Technology in Counselor Education: HIPAA and HITECH as Best Practice

The Professional Counselor
Volume 5, Issue 3, Pages 407–418
http://tpcjournal.nbcc.org

doi:10.15241/tw.5.3.407

Tyler Wilkinson, Rob Reinhardt

The use of technology in counseling is expanding. Ethical use of technology in counseling practice is now a stand-alone section in the 2014 American Counseling Association *Code of Ethics*. The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act provide a framework for best practices that counselor educators can utilize when incorporating the use of technology into counselor education programs. This article discusses recommended guidelines, standards, and regulations of HIPAA and HITECH that can provide a framework through which counselor educators can work to design policies and procedures to guide the ethical use of technology in programs that prepare and train future counselors.

Keywords: **counselor education, technology, best practice, HIPAA, HITECH**

The enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) brought forth a variety of standards addressing the privacy, security and transaction of individual protected health information (PHI; Wheeler & Bertram, 2012). According to the language of HIPAA (2013, §160.103), PHI is defined as "individually identifiable health information" (p. 983) that is transmitted by or maintained in electronic media or any other medium, with the exception of educational or employment records. "Individually identifiable health information" is specified as follows:

> Information, including demographic data, that relates to:
> - the individual's past, present or future physical or mental health or condition,
> - the provision of health care to the individual, or
> - the past, present, or future payment for the provision of health care to the individual, and that identifies the individual for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers. (U.S. Department of Health and Human Services [HHS], n.d.-b, p. 4)

The HIPAA standards identify 18 different elements that are considered to be part of one's PHI. These include basic demographic data such as names, street addresses, elements of dates (e.g., birth dates, admission dates, discharge dates) and phone numbers. It also includes information such as vehicle identifiers, Internet protocol address numbers, biometric identifiers and photographic images (HIPAA, 2013, § 164.514, b.2.i).

According to language in HIPAA, the applicability of its standards, requirements and implementation only apply to "covered entities," which are "(1) a health plan (2) a health care

Tyler Wilkinson, NCC, is an Assistant Professor at Mercer University. Rob Reinhardt, NCC, is in private practice in Fuquay-Varina, NC. Correspondence may be addressed to Tyler Wilkinson, 3001 Mercer University Drive, AACC 475, Atlanta, GA 30341, Wilkinson_rt@mercer.edu.

clearinghouse (3) a health care provider who transmits any health information in electronic form in connection with [HIPAA standards and policies]" (HIPAA, 2013, § 160.102). Covered entities have an array of required and suggested privacy and security measures that they must take into consideration in order to protect individuals' PHI; failure to protect individuals' information could result in serious fines. For example, one recent ruling found a university medical training clinic to be in violation of HIPAA statutes when network firewall protection had been disabled. The oversight resulted in a $400,000 penalty (Yu, 2013). Moreover, the recent implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009 increased the fines resulting from failure to comply with HIPAA, including fines for individuals claiming they "did not know" that can range from $100–$50,000 (Modifications to the HIPAA Privacy, 2013, p. 5583). The final omnibus ruling of HIPAA–HITECH, enforcing these violations, went into effect on March 26, 2013 (Modifications to the HIPAA Privacy, 2013; Ostrowski, 2014). Enforcement of the changes from the HITECH Act on HIPAA standards began on September 23, 2013, for covered entities (Modifications to the HIPAA Privacy, 2013).

Academic departments and universities must understand the importance of HIPAA and HITECH regulations in order to determine whether the department or university is considered a covered entity. Risk analysis and management need to be employed to avoid violations leading to penalties and fines (HIPAA, 2013, §164.308). Some counselor education programs that have students at medically related practicum or internship sites also may be considered business associates (see HIPAA, 2013, § 160.103) and would need to comply with HIPAA regulations (see HIPAA, 2013, § 160.105). The authors recommend that all counselor education programs confer with appropriate legal sources to understand any risks or liabilities related to HIPAA regulations and relationships with practicum and internship sites. Many states also have their own unique privacy laws that must be considered in addition to those described in HIPAA regulations. The purpose of this article assumes that a counselor education department is not considered a covered entity by the regulations set forth by HIPAA. However, as an increasing number of counselor education programs incorporate the use of digital videos or digital audio recordings, a need for a set of policies and procedures to guide the appropriate use of digital media is evident.

The authors believe that the regulations set forth by HIPAA and HITECH create a series of guidelines that could dictate best practices for counselor educators when considering how to utilize technology in the collection, storage and transmission of any individual's electronic PHI (Wheeler & Bertram, 2012) within counselor education programs. HIPAA regulations (2013, §160.103) describe electronic protected health information (ePHI) as any information classified as PHI, as described above, either "maintained by" or "transmitted in" (p. 983) electronic media. For example, audio recordings used in practicum and internship courses are often collected electronically by digital recorders. If the recordings remain on the device, this protected information is being maintained in an electronic format. If the data is shared through e-mail or uploaded to a computer, then it is being transmitted in electronic format. As it relates to counselor training, the PHI that is collected could be real or fictitious (i.e., from someone role playing in the program). Though fictitious information is not necessarily protected, encouraging students to engage in implementing a set of policies and procedures guided by regulations of HIPAA and HITECH creates an experiential milieu whereby students become aware of and learn the importance of security and privacy when handling digital ePHI. The authors will discuss throughout this article how specific regulations from HIPAA and HITECH can be utilized to create a set of policies and procedures that guide the ways in which members of counselor education programs can handle any ePHI they encounter during their training. These direct experiences will give faculty and students greater familiarity with current HIPAA and

HITECH regulations, thus making them better prepared to work ethically and legally in modern mental health culture.

This article is not meant to cover HIPAA and HITECH regulations in a comprehensive manner. Overviews of these standards have been written concerning the regulations of HIPAA and HITECH regarding the work of mental health practitioners (see Letzring & Snow, 2011). The degree to which the myriad regulations of HIPAA will be implemented in various counselor education programs will need to be decided by the members of individual programs and by necessary stakeholders. The authors hope to introduce a dialogue regarding the thoughtful use of technology in counselor education programs guided by the parameters set forth by HIPAA.

According to the Substance Abuse and Mental Health Services Administration (SAMHSA; 2013), the trend in mental health care treatment spending is in the direction of public (i.e., Medicare and Medicaid) and private insurance growth as a means of payment. Spending for all mental health and substance abuse services totaled $172 billion in 2009; moreover, this spending accounted for 7.4% of all health care spending that year. Additionally, it is projected that spending on all mental health and substance abuse services could reach $238 billion by 2020 (SAMHSA, 2014). However, the rate at which individuals pay out-of-pocket for mental health and substance abuse services is expected to decrease steadily (SAMHSA, 2014). Historical trends show out-of-pocket spending decreased from 18% of all spending in 1986 to 11% in 2009 (SAMHSA, 2013, 2014). It is projected that out-of-pocket spending for mental health treatment will level off to account for approximately 10% of all spending while Medicaid, Medicare, and private insurance will account for approximately 70% of spending (SAMHSA, 2014). The trend toward greater insurance use will increase the number of professional counselors who will be seen as or will be working within organizations that are considered HIPAA-covered entities. Implementing policies and procedures in counseling departments that incorporate some of the HIPAA regulations is a useful way to prepare future professionals for the working environment they will enter (SAMHSA, 2013).

The implementation of the HITECH Act (2009) as a supplement to HIPAA emphasized the need to make sure future counselors understand the importance of the increasing role of technology in the practice of counseling (Lawley, 2012). The HITECH Act established an expectation that professionals in health care must be familiar with technology, specifically as it relates to policies guiding the storage and transmission of ePHI. The objectives of HITECH include "the electronic exchange and use of health information and the enterprise integration of such information" and "*the utilization of an electronic health record for each person* in the United States by 2014" (HITECH, 2009, §3001.c.A, emphasis added). Additionally, HITECH strengthened the enforcement of penalties for those who violate HIPAA (Modifications to the HIPAA Privacy, 2013). A multi-tiered system of violations allows for civil money penalties to range from $100–$50,000 per violation (Modifications to the HIPAA Privacy, 2013). The American Counseling Association's (ACA) 2014 *Code of Ethics* acknowledged the increasing use of technology by professional counselors by introducing a new section (Section H) addressing the ethical responsibility of counselors to understand proper laws, statutes, and uses of technology and digital media. Ethical counselors are expected to understand the laws and statutes (H.1.b), the uniqueness of confidentiality (H.2.b), and the proper use of security (H.2.d) regarding the use of technology and digital media in their counseling practice.

The mental health care system exists inside the broader health care system. As such, graduates of counseling programs must be familiar with HIPAA regulations and the various modes of technology to implement these regulations (ACA, 2014; Lawley, 2012). Students will be expected to understand what security and privacy standards are required of them once they begin working as counseling

professionals (ACA, 2014). For example, the movement toward increased use of ePHI across health care will place increasing demands on students to understand how to appropriately keep electronic data private and secure. Counselor educators need to be mindful of how the use of technology in the practice of counseling is being taught and implemented with counseling students. Counselor educators should thoughtfully consider how students will learn the ways in which technology can be used professionally while maintaining ethical and legal integrity (Association for Counselor Education and Supervision [ACES] Technology Interest Network, 2007; Wheeler & Bertram, 2012). Having standards to guide the use of ePHI throughout counselor education programs is a way in which students can become knowledgeable and skilled regarding the laws and ethics surrounding digital media. Policies and procedures should include information guiding the ways in which students collect, store and transmit digital media (e.g., audio recordings or videotapes) while a member of the counseling program. By requiring students to utilize the ePHI (real or fictitious) they collect in accordance with policies and procedures informed by HIPAA and HITECH, students crystallize their understanding of these complicated laws.

HIPAA Compliance and Technology

Complying with HIPAA Privacy and Security Rules requires individuals to be mindful of policies and procedures, known as "administrative safeguards" (HIPAA, 2013, §164.308, p. 1029), and work to implement safeguards consistently. The HHS has made clear that it does not provide any type of credential to certify that an individual, business, software or device is *HIPAA compliant* (HHS, n.d.-a; Reinhardt, 2013). Complying with HIPAA rules requires organizations and individuals to address many different processes where choice of hardware or software is only one aspect (Christiansen, 2000). Being HIPAA compliant is less about a certification or a credential on a device and more about having a set of policies and procedures in place that ensure the integrity, availability and confidentiality of clients' ePHI (Christiansen, 2000; HHS, n.d.-b). Hardware and software technology companies who make claims that a product or an educational resource is HIPAA compliant are likely doing so for marketing purposes. Claims of this type are mostly meaningless (HHS, n.d.-a) and would not provide protection in the case of a breach (HITECH, 2009). Being HIPAA compliant is an "organizational obligation not a technical specification" (Christiansen, 2000, p. 7). The distinction is important for educators to understand as they seek to implement technology in counselor education programs. When establishing a set of policies and procedures within a counseling department, the recommendations set forth in describing the security and privacy of PHI in Part 164 of HIPAA (2013) can be an appropriate framework for establishing best practices for counselors and counselor educators. The general requirements in complying with HIPAA security standards are to ensure the confidentiality, integrity and availability of individuals' ePHI while protecting against any reasonably anticipated threats to the security and privacy of said ePHI (HIPAA, 2013, §164.306.a). The key phrase to consider is that covered entities are asked to protect against any "reasonably anticipated" (HIPAA, 2013, §164.306.a, p.1028) threat. Educators must understand the importance of spending time considering reasonable, foreseeable risks. A primary responsibility is to create administrative safeguards that address any reasonable, foreseeable risks, which the individual, department or covered entity establishes.

Before looking at key aspects of HIPAA Privacy and Security guidelines, key definitions should be understood:

- Administrative safeguards include policies and procedures used to manage the development, selection, implementation and security in protecting individuals' ePHI (HIPAA, 2013, § 164.304).

- Authentication includes "the corroboration that a person is the one claimed" (HIPAA, 2013, § 164.304, p. 1027).
- Confidentiality defines "the property that data or information is not made available or disclosed to unauthorized persons or processes" (HIPAA, 2013, § 164.304, p. 1027).
- Encryption is "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key" (HIPAA, 2013, § 164.304, p. 1027).
- Security incident is described as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operation in an information system" (HIPAA, 2013, § 164.304, p. 1027).

HIPAA (2013) standards are categorized as either *required* or *addressable* as indicated in Section 164.306.d.1. The rest of this document will highlight the standards that the authors believe shape a set of best practices for counselor educators when implementing technology into their counselor education programs. The degree to which a counseling program decides to implement those standards that are considered required or addressable will be determined by their status as a covered entity, state laws, needs of their counseling program and the financial feasibility of implementing these standards.

Safeguards

HIPAA requires that all covered entities maintain policies and procedures that (1) ensure confidentiality and availability of all electronic PHI, (2) protect against any *reasonably* (emphasis added) anticipated threats or hazards to the security or integrity of ePHI, (3) protect against any *reasonably* anticipated uses or disclosures of ePHI, and (4) ensure compliance by the workforce. The following sections will discuss ways in which HIPAA Privacy and Security rules can be utilized as best practices in counselor education programs so that foreseeable risks, threats and vulnerabilities may be minimized. Please note that this interpretation of safeguards is intended for the consideration of counselor education programs that are *not* covered entities, but may use HIPAA Privacy and Security rules to establish a set of policies and procedures as a means of best practice. (For a sample guide for counselor educators to use in developing policies and procedures, please contact the first author).

Administrative Safeguards

Administrative actions and oversight make up an important component of the language within HIPAA (2013). Administrative safeguards consist of the policies and procedures designed to "manage the selection, development, [and] implementation" (§ 164.304, p. 1027) of the security and privacy of one's ePHI. This section describes HIPAA standards to consider when establishing administrative safeguards.

Assigned responsibility. A faculty or staff member within the counselor education program should be identified as responsible for the development, oversight and implementation of the policies and procedures for the department. The faculty member needs to be familiar with the privacy and security policies of HIPAA in order to implement the policies and procedures and to facilitate student training in ways that address the specific needs of the program. Developing a relationship with a staff member in the university information technology department may result in collaborative efforts regarding specific procedures for the use of technology within the university.

Risk analysis. Before counselor educators can design a set of policies and procedures to guide appropriate technology use, the foreseeable risks must be analyzed. An accurate and thorough assessment is needed to identify potential risks to the protection and security of ePHI (HIPAA, 2013, §164.308) that is collected, stored and transmitted in the counseling program. Analyzing potential risk is essential to the minimization of potential disasters in the future (Dooling, 2013). HHS (2007) makes clear that it is important to spend time considering reasonably anticipated threats and vulnerabilities and then to implement policies and procedures to address the assessed risks. HIPAA security standards do not state that covered entities should protect against *all possibly conceived* threats, but those that can be "reasonably anticipated" based upon the technologies employed, work environments and employees of the covered entity. The National Institute of Standards and Technology (NIST; 2012) defines a threat "as any circumstance or event . . . with the potential to adversely impact organization operations . . . through an information system via unauthorized access, destruction, disclosure, or modification of information" (p. B-13). A risk is a measure of the probability of a threat triggering a vulnerability in the procedures that an organization uses to ensure the privacy and security of ePHI (NIST, 2012). Vulnerabilities are technical and non-technical weaknesses, which include limitations in utilized technology or ineffective policies within the organization (HHS, 2007). In counselor education programs, risk analysis may include looking at the threats and vulnerabilities associated with counseling students traveling between their residence, campus, and practicum or internship sites while carrying ePHI. Moreover, the analysis must include assessing the potential risks associated with the transmission and storage of protected information using technological media (e.g., e-mail, personal computers, cloud-based storage, external storage devices).

Risk management. Risk management is the ongoing process of implementing measures to reduce the threats that were determined as a part of the risk analysis (HHS, 2007). Once a counseling program has assessed and identified potential risks associated with the collection, transmission and storage of any identifiable information, it must begin to manage these risks. HHS has provided an example list of steps to assist organizations in conducting risk analysis and risk management (see Table 1). Members of counselor education programs can begin to incorporate programmatic policies and procedures that address how media containing ePHI should be handled by members of the program. The previously mentioned document (available from the first author) provides sample policies and procedures developed to serve as a guide for counseling programs. Many counselor education programs utilize student handbooks that detail policies related to the academic and professional expectations of students enrolled in their program. Incorporating an additional set of policies to address the treatment of ePHI is a seamless way to begin managing the risks of technology use in mental health. By implementing policies and procedures across the curriculum, students become increasingly knowledgeable and skilled at handling ePHI in an ethical manner.

Table 1

Example Risk Analysis and Risk Management Steps

Risk Analysis
1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine likelihood of threat occurring.
6. Determine potential impact of threat occurrence.
7. Determine level of risk.
8. Identify security measures and finalize documentation.
Risk Management
1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

Note. Adapted from "Basics of Risk Analysis and Risk Assessment," by the U.S. Department of Health and Human Services, 2007, *HIPAA Security Series*, 2(6), p. 5.

Sanction policy. It must be communicated to all members of counselor education programs that failure to comply with the policies will result in sanctions. HIPAA (§164.308, 2013) requires organizations to enforce sanctions against individual members for failing to comply with their organization's policies and procedures. A counselor education program should have clearly documented policies and procedures for students and staff involved with the facilitation of ePHI. The language of HIPAA makes no attempt to clarify as to what these sanctions should entail; however, language needs to exist that addresses individuals' failure to comply. For counseling students, a potential option is to consider a tiered sanction policy similar to that of the structure established by the HITECH Act (Modifications to the HIPAA Privacy, 2013) and § 1176 of the Social Security Act (2013). Varying categories of violations from "did not know" (p. 5583) to uncorrected–willful neglect result in increasingly severe fines (Modifications to the HIPAA Privacy, 2013). Since this experience is most likely educational for students, varying degrees of failure to comply could exist. For counselor education programs, this language also could easily be tied to student remediation processes that many counseling programs utilize.

Information review. Ongoing review of the activity of students, faculty and staff that involves the creation, storage and transmission of ePHI is a required safeguard according to HIPAA standards (2013, §164.308). As an educational unit, it is understandable that individuals might make mistakes regarding the implementation of HIPAA safeguards. A regular review of the activity and records of the individuals whose ePHI are being collected is important. It is required for organizations to have policies in place for recording system activity, including access logs and incident reports (§ 164.308). Additionally, protections must be in place to ensure that only those individuals who should have access to any ePHI are able to access this protected information. In the case of the sanctioned university medical training clinic cited earlier, the breaches might have been avoided with an ongoing review of the system's firewall settings (Yu, 2013). Monitoring and developing policies regarding information review may require developing relationships and discussions with the appropriate information technology personnel at the organization.

Response, recovery and reporting plan. HIPAA regulations require that a covered entity have a plan in place should ePHI be breached or disclosed to an unauthorized party (HIPAA, 2013, § 164.308). When developing departmental policies and procedures, it is important to have such a plan in place. Whether the breach or disclosure is intentional or unintentional, each individual whose information has potentially been compromised needs to be notified. Moreover, in cases where more than 500 individuals' PHI have been breached, the entity may need to report this information to local media or to HHS (HIPAA, 2013, §164.406–164.408). It should be noted that covered entities could be exempted from breach notification through employing security techniques such as encryption (Breach Notification, 2009; HIPAA, 2013, §164.314). The regulations of HIPAA require that a plan be in place to address emergencies (HIPAA, 2013, §164.308). In the case of theft, emergency or disaster, counseling departments need a data backup and recovery plan in place to retrieve ePHI.

Physical Safeguards

Establishing policies and procedures that protect against unauthorized physical access and damage from natural or environmental hazards is critical to maintaining the security and privacy of PHI (HIPAA, 2013, §164.310).

Access control. When using technology to store and transmit ePHI, the recommendation is that policies address ways in which physical access to protected information will be limited. For example, many counseling departments now incorporate the use of digitally recorded data from counseling sessions (e.g., audio or video). Policies need to clearly address how to best limit physical access to these recordings. Students need to understand what it means to keep data physically secure. The HITECH Act (Modifications to the HIPAA Privacy, 2013) includes the category "did not know" as a punishable violation. Students need to understand the consequences of failing to implement such physical safeguards. For example, keeping devices stored under lock and key when not in use is just one important step in moving toward a set of best practices. Many universities already require students to utilize login information with a username and passcode in order to access computers affiliated with their respective university. Consideration may need to be given regarding policies and procedures for accessing ePHI off campus, where the technical security may be less controlled.

Disposal and re-use. HIPAA requires covered entities to implement policies that address the disposal and re-use of ePHI on electronic media. A detailed discussion of the various types of disposal, also known as media sanitization, and re-use is beyond the scope of this article (see Kissel, Regenscheid, Scholl, & Stine, 2014). Counselor education programs must recognize the importance of properly removing protected information from media devices after it is no longer required. Media

sanitization is a critical element in assuring confidentiality of information (Kissel et al., 2014). For example, in counseling internship courses, students may be asked to delete recorded sessions during the last day of classes so that the instructor can have evidence of the appropriate disposal of this information. NIST identifies four different types of media sanitization: disposal, clearing, purging and destroying (Kissel et al., 2014). The decision as to which type of media sanitization is appropriate requires a cost/benefit analysis, as well as an understanding of the available means to conduct each type of sanitization. (The authors recommend counseling departments consult with an individual from the university information technology department).

Technical Safeguards

The language in HIPAA is clear regarding the implementation of technical safeguards, requiring that access to electronic media devices containing PHI be granted only to those who need such access to perform their duties.

Unique user identification. If a device allows for unique user identification, one should be assigned to minimize the unintended access of ePHI. HIPAA standards (2013, §164.514) state that an assigned code should not be "derived from or related to information about the individual" (p. 1064).

Emergency access. Covered entities are required to have procedures in place that allow ePHI to be accessed in the event of an emergency (HIPAA, 2013, §164.310). The procedures can be addressed within counselor education programs so as to ensure that the student and the supervisor have access to the ePHI at the designated storage location.

Encryption. Encryption is a digital means of increasing the security of electronic data. Using an algorithmic process, the data is scrambled so that the probability of interpretation is minimal without the use of a confidential key to decode the information. Though the language of HIPAA categorizes encryption as addressable rather than required, the implementation of encryption policies is a best practice to help ensure the protection of ePHI. The language of HIPAA makes it clear that an "addressable" item must be implemented if it is "reasonable and appropriate" (HIPAA, 2013, §164.306, p. 1028) to do so. Huggins (2013) has recommended that ePHI be stored on drives that allow for "full disk encryption" at a minimum strength of 128 bits. With the availability of many different types of software packages that can encrypt at a recommended strength, implementing encryption standards in a counseling department is affordable and reasonable. Most modern computer operating systems have options to encrypt various drives built into the functionality of the system. Full disk encryption is recommended because of its higher level of security and also because it can provide exemption from the Breach Notification Rule mentioned earlier (Breach Notification, 2009). In case of a breach, the burden is on the covered entity to prove that the ePHI was not accessed; otherwise, Breach Notification Rules must be followed. The assumption is that if a disk is fully encrypted, even if accessed by an unauthorized person, it is highly unlikely that an unauthorized party will obtain access to the ePHI (Breach Notification, 2009). The authors strongly encourage the use of encrypted devices as a standard policy for the collection and storage of ePHI (see Scarfone, Souppaya, & Sexton, 2007). The policy creates greater protection against the accidental disclosure of an individual's ePHI. Additionally, organizations that use commercial cloud storage service providers should investigate whether these providers are willing to sign a Business Associate Agreement, in which the provider agrees to adhere to regulations of HIPAA (2013, §160.103). If not, the storage of ePHI may not be in alignment with HIPAA standards.

Disk encryption works well for the storage and collection of protected information while at rest (Scarfone et al., 2007); however, counselor education programs also should consider assessing the risk associated with the transmission of ePHI (HIPAA, 2013, §164.312). Protected information often remains encrypted while at rest, yet becomes unencrypted while in transmission. Programs need to "guard against unauthorized access to electronic PHI that is being transmitted over an electronic communication network" (HIPAA, 2013, §164.312, p. 1032). Commonly used e-mail systems, for example, often do not transmit information in an encrypted state. Assessment of the risks in sending protected information by an unsecured means should be conducted.

Discussion

The language of HIPAA allows each covered entity some leeway in how it wants to implement policies. However, HIPAA standards (2013, §164.316) are very clear that entities should "implement reasonable and appropriate policies"(p. 1033) that include administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits. The implementation of HITECH (2009) and the meaningful use policies of the Affordable Care Act (Medicare and Medicaid Programs, 2014) emphasized the movement of the broader health care system toward increasing use of health care technology such as Electronic Health Records. Students graduating from counseling programs find themselves working in myriad settings, many of which are considered covered entities as defined in the HIPAA standards (2013, §160.103). It is imperative for counselor educators to recognize the trend toward increased technology use in the health care market and to consider ways that technology can be infused into counselor education so that students are entering the workforce with greater technological competence. Specifically, counselor educators have an imperative to teach the ethical and legal technological mandates that exist as they relate to regulations of HIPAA (2013) and HITECH (2009) so as to create competent counselors. As the health care industry continues to incorporate more technology, counselor educators must stay informed regarding ways in which graduates will utilize this technology in their professional careers.

Recommendations for Counselor Educators

ACES (2007) published a document that recommends guidelines for infusing technology into counselor education curriculum, research and evaluation. This document provides a basic overview by which programs should guide the very broad use of technology in counseling programs. Technology is presented as a useful enhancement or supplement to practice. The shift in the broader health care culture has moved technology from a supplementary role into one in which it is primary to the ongoing success of a practitioner. The authors believe that counselor educators can utilize HIPAA and HITECH regulations to continue to infuse technology into counselor education programs, and recommend the following:

1. Counselor educators need to increase the importance placed on technology in counselor education programs. The movement of technology into increasingly primary roles in health care is indicative of the need for it to become a primary focus during the education and training of counselors. Counselors and counselor educators must stay abreast of the trends and developments regarding health care law and technology. The implementation of Section H, "Distance Counseling, Technology, and Social Media," in the 2014 *ACA Code of Ethics* also is indicative of this need. The counseling profession needs to increase the research, education and training available to counselors and counselor educators.

2. Counselor educators need to have policies and procedures in place guiding the use of technology in their departments. The overview of HIPAA regulations will help provide guidelines for developing a set of policies and procedures. All policies and procedures must be in writing and accessible to students, faculty and staff who have access to any ePHI. Many counseling programs maintain a student handbook in which a set of standards that dictate the use of technology could easily be incorporated. Departmental policies should be in place that dictate the consequences should an individual fail to adhere to the stated policies and procedures.

3. Counselor educators should be actively seeking ways in which technology and HIPAA can be incorporated to best prepare students for their future work environment. The regulations and language of HIPAA and HITECH should be addressed in course activities. Are counseling students getting opportunities to become familiar with Electronic Health Records? Are students having opportunities to write and store notes electronically? Have students addressed the ethical and legal concerns related to the use of technology in practice? Do students understand what it means to maintain encrypted files or how to appropriately de-identify ePHI? Do students understand how to submit health insurance claims electronically? Questions like these are necessary for students to understand so they can be prepared to work in the current mental health environment as competent professionals.

The use of technology in counseling is moving from a secondary to a primary place in counselor education. The expectation that students can find this information after graduation in the form of a workshop is no longer acceptable. The shifts in the language of HIPAA and HITECH have moved the broad health care field in an electronic, digital direction. The familiarity with technology seems to be growing toward a core competency of counselor education programs and faculty. The laws dictated by HIPAA and HITECH provide a framework by which counselor educators can continue to infuse technology into the classroom and clinical experiences.

Conflict of Interest and Funding Disclosure
The authors reported no conflict of interest or funding contributions for the development of this manuscript.

References

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

Association for Counselor Education and Supervision Technology Interest Network. (2007). *Technical competencies for counselor education: Recommended guidelines for program development*. Retrieved from http://www.acesonline.net/sites/default/files/2007_aces_technology_competencies.pdf

Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 162 (August 24, 2009) (to be codified at 45 CFR §§ 160 & 164).

Christiansen, J. (2000). Can you really get "HIPAA Compliant" software and devices? *IT Health Care Strategist*, *2*(12), 1, 7–8.

Dooling, J. A. (2013). It is always time to prepare for disaster. *Journal of Health Care Compliance*, *15*(6), 55–56.

Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII § 13001 of Division A of the American Recovery and Reinvestment Act of 2009 (AARA), Pub. L. No. 111-5 (2009).

Health Insurance Portability and Accountability Act (HIPAA), 45 CFR §§ 160, 162, & 164 (2013). Retrieved from http://www.gpo.gov/fdsys/pkg/CFR-2013-title45-vol1/pdf/CFR-2013-title45-vol1-chapA-subchapC.pdf

Huggins, R. (2013, April 5). *HIPAA "safe harbor" for your computer (the ultimate in HIPAA compliance): The compleat [sic] guide* [Blog post]. Retrieved from http://www.personcenteredtech.com/2013/04/hipaa-safe-harbor-for-your-computer-the-ultimate-in-hipaa-compliance-the-compleat-guide/

Kissel, R., Regenscheid, A. Scholl, M., & Stine, K. (2014). *Guidelines for media sanitization* (NIST Publication No. 800-88, Rev. 1). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Lawley, J. S. (2012). HIPAA, HITECH and the practicing counselor: Electronic records and practice guidelines. *The Professional Counselor*, *2*, 192–200. doi:10.15241/jsl.2.3.192

Letzring, T. D., & Snow, M. S. (2011). Mental health practitioners and HIPAA. *International Journal of Play Therapy*, *20*, 153–164. doi:10.1037/a0023717

Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program for 2014 and Other Changes to the EHR Incentive Program; and Health Information Technology: Revisions to the Certified EHR Technology Definition and EHR Certification Changes Related to Standards Final Rule, 79 Fed. Reg., 179 (September 4, 2014) (to be codified at 45 CFR pt. 170).

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg., 5566 (January 25, 2013) (to be codified at 45 CFR pts. 160 and 164).

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication No. 800-30, Rev. 1). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Ostrowski, J. (2014). *HIPAA compliance: What you need to know about the new HIPAA-HITECH rules*. Retrieved from http://www.nbcc.org/assets/HIPAA_Compliance.pdf

Reinhardt, R. (2013, October 3). *Your software and devices are not HIPAA compliant* [Blog post]. Retrieved from http://www.tameyourpractice.com/blog/your-software-and-devices-are-not-hipaa-compliant

Scarfone, K., Souppaya, M., & Sexton, M. (2007). *Guide to storage encryption technologies for end user devices: Recommendations of the national institute of standards and technology* (NIST Special Publication No. 800-111). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Social Security Act, 42 U.S.C. § 1176 (a)(1). (2013). Retrieved from http://www.ssa.gov/OP_Home/ssact/title11/1176.htm

Substance Abuse and Mental Health Services Administration. (2013). *National expenditures for mental health services & substance abuse treatment, 1986–2009* (HHS Publication No. SMA-13-4740). Retrieved from http://store.samhsa.gov/shin/content//SMA13-4740/SMA13-4740.pdf

Substance Abuse and Mental Health Services Administration. (2014). *Projections of national expenditures for treatment of mental and substance use disorders, 2010–2020* (HHS Publication No. SMA-14-4883). Retrieved from http://store.samhsa.gov/shin/content//SMA14-4883/SMA14-4883.pdf

U.S. Department of Health and Human Services. (n.d.-a). *Be aware of misleading marketing claims*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/misleadingmarketing.html

U.S. Department of Health and Human Services. (n.d.-b). *Summary of the HIPAA privacy rule*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

U.S. Department of Health and Human Services (HHS). (2007). *Basics of risk analysis and risk management*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

Wheeler, A. M. N., & Bertram, B. (2012). *The counselor and the law: A guide to legal and ethical practice* (6th ed.). American Counseling Association: Alexandria, VA.

Yu, E. H. (2013). HIPAA privacy and security: Analysis of recent enforcement actions. *Journal of Health Care Compliance*, *15*(5), 59–61.