HIPAA, HITECH and the Practicing Counselor: Electronic Records and Practice Guidelines

Jeffrey S. Lawley

The Professional Counselor
Volume 2, Issue 3 | Pages 192–200
http://tpcjournal.nbcc.org

www.nbcc.org
doi:10.15241/jsl.2.3.192

The use of technology in counseling practice is constantly expanding, offering new tools for communication and record-keeping. These tools come with significant legal and ethical risks for counselors as well as counselor educators and supervisors. Rules from HIPAA and HITECH are discussed in relation to counselor practice. Guidelines for electronic records and communication are suggested.

Keywords: counselor education, ethical risks, supervision, technology, electronic records

In April 2005, the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA; 2007) went into effect for all health care providers. New security standards (which specifically address protection of access to medical records, as opposed to privacy standards which address issues related to sharing of medical records with other entities) are now enforced for any professional that handles electronic Protected Health Information (ePHI), including professional counselors. Some aspects of the impact of HIPAA on individuals who are practicing as independent clinicians have been addressed previously (See Benefield, Ashkanazi,& Rozensky, 2006, and Brendel & Bryan, 2004 for examples). However, many discussions of HIPAA have been aimed at other types of practitioners.

HIPAA's rules have since been amended in a number of ways by the Health Information Technology for Economic and Clinical Health (HITECH) act, which was passed in 2009 and went into effect in February 2010. HITECH (2009) makes changes to some HIPAA rules regarding electronic security and access to ePHI. In comparison to discussions of other technological issues regarding counseling, such as online counseling (Richards, D., 2009; Rummel & Joyce, 2010), electronic security is a relatively new and sparse area in the counseling literature. The shifts in law regarding ePHI have direct effects on the way that some current counseling practices, such as e-mail interactions with clients (McDaniel, 2003), must be pursued. The question of practical implications of changing laws is made more complex by the fact that many of these rules are written with large organizations or medical practices in mind. This can leave the individual or small group practitioner without the resources of larger practices feeling overwhelmed. Regardless, counselors are required to be aware of not only important aspects of the HIPAA security rule, but also the ways in which it is amended by HITECH. Awareness of laws regarding practice and the use of technology is part of the American Counseling Association's (ACA; 2005) ethical guidelines regarding limitations to confidentiality and privacy in the counseling process. Counselors may wish to discuss limitations specific to electronic medical records as part of this process (Richards, M., 2009).

ePHI is defined as any Protected Health Information (PHI) that is stored on any form of electronic media, or which is transmitted in any electronic form (e.g., fax or Internet). This would include scanned records or correspondence that is written on a computer and then printed (Freeny, 2007). This does not include ePHI in educational records, which falls separately under the Family Educational Rights and Privacy Act (HIPAA, 2007). The security rule requires that medical professionals take measures to keep ePHI confidential and to protect it from disclosure. Additionally, counselors are to safeguard ePHI from any "reasonably anticipated threats or hazards to the security or integrity of such information" (HIPAA, 2007, §164.306 (a) (2)).

Jeffrey S. Lawley is an Assistant Professor at Louisiana State University-Shreveport. Correspondence can be addressed to Jeffrey S. Lawley, Louisiana State University-Shreveport, 1 University Place, BE Building 348, Shreveport, LA 71115, jslawley@gmail.com.

Poorly maintained ePHI systems are a significant legal and ethical risk for counselors for a variety of reasons. This risk involves a breadth of information typically kept by counselors, including reports, case notes, billing materials, correspondence, personal notes, and research kept on electronic devices including computers, smartphones, and other electronic devices (particular issues related to smartphones and similar devices are discussed below). This is due to the expanded definition of protected health information (PHI) that HIPAA creates—virtually anything that could be traced back to a client that confirms their treatment. HIPAA defines PHI as material in any format that "relates the past, present, or future physical or mental health or condition of an individual" (HIPAA, 2007, §160.103(2)[definition of individually identifiable health information]). It also covers information that is involved in payment for these services. In order to be categorized as ePHI, the information must be used to identify an individual—that is, de-identified information is not covered under this definition.

HIPAA includes requirements for both physical and electronic safeguarding of ePHI (or computers that store ePHI). Physical security includes access to devices on which information is kept. Tools and procedures related to physical security involving access to records will probably be familiar to most counselors. Typically, this refers to basic practices such as antivirus software and other technical practices, but additionally refers to specific access and data management practices as discussed below. Concerns related to electronic security are somewhat more complex and come with broader implications. For example, there is little information to help counselors determine what counts as a "reasonably anticipated" (HIPAA, 2007, §164.306 (a)(2)) electronic threat.

Note that there are other areas where HIPAA may affect mental health practice in ways that may conflict with generally accepted standards of practice or ethical guidelines, such as the fact that communication for continuity-of-care or insurance billing purposes no longer legally requires a release. This discussion falls out of the area of focus of this article, which is on the specific effects of the security rule on counseling practice. (A general discussion of HIPAA issues affecting counselors can be found in Freeburg & McCaughan, 2008).

Ethics, Law and Client Files

Counselors will be happy to learn that there are few significant conflicts between counseling ethics (ACA, 2005) and law in regards to ePHI. Differences are typically found when ethics codes within the mental health profession do not address issues that are addressed by HIPAA and HITECH. For example, general guidelines for the protection of client records are discussed in the most recent ethics code of the American Counseling Association (ACA, 2005). However, these guidelines focus more on a general need to keep confidentiality and possible reasons for breaking confidentiality. The code does not suggest specific guidelines for keeping electronic records, but only notes that "records are kept in a secure location and that only authorized persons have access to records" (ACA, 2005, Standard B.6.a). No specific measures regarding ways to manage confidentiality, security or privacy of ePHI are offered. HIPAA and HITECH lay out a number of details in addition to this general rule.

Data Backups

One primary concern not applicable to paper records is the legal requirement to keep an easily accessible, but equally secure and encrypted, backup of all ePHI (HIPAA, 2007, §164.308, (7)(ii)(a): an entity must "establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information"). Since this guideline is meant as part of a disaster recovery plan, assuming loss of all data in a counselor's office, this backup may often be kept offsite. That is, an additional secure location outside of the office is now necessary. With this rule and the advent of nominally secure and easily accessible cloud backup services, the variables defining a "secure location" have changed significantly since HIPAA was established.

Counselors may be tempted to use an online backup service as an offsite backup, and can be aided by provisions of HIPAA and HITECH in making a choice between an offsite physical backup in an additional secure location and the use of an online backup service. Under HIPAA and HITECH, the appropriateness of online backup can be somewhat murky. Separate encryption of data on the local computer (as required by HITECH, see below) before sending the data over an encrypted connection to an online service may alleviate this concern. Before using any cloud backup solution, counselors

should determine whether the company meets a brief checklist of requirements (see Table 1). There are a number of online backup services, marketed towards healthcare professionals, which describe themselves as "HIPAA-compliant." However, this does not have a technical meaning—there is no certification for HIPAA compliance regarding client data backup services. It is the responsibility of the counselor or designated individual in a group practice to ensure that online backup meets HIPAA and HITECH requirements.

Table 1

Quick Checklist for Online Backup

HIPAA and HITECH require the counselor to be able to access accurate and current copies of all ePHI at any time, even in the event of a disaster that destroys copies located in a counselor's office. Some forms of cloud storage may be an option if they meet the following minimum requirements, which can typically be ascertained by reading a site's terms of service:

- Data is monitored for changes and backed up immediately
- Client-side software can be set up in such a way that unauthorized individuals cannot access data
- Data is transmitted over an encrypted connection (e.g., https connections)
- Documentation of physically secure storage; some services have multiple backup locations
- Data cannot be accessed by staff at storage site under any circumstances, including a court order
- Data is encrypted before transmission with at least 256-bit encryption (e.g., encryption is automatically performed client-side by the client software). Alternatively, data can be encrypted manually by the counselor before backup
- (optional) Two-factor authentication (requiring a USB key or other secondary "token" to access archived data)

Most popular cloud storage services advertise secure online backup with varying levels of encryption. However, these services are not all created equally and in many cases their process does not meet minimum standards. While transmission is typically encrypted as required by HIPAA, information stored by these services is not necessarily secure. Information may be encrypted at a physically secure site, but some services do have the technical ability to access any ePHI that is stored with them. For example, the terms of service at Dropbox, a popular backup and syncing service, state that:

> We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) to protect Dropbox's property rights. If we provide your Dropbox files to a law enforcement agency as set forth above, we will remove Dropbox's encryption from the files before providing them to law enforcement. However, Dropbox will not be able to decrypt any files that you encrypted prior to storing them on Dropbox (Dropbox, 2011, section 3, para 4).

This means that someone other than the counselor or a designated individual could access ePHI. For example, if a counselor is involved in a lawsuit, a court order could cause the online storage company to disclose unencrypted ePHI without input from the counselor. However, as noted, they are not able to decrypt any information that the counselor encrypts before backing up, as suggested by HITECH. In most cases, counselors must ensure that data is encrypted before being sent to any such service. Counselors also are cautioned to pay close attention to the privacy policies at any backup service that they might use; many are less specific than the example above but still allow for the possibility of decrypting and releasing data with a court order.

Counselors also should note that there are other backup services that offer what is called user or client-side encryption. ePHI is encrypted before it leaves the counselor's computer, and no individual at the physical storage site can access the information. This protects the counselor, as they cannot provide any information about data that they are storing for the counselor. It is important to note that this does not mean that information on the counselor's own computer is encrypted.

Communication of Client Information

HIPAA also addresses the transmission of ePHI via electronic methods such as e-mail. The law states that medical professionals must have some sort of measure to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network" (HIPAA, 2007, § 164.312(e) (1)) such as the Internet. Similar language regarding secure electronic communication is found in the ACA ethics code. It is important for counselors to be aware of this requirement, as communication with clients via e-mail or other online communication is likely to become more common for general communication as well as therapeutic tasks. As an example, McDaniel (2003) discusses the benefits of having clients e-mail weekly journals to their clinicians. This work was published before the HIPAA security rule went into effect and the general idea is certainly no less useful today. However, the online transmission of identifiable material directly related to clinical work certainly falls under the legal guidelines discussed here. While in most cases clients are clearly giving permission for counselors to correspond via e-mail or by other means such as videoconferencing or online chat (Haberstroh et al., 2008), the laws regarding secure electronic transmission still apply. It is important to note that the counselor is not liable for encryption or safety of material on the receiving end of the transmission (HITECH). This problem could be solved by using an e-mail service that forces encryption before transmission, an option available through most e-mail services. As indicated in the ACA ethics code, if online communication is utilized by a counselor, they should indicate the limitations of this method of communication in regards to the possible insecurity of online communication and encourage the client to take similar precautions when sending messages to the counselor.

Loss of Data or Involuntary Breaches of Confidentiality

One aspect of the care of ePHI that is not completely addressed by HIPAA or the most recent ethical codes is what should happen when ePHI is accessed inappropriately. For example, there is no specific guideline in the ACA ethics code indicating that clients should be notified when their files are accessed. It is up to the individual counselor to determine what to do if a client's paper file is stolen. HITECH has changed this in regards to ePHI, however. The law requires medical professionals to have a specific plan in place to notify affected clients in the case of a breach of *unprotected* (e.g., unencrypted) electronic information—and to immediately notify the Secretary of Health and Human Services (HHS) if the breach involves more than 500 individual clients. At first glance this may seem like a large number, especially for an individual in private practice. However, any practicing individual who has used electronic records for some time will have at least this many case files over the lengthy period (often at least seven years) in which documentation may be kept. This means that if an unprotected backup of ePHI is stolen, the counselor is responsible for notifying every individual whose identity may be compromised within 60 days. There are no ethical or legal requirements for disclosure after the loss of encrypted data, leaving it to the counselor to choose whom to notify.

Case Notes and Assessment Data

Another important ethical question that presents itself regarding ePHI involves unique types of medical information that are typically handled by counselors. Counselors may handle some types of information that have differing practical and legal status than "traditional" medical records, including case notes and testing material. Case notes have historically enjoyed nearly absolute privacy protection in the United States (Mosher & Swire, 2002) and are specifically addressed in HIPAA. They continue to retain expanded protection under current law, requiring a separate release when they are accessible at all (see Hixson & Hunt-Unruh, 2008). These include the type of separate notes that some counselors keep separately from the patient file and specific to the counseling process. They include observations, inferences and conceptualizations of the client; however, typical case notes including such information as diagnosis, prognosis, and changes in symptoms, etc. are not covered under this expanded protection (HIPAA, 2007).

The case of assessment records, particularly raw data, is somewhat murkier. The general idea is that data may be misused or misinterpreted by individuals who are not trained in interpretation of test data, in addition to concerns about

the security of test instruments themselves (Committee on Legal Issues, 2006). Given the historical view of the fields of psychology (Committee on Legal Issues, 1996) and the current view of counseling (ACA, 2005) on the security of test data, particularly raw data, one might expect assessment data to be separated in a manner similar to case notes in regards to release of the information. However, rules in HIPAA regarding test data state that a client can choose to sign their entire medical record (sans case notes) to any third party (HIPAA, 2007). While HIPAA allows the medical professional to exclude certain information based on client safety, or if the counselor obtained the information under separate release from another practice, possible misuse of test data is not an acceptable reason to exclude portions of a counselor's record (Erard, 2004). There are no stipulations in HITECH that change this. However, ACA's 2005 ethics code is clear in its statement that "[test] data are released only to persons recognized by counselors as qualified to interpret the data" (Standard E.4). This is the most significant difference between the ACA ethics code and current law.

Online assessment and treatment is another activity that counselors may not have considered when reviewing the impact of law on their practice. A growing number of therapists, for example, are using online tools for various tasks such as career assessment (Gysbers, Heppner, & Johnston, 2009), and are starting to pursue online counseling activities (Haberstroh et al., 2008). This information is typically stored on computers that belong to the test owner, not the counselor, and the counselor is not directly responsible for information on these machines. However, counselors have an ethical responsibility to ensure the integrity of the website that a client may use for such an assessment. The ACA ethics code specifically addresses this issue by stating that counselors should be aware of the limitations of online activities and share this information with the client. It also discusses guidelines for supervision of online activities (ACA, 2005). This is a relatively new area of practice that is not covered by HIPAA or the more recent HITECH. However, the same care should be taken with any information downloaded from these sites as with any other ePHI.

A Note About Smartphones

It also is important to note that as "alternative" (and easily lost) computing devices such as smartphones and tablet computers become more common, counselors are likely to use these to monitor and keep client records as well. Most cloud storage systems offer mobile applications for smartphones, or have websites that may be accessed by smartphones. Additionally, there are a number of smartphone tools designed to assess symptoms or help a client keep a journal. As a part of informed consent in treatment, clients should be reminded of the risk of keeping such information on their phone. At the current time, it is not advisable to use smartphones or tablet devices to access ePHI unless it is being accessed over a secure network and then deleted (e.g., information is accessed through a local network or virtual private network). Often, information such as this may be cached on the device and accessible if the device is stolen or lost. Counselors also should be encouraged to utilize a passcode on these devices, as required under the rules regarding computer access under HITECH.

Finally, counselors should take care to monitor the security of any messaging that they use on their phone. While secure e-mail can be configured on most smartphones, there is no way to secure a text message and clients must be informed of this risk if text messaging is used as a form of communication between counselor and client. (For good examples of situations where text messaging may be a productive tool in counseling, see Agyapong, Farren, & McLoughlin, 2011, and Suffoletto, Callaway, Kristan, Kraemer, & Clark, 2012).

Practice Guidelines

Access Policies and Documentation

Counselors are responsible for a number of procedural issues regarding "live" practice. The organization is required to have a designated individual who is responsible for ensuring the practice meets legal guidelines regarding records as well as other issues. In solo practices, this would mean the individual counselor. In group practices, this person needs to be readily identifiable and does not have to be a licensed individual, or someone who is an active counselor in the practice. The practice also must have a manual of procedures regarding such things as password policies, access policies, standards regarding computer security, instructions for encryption and storage of files, and documentation that everyone in the office has been kept up to date on these policies. This is not an exhaustive list, but indicative of the types of information that need to be covered and readily available in the case of an audit. "Case notes" also are required for this list of procedures,

documenting changes to these policies as they are made (HIPAA, 2007).

Not only must counselors have general physical safeguards in place, there must be policies specific to physical access to any computers that can access or modify records. Controlled access to individual machines is required, including user-specific logins with passwords and automated logoff in case an individual leaves their desk and forgets to log off. Counselors should be encouraged in particular to pay close attention to their password policies (see Proctor, Lien, Vu, Schultz, & Salvendy, 2002).

Ideally, in small group practices each individual will have their own computer which is only accessible using their personal login. If more than one counselor uses a computer, the counselor must be able to show that individuals who should not be able to access certain information are not able to do so. For example, in many situations graduate counseling students might access services through a college counseling center. If some of their peers work at this site, steps would need to be taken to ensure that they do not have access to these files. In another case, in many areas with less access to counseling services, an individual with a close relationship to one counselor may be seeing another individual in the practice. Depending on the nature of a practice's electronic records, keeping a separate individual paper file may be easier than modifying ePHI procedures to account for this type of issue. Another alternative might be to keep a file on a counselor's individual computer, if records are kept on a central storage device or server.

Encryption

Although not specifically addressed by ethical standards, encryption of electronic files is encouraged by relevant law. This concerns not only local files, but also offsite backups. According to HIPAA, an electronic file had to be kept in such a way that it was not able to be modified by unauthorized individuals. This could be interpreted as encryption, but controlled access to computers technically counted as this type of protection. HITECH, however, encourages medical professionals to encrypt all local data. In addition to the required notification discussed above, fines of up to $50,000 (per incident) have been instated for loss of client data. As noted, notification of clients or the department of HHS is not legally required for the loss of adequately encrypted data, and it is up to the counselor to create a policy regarding notification to clients of loss of encrypted data. The current ACA ethics code does not specifically address encryption or backup of ePHI.

Additional HITECH Practice Guidelines

There are other changes in HITECH that will affect counseling practice that are not specifically related to the use of electronic records. HIPAA and HITECH also have guidelines regarding what are labeled as "business associates." Counselors may occasionally share information regarding clients with other individuals or agencies in order to assist with such activities as billing or collections. This information is part of a client's PHI. As such, it is the responsibility of the counselor to create a contract with this "business associate" that includes language stating that the associate also will maintain HITECH-compliant security (similar to HIPAA, but including rules regarding encryption, etc.) related to any information that the counselor shares with this agency. The counselor is presumably, but not specifically, also responsible for ensuring that the other agency has some awareness of security requirements for ePHI. The counselor is not, however, responsible for monitoring this other agency and is not responsible for data lost by this other agency (HIPAA, 2007; HITECH, 2009).

HITECH has made some changes in regards to the provision of records to the client and to insurance companies. Clients must be provided with a complete copy of their records upon request at "reasonable" cost—if the counselor charges any amount for release of records, ePHI must be shared with only a reasonable cost of labor. Clients also have the right to records about the sharing of records with other entities for up to three years. This means that in addition to typical record-keeping, counselors also must keep some sort of receipt or other notes indicating exactly what information has been shared with others, such as providers or insurance companies.

Finally, while this was an existing ethical requirement (ACA, 2005), counselors are now legally allowed to share only the minimum necessary amount of information in order to meet the needs of the other agency or individual who is requesting the information. For example, records shared with another entity such as an insurance company should involve only the information necessary for the insurance company to be able to appropriately bill for services. HITECH clarifies

that the counselor is the individual who is allowed to make the determination of the minimum amount of necessary information. The counselor might find it helpful to have a few treatment summary templates for sharing with other entities such as schools, where all of the information in a child's file is not necessarily relevant to the other entity. Additionally, counselors may, at the client's request, withhold treatment information from insurance companies if the client pays out of pocket for services. For example, if the client wishes that their insurance company or employer not know about their treatment for a specific issue (e.g., substance abuse), the counselor may see the client at any rate they choose and keep this information secure (HITECH, 2009).

Summary and Implications for Professional Counselors

While most counselors are at this point aware of changes necessary to remain in compliance with the HIPAA security and privacy rules, HITECH has changed some aspects of practice again, in some cases significantly. Of particular impact for counselors are rules involving encryption, fines for loss of unencrypted data and changes in rules regarding communication with other individuals involved in a client's care. It is notable that rules regarding ePHI are in many ways more restrictive than those involving management of traditional paper files, requiring encryption, offsite backups and other safeguards that were not even possible with paper. However, it can be argued that ePHI carries significantly more risk of loss than traditional paper records, as it is much easier to obtain large amounts of information off of an unguarded computer than from a file cabinet. It also is important to note that as of yet, aside from a few prominent cases involving the loss of data, there is little or no case law regarding the specifics of HIPAA implementation—that is, even the best guides are not yet able to state the best way to do this "right." For example, there are no specific encryption standards, although there are industry standards that can be used as a rough guide. Significant implications for counselors are summarized in Table 2.

Table 2

Significant Implications for Counselors, Counselor Educators, and Supervisors

HITECH, the cloud, and electronic records modify the meaning of technological competence in counseling in many ways. Below are some significant practical implications for practice and training in counseling:

- Continuing education programs and graduate coursework need to address ePHI and the differences between requirements for electronic and paper records; even counselors who do not utilize electronic records likely utilize electronic communication with clients
- Awareness of technological issues, such as the limitations of cloud backup, strong password generation, and the basics of how encryption works, is crucial for counselors
- Counselors need to be able to explain to clients the limitations of electronic communication and include any relevant limitations on their statements of practice and other informed consent materials
- Mobile technology such as SMS (text messaging) is coming into greater use in counseling, but ethical and legal guidelines for these methods do not yet exist. SMS in particular may not technically meet legal requirements but is utilized with good effect in recent research (Aguilera & Muñoz, 2011)
- If counselors use smartphone apps in their practice, they need to be able to explain ways to keep clients' smartphones secure (e.g., instructing a client in how to create a PIN lock on an iPhone or iPod).
- Existing ethical guidelines need to specifically address electronic tools that are used in counseling
- "Current best practice" in technology changes much faster than in counseling. Limiting one's exposure to changes in technology to an occasional CE program is not advisable.
- Supervisors have added responsibility, as they can be seen as the best way to propagate this information
- Counselors may find it helpful to seek out a dependable "technology supervisor" with whom they can consult on issues related to technology

There appear to be few conflicts between the new law and the current ACA ethics code. In fact, the law addresses some things that the current ethics code does not. The next revision of the ethics code would do well to cover some issues related to electronic communication and record-keeping in addition to its guidelines on the use of online counseling services and tools. Counselors would benefit from guidelines regarding whom to notify in the case of data loss, and may be well advised to pursue encryption of any ePHI that they handle within their practice. Counselors also would benefit from guidelines regarding awareness of current issues regarding electronic security, such as good password policies and the use of "smart" handheld devices for data access. Guidelines regarding the backup of ePHI may be of assistance to counselors who are attempting to utilize online services.

Finally, CACREP (2009) guidelines for counselor training include the need of counselor educators to show that they are teaching their students about the ways that technology is changing counseling. Discussion of issues regarding ePHI should be clearly evident in training programs, specifically in ethics courses, practica, and internship. For counselor educators, these points may be easiest to integrate into existing ethics courses. While these discussions are often centered on the use of online tools as described in the current ethics code, the growing use of ePHI in the medical and mental health communities may be the most important change that technology has yet brought to the field.

References

Aguilera, A., & Muñoz, R. F. (2011). Text messaging as an adjunct to CBT in low-income populations: A usability and feasibility pilot study. *Professional Psychology: Research and Practice*, *42*, 472–478. doi:10.1037/a0025499

Agyapong, V. I. O., Farren, C. K., & McLoughlin, D. M. (2011). Mobile phone text message interventions in psychiatry—What are the possibilities? *Current Psychiatry Reviews,* 7, 50–56.

American Counseling Association (2005). ACA code of ethics. Alexandria, VA: Author.

Benefield, H., Ashkanazi, G., & Rozensky, R. H. (2006). Communication and records: HIPAA issues when working in health care settings. *Professional Psychology: Research and Practice*, 37, 273–277.

Brendel, R. W., & Bryan, E. (2004). HIPAA for psychiatrists. *Harvard Review of Psychiatry, 12*, 177–183.

Committee on Legal Issues. (1996). Strategies for private practitioners coping with subpoenas or compelled testimony for client records or test data. *Professional Psychology: Research and Practice*, *27*, 245–251.

Committee on Legal Issues. (2006). Strategies for private practitioners coping with subpoenas or compelled testimony for client records or test data. *Professional Psychology: Research and Practice*, *37*, 215–222.

Council for Accreditation of Counseling and Related Educational Programs. (2009). *CACREP 2009 standards*. Retrieved from http://www.cacrep.org/

Dropbox. (2011, July). Dropbox privacy policy. Retrieved from http://www.dropbox.com/privacy

Erard, R. E. (2004). Release of test data under the 2002 ethics code and the HIPAA privacy rule: A raw deal or just a half-baked idea? *Journal of Personality Assessment*, *82*, 23–30.

Freeburg, M., & McCaughan, A. (2008). HIPAA for dummies: A practitioner's guide. In G. R. Walz, J. C. Bleuer, & R. K. Yep (Eds.), *Compelling counseling interventions: Celebrating VISTAS' fifth anniversary* (pp. 305–312). Alexandria, VA: American Counseling Association.

Freeny, M. (2007). Whatever happened to clinical privacy? *Annals of the American Psychotherapy Association*, *10*, 13–17.

Gysbers, N. C., Heppner, M. J., & Johnston, J. A. (2009). *Career counseling: Contexts, processes, and techniques* (3rd ed.). Alexandria, VA: American Counseling Association.

Haberstroh, S., Parr, G., Bradley, L., Morgan-Fleming, B., & Gee, R. (2008). Facilitating online counseling: perspectives from counselors in training. *Journal of Counseling and Development*, *86*, 460–470.

Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. §§300jj et seq.; §§17901 et seq. (2009).

Health Insurance Portability and Accountability Act, 45 C.F.R. § 164 (2007). Retrieved from http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html

Hixson, R., & Hunt-Unruh, D. (2008). Demystifying HIPAA. *Annals of the American Psychotherapy Association*, *11*, 10–14.

McDaniel, S. H. (2003). E-mail communication as an adjunct to systemic psychotherapy. *Journal of Systemic Therapies*,

22, 4–13.

Mosher, P. W., & Swire, P. P. (2002). The legal and ethical implications of Jaffee v. Redmond and the HIPAA medical privacy rule for psychotherapy and general psychiatry. *Psychiatric Clinics of North America, 25*, 575–584.

Proctor, R. W., Lien, M. -C., Vu, K. -P., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of protective password restrictions. Behavior Research Methods, *Instruments, & Computers*, *34*, 163–169.

Richards, D. (2009). Features and benefits of online counseling: Trinity College online mental health community. British *Journal of Guidance and Counseling*, *37*, 231–242.

Richards, M. M. (2009). Electronic medical records: Confidentiality issues in the time of HIPAA. *Professional Psychology: Research and Practice, 40*, 550–556.

Rummell, C. M., & Joyce, N. R. (2010). "So wat do u want to wrk on 2day?": The ethical implications of online counseling. *Ethics & Behavior*, *20*, 482–496.

Suffoletto, B., Callaway, C., Kristan, J., Kraemer, K., & Clark, D. B. (2012). Text-message-based drinking assessments and brief interventions for young adults discharged from the emergency department. *Alcoholism: Clinical and Experimental Research*, *26*, 552–560.