called "parallel construction" (Fakhoury, 2013; Shiffman & Cooke, 2013). This may carry elevated potential to be harmful to one's current or former client. Thus, the above two scenarios are at least plausible.

Case Discussion

While the legal dimensions of technology are rapidly changing, counselors have some recourse. First, become familiar with laws of your area and seek qualified legal advice relative to your situation (ACA, 2014, section H.1.b). Equally important, these scenarios could have been avoided with the application of more sophisticated technology in accordance with ACA ethical principles. For example, "Greg," the counselor at a recovery program, should consider whether it is wise to have an online social media (i.e.,

"virtual") relationship with a formerly-discharged client, considering the Ethics prohibit such virtual relationships with current clients (ACA, 2014, section A.e.5). Were the risks communicated in relation to potential benefits (ACA, 2014, section H.6.b) in this case? But also, configuration of the telephone itself may have circumvented the event: Some smartphones (notably, recent builds of Android) make it possible to assign a screen lock while keeping the phone dialer and text messaging history outside of the screen lock restriction. Presenting the phone in this state might have allowed the officer to perform critical duties, averting a conflict.

Protecting the Counselor's Technology Footprint

Skillful use of technology has the potential to mitigate the risks of accidental disclosure of client info, in regards to smartphones, computers, and data stored in cloud services. Among these, computer security experts explain why smartphones present the most complex risk profile (Federal Communications Commission, 2012; Jeon, Kim, Lee, & Won, 2011). Few smartphones have a functioning anti-virus system. Periodic reviews by Google and Apple have found their app stores to be populated with "spy-ware" type programs. Even more troubling, the U.S. Department of Justice has found that cellular telephones are increasingly involved with the stalking of intimate partners (Baum, Catalano, Rand, & Rose, 2009). The counselor who works with and advocates for such clients thus represents a high-value target. A number of commercially available products install viruses onto a smartphone, capable of recording numbers dialed and even activating the headset microphone to listen in on conversations. Some of these viruses can be installed through physical hardware (e.g., by plugging the phone into a special charging "dock") without needing a passcode to unlock the screen, although it is still a recommended practice to set up a screen lock.

Recommendations for Smartphones

To help protect their client's identities and confidences, counselors can:

- Control the physical presence of a smartphone in sessions. Sometimes carrying a phone cannot be avoided (e.g., the counselor whose small children attend school must be available by telephone for emergency calls). If necessary, keep the phone inside a garment so that a layer of clothing muffles the audio of the counselor-client conversation.
- Turn off the Bluetooth connection, if equipped, when not in use. Viruses have been identified that activate a phone or computer's Bluetooth adapter to catalog the presence of nearby Bluetooth networks (Albanesius, 2012). What this means in practical terms is that if your phone detects a client's Bluetooth network named "AmyZ0123," then your phone could maintain a record that you were in a counseling session in close proximity to Amy Z.
- Turn off wi-fi when not in use, and configure your phone to prefer the cellular data network over free public wi-fi.
- Minimize the installation of apps, especially third-party apps (i.e., not from the manufacturer's online "store"). Do install an anti-virus app from a reputable sources (e.g., AVG, Avast, Kaspersky, Norton, Symantec).
- Activate the screen lock or passcode feature.

- Activate the "locate my phone" feature, if equipped.
- If you are a relatively non-technical user, do not allow a technician to "root" or "jailbreak" your phone (i.e., disable an array of security protocols, typically for the purpose of enhancing performance and control over the phone's operation). However, it is generally safe to "unlock" a GSM phone (one which has a SIM card) so that it can be used on another carrier.
- Never leave your phone unattended, even momentarily, even if switched off.
- Actively limit the extent and depth of confidential information stored on your phone; despite all precautions, smartphones have high potential for loss or theft, and it simply cannot be guaranteed that these data can be safeguarded.
- Note: All recommendations for smartphones may potentially apply to tablets, which typically run on the same operating systems as phones.

Desktop and Laptop Computers

Desktop and laptop computers present different risks, but also strengths. For example, anti-virus and firewall software is in widespread use; make sure your computer has one (e.g., from the publishers above). Some additional steps will increase security greatly.

Short-term storage and transmittal. First, encrypt short-term storage of data, especially those associated with transmittal (ACA, 2014, section B.3.e). E-mail in general lacks privacy (H.2.c), but internal e-mail to a recipient in the same organization may be relatively more secure if all server connections are encrypted and e-mail is never forwarded outside the organization. To maintain this level of security, avoid sending Word documents by e-mail, because a copy of the document is always cached in the computer's Temp folder (or equivalent). It is better to type or paste the information directly into the e-mail message than to attach a file. If a file attachment cannot be avoided (e.g., because some functionality such as spreadsheet tables or precise page layout is needed), use the encryption feature in recent MS Office versions to set a file password, even if it's a simple one; e-mail the password along with the file. Similar measures can be taken with Adobe PDF documents by "securing" the document with a password (requires full version of Acrobat Professional). Note that the MS Office encryption is extremely weak and PDF restrictions likewise can be bypassed by expert users; these are "screen-door" security measures at best, but they provide an additional layer to protect caches of "temp" files left in various locations on your computer. Learn these locations and periodically delete them.

Long-term storage. Files kept on your computer can be secured using TrueCrypt, a free open-source program that has been the subject of much academic and applied study (e.g., Forte, 2009). TrueCrypt creates an encrypted file "container" that can be very large (tens of gigabytes). When the correct password is entered, the container appears as if it were a removable flash drive into which files can be dragged and dropped; when the software disappears, the drive is closed and secured. Other, similar encryption products exist, both Windows- and Mac-specific, however TrueCrypt has two unique aspects: (a) it is cross-platform, meaning the encrypted file container can be archived, if necessary, and utilized on another platform, and (b) TrueCrypt can create an undetectable, hidden storage area within a visible storage area. Even if a counselor is compelled to unlock the visible storage area, the hidden area remains undetectable and unknown. Such a hidden

storage area potentially is ideal for storing sole-possession notes, documents that the counselor keeps as a memory aid and which are exempt from legal "discovery." This helps the counselor achieve the goal of disclosing to a court only those documents that are germane to a subpoena, as a way of protecting the client (ACA, 2014, section B.2.d).

Web Searches

Encryption can help protect clients' privacy when counselors rely on the Internet to become more educated about clients' needs and concerns, because Web search keywords normally are archived in server logs maintained by an Internet service provider, or institutional IT department. Consider this example: Kathy is a counselor at a school who works with at-risk teen girls. At an enrollment meeting of a new student, the parents confide that their daughter has HIV and needs support as she receives medical treatments. In order to understand the teen's needs, Kathy uses a search engine to find credible health resources. She takes appropriate precautions, such as using Private Browsing (in Firefox or Internet Explorer, which keeps no history and stores no cookies). She ensures her connection to the search engine is encrypted via https, and she only downloads information from reputable sources, such as the National Institutes for Health (NIH). However, many search engines pass along the search keywords via the page request URL, the address which is visible in the top of the browser. (In other words, search engines "remember" the words you have typed by adding them to the web page address, which cannot be encrypted; fortunately, usernames and passwords are not treated with the same openness!) URLs usually are logged and retained for some time by the internet service provider, in this case the district office. An IT technician happens to notice this search pattern. He resolves (traces) the requesting IP address to Kathy's office computer, and concludes that one of her students must be HIV-positive. While nominally bound by FERPA, the IT technician is not responsible to the ACA code of ethics, and therefore the future potential is unknown whether this information might be disclosed inappropriately.

Anonymity and Tor. The best mechanism for searching the Web anonymously is the Tor browser. Tor is an open-source software project, developed initially for the U.S. Navy and sustained largely with funding from the U.S. State Department for the purpose of encouraging Internet freedom in countries where criticism of the government is unlawful; most recently, movements associated with the "Arab Spring" used Tor to help organize while circumventing censorship (Fifield et al., 2012; Peterson, 2013; Smith, 2013). In appearance, Tor works like an ordinary Web browser, but it hides from local Internet providers the nature of Web sites that your search connects to – though your movement across those Web sites can still be tracked by the Web sites themselves. Ethically, counselors who use an employer-owned computer should seek permission before installing this or any other software, but on a technical level, installing the Tor browser does not require an "administrator" password (however, see Baker [2012a, 2012b] for a discussion of why employer-owned computers pose additional privacy concerns). The Tor browser is slightly less convenient to use because it may navigate some search requests more slowly. Finally, it is not effective with all types of media; downloading Word .doc and PDF files is not recommended, and some multimedia (e.g., YouTube videos) will not play. However, Tor offers an optimum level of online privacy

and is an essential tool for counselors to avoid revealing indirectly information about clients through their online research patterns.

Cloud Computing and Web-Based Storage

Although issues with cloud computing are complex, they could be condensed to one simple question: "Who are your neighbors?" Cloud services are used by many parties, some reputable, some less so. Most counselors would understand intuitively why their practice office location should not be located between, for example, an adult bookstore and a tobacco shop. But what is the harm in sharing server space with seedy enterprises if they are not even apparent to the counselor's clients? First, realize that some Web sites will be blocked by firewall rules at sensitive institutions, such as public schools, because low-cost Web hosting plans run dozens of Web sites on a single IP address (i.e., "name-based virtual domain" hosting). Some of the counselor's "neighbors" on the server may sponsor prohibited content, such as gambling, with the result that all co-hosted Web pages from that IP address are blocked by the institutional firewall. But a more serious consideration is that law enforcement and national security agencies also must periodically demand that server operators disclose their clients' data. As a counselor, your cloud-maintained data may be kept "secure" and encrypted, but it is likely that these data are secured using the same encryption key and stored in the same database as those of all other server users – possibly including illicit enterprises. In the event a search warrant is presented to the server owner, not only will law enforcement agencies have access to your data, it is possible that your data are so commingled with the data of interest that by necessity, your data must be downloaded for analysis for the sake of executing the search warrant correctly. In other words, once another user's data are accessed under the provisions of the warrant, you the counselor may become powerless to prevent breach of your clients' data as well (Poulsen, 2013). This would be a good justification for using cloud storage services that cater specifically to healthcare services (as opposed to general-purpose storage) or which take other precautions to compartmentalize the encryption of user data.

The legal and technical dimensions of evaluating a cloud storage service are daunting. However, a simple rule of thumb is for counselors to avoid using Web-based services that would appeal to illicit organizations and individuals, perhaps because they are free and require no identity verification. The time has come to eschew "Swiss army knife" technologies that promise to do everything for everyone: The photo-sharing Web site which allows 2 GB of "free, secure" storage may seem a very appealing tool for grad students to share their counseling videos with a faculty supervisor; but it may also seem convenient by members of a terrorist cell who plot to share surveillance video of a potential target with a nameless commander, thousands of miles away. By preferring Web sites that charge a nominal fee via credit card, or require some other form of identity verification, counselors take a step in the right direction. Such Web sites may be more likely to promise specific responsibilities to maintain the data of their users. An even better measure is the installation of a file-share server that is local to an institution, as electronic and also physical access might be more tightly controlled, and so are the identities of technicians who will maintain the equipment.

Continued Awareness and Lifelong Education

Finally, lifelong connections to learning must be maintained in order to keep with technology best-practices. The best way to do this is by reading mainstream news outlets, with attention to computing industry publications. Reading peer-reviewed journals in computer science is not required or particularly helpful, as these outlets tend to focus more on development of theory. Edited publications in computer technology can report credibly on complex technological trends, as technologies can change much more quickly than the peer review process can function. In diminishing order of accessibility to non-technical consumers, some technology news sources are:

- PC World magazine
- Wired magazine
- Ars Technica blog
- the Electronic Frontier Foundation, a civil liberties group

News media sources are indispensable for best practice in technology; counselors cannot afford to wait for authoritative texts to be published in professional journals. For example, consider that recently Apple released a "patch" (software code repair) for a major bug in the Safari browser that had prevented it checking whether the name of a Web site was the same name on the security certificate (Cunningham, 2014). In application, this could result in users logging into a "fake" Web site, especially when connecting to the Internet via public wi-fi. Apple published the patch for iOS (iPhones and iPads) eight days before the Mac software patch was released. When the iOS patch was released, engineers (reputable ones, as well as presumably hackers) analyzed the code within hours and extrapolated to a description of the nature of the software defect (Greenburg, 2014). This means that for eight days, hackers had the knowledge and opportunity to exploit the Safari security flaw for users of the Mac platform. Mac users informed of the situation could simply use a different browser temporarily, but only by following news media would they have become informed of the situation in time to take preventative measures.

Conclusion

The ACA Code of Ethics (2014) addresses current trends in technology that carry a long-term impact and describes counselors' responsibilities to clients whenever technology is used. The Code describes appropriate steps counselors should take with regards to clients' private data, among other aspects, while specific modern technologies can provide counselors with the tools in the short-term to meet these challenges, particularly for those counselors who work in non-HIPAA workplaces and therefore may be responsible for selecting their own technology practices.

References

Albanesius, C. (2012). Massive 'Flame' malware stealing data across Middle East. PCMag.com. Retrieved from http://www.pcmag.com/article2/ 0,2817,2404951,00.asp

American Counseling Association (ACA). (2014). *ACA code of ethics*. Alexandria, VA: Author.

Baker, T. D. (2012a). Confidentiality and electronic surveys: How IRBs address ethical and technical issues. *IRB: Ethics and Human Research, 5,* 8-15.

Baker, T. D. (2012b). Digital confidentiality: A holistic security model for counselors. *VISTAS*. Retrieved from http://www.counselingoutfitters.com/ vistas/vistas12/ Article_39.pdf

Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking victimization in the United States: Special report.* U.S. Department of Justice. Washington, DC: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/ index.cfm?ty=pbdetail&iid=1211

Cunningham, A. (2014, February 25). Apple releases OS X 10.9.2, patches SSL flaw and adds FaceTime Audio support. *Ars Technica*. Retrieved from http://arstechnica.com/apple/2014/02/apple-releases-os-x-10-9-2-patches-ssl-flaw-and-adds-facetime-audio-support/

Fakhoury, H. (2013). *DEA and NSA team up to share intelligence, leading to secret use of surveillance in ordinary investigations*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering

Federal Communications Commission. (2012). *Ten steps to smartphone security for Apple iOS.* Retrieved from http://www.fcc.gov/smartphone-security/ Apple%2BiOS

Fifield, D., Hardison, N., Ellithorpe, J., Stark, E., Boneh, D., Dingledine, R., & Porras, P. (2012). Evading Censorship with Browser-Based Proxies. *Privacy Enhancing Technologies: Lecture Notes in Computer Science, 7384*, 239-258.

Forte, D. (2009). Do encrypted disks spell the end of forensics? *Computer Fraud & Security*, *2*, 18-20.

Greenburg, A. (2014, February 22). Stop using Safari and update iOS to avoid Apple's critical 'Gotofail' security bug. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2014/02/22/stop-using-safari-and-update-ios-to-avoid-apples-critical-gotofail-security-bug/

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. *Human Interface and the Management of Information. Interacting with Information Lecture Notes in Computer Science*, *6771*, 311-320.

Peterson, A. (2013, October 5). The NSA is trying to crack Tor. The State Department is helping pay for it. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/

Poulsen, K. (2013). Edward Snowden's e-mail provider defied FBI demands to turn over crypto keys, documents show. *WIRED*. Retrieved from http://www.wired.com/threatlevel/2013/10/lavabit_unsealed/

Schmidt, M. S., & Lichtblau, E. (2012). Racial profiling rife at airport, U.S. officers say. *The New York Times*. Retrieved from http://www.nytimes.com/2012/08/12/us/racial-profiling-at-boston-airport-officials-say.html

Shiffman, J., & Cooke, K. (2013). U.S. directs agents to cover up program used to investigate Americans. *Reuters*. Retrieved from http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805

Smith, G. (2013, July 18). Meet Tor, the military-made privacy network that counts Edward Snowden as a fan. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/07/18/tor-snowden_n_3610370.html

Note: This paper is part of the annual VISTAS project sponsored by the American Counseling Association. Find more information on the project at: http://counselingoutfitters.com/vistas/VISTAS_Home.htm