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 50

A Counseling Clinic Digital Recording System—In a Box

Timothy D. Baker

Baker, Timothy D., is an associate professor in the School Counseling program at St. Cloud State University in St. Cloud, Minnesota. His research interests include school safety and climate, emergency mental health, and ethical issues in technology use by counselors.

Abstract

The graduate training of professional counselors requires video recording of practice sessions with clients. Legacy recording technologies, such as VCRs and analog video-cameras hard-wired into interview rooms, are becoming difficult to maintain. This document describes a technology which has matured in recent years: low-cost IP cameras designed for home security applications and marketed directly to consumers. A demonstration was conducted to evaluate the cameras' durability in continuous use and whether it was possible to configure them securely. Results are presented alongside detailed discussion of the HIPAA Security Rule.

In the United States, entry-level employment as a professional counselor requires a master's degree. In graduate programs accredited by the Council for Accreditation of Counseling and Related Educational Programs (CACREP), trainees video record their sessions or are supervised live (CACREP, 2009). Benefits to trainees include enhanced conceptualization and applied skills. Counseling pioneer Carl Rogers was among the first to record using audiotape; later counselor educators used videocassette recorders (VCRs), which were often installed the cameras unobtrusively in an interview room, hard-wired to VCR equipment in a locked control booth.

VCRs are no longer ubiquitous, and though many digital alternatives exist (e.g., portrait and sports cameras, smartphones, laptop webcams), each has unique potential risks and may be difficult to install in a small, shelf-less interview room that was designed for a camera in the ceiling. Faculty members may ask: What digital recording technology can easily be standardized, can be made private and secure, does not cost tens of thousands of dollars, and will not become obsolete within years?

Internet Protocol (IP) Cameras

Just as the consumer VCR once descended from high-end television studio gear, a new family of consumer electronics has been streamlined from professional equipment:

the Internet Protocol (IP) camera. (Despite the name, the camera is not necessarily connected to the Internet, but rather to a local network within the building, similar to a shared office printer.) Early IP cameras were specialized devices for videoconferencing and commercial security. Today IP cameras are mass-produced. They support multiple levels of password protection and encryption, can be configured for allowing (or blocking) remote viewing, and some models offer "pan-tilt-zoom" (PTZ) rotation (side-to-side and up-and-down). Different brands of IP camera can co-exist on the same network, and be integrated using third-party software. IP cameras for home security use are inexpensive, can be purchased from major retailers, and are designed to be simple for consumers to install on home Wi-Fi® networks. (Wi-Fi® is a trademark of the Wi-Fi Alliance®, an industry group that also certifies equipment that operates on a Wireless Local Area Network [WLAN] conforming to the IEEE 802.11 standard. The term is in general household use; however, due to the costs of optional certification through the Wi-Fi Alliance®, not all equipment of good quality will bear the Wi-Fi® logo. In the remainder of this document, Wi-Fi® networks will be described as "wireless LAN" or "WLAN" unless referring to a specific software button or control, such as a configuration page labelled "wifi" [s.i.c.] in the router control panel.)

The goal of this demonstration was to test the reliability of home security IP cameras and assess their potential for secure use in a counselor training setting. To this end, a low-cost, reliable video recording system was built entirely with off-the-shelf components from a major consumer electronics store—a clinic recording system that comes in a box, can be unpacked and installed simply, and secured practically.

HIPAA Aspects

Counseling program faculty naturally may be inclined to prefer HIPAA-compliant software products, even though most training programs are not HIPAA "covered entities" (i.e., healthcare providers whose services are electronically billed to a third party). One difficulty with identifying HIPAA-compliant software is that HIPAA regulates entities—healthcare providers and also software vendors—not products. When software is described as HIPAA-compliant, in reality this means the vendor is willing to sign a Business Associate agreement promising to help the covered entity be compliant. However, the U.S. Department of Health and Human Services (HHS; 2007) warns covered entities that merely purchasing software is not the same thing as entering into a Business Associate agreement. Covered entities become HIPAA-compliant only through a self-study process, and HHS (2010) does not recognize HIPAA "certifications" provided by private companies. It does matter that some software packages are of higher quality than others, but it matters more whether the covered entity understands the HIPAA security rule well enough to apply the software appropriately. (For a conversational discussion of these nuances from the private practitioner's perspective, see Reinhardt [2013] and Quinn [2009]).

Rather than advocate one-size-fits-all implementations, HIPAA expects a covered entity to understand the Security Rule and devise a plan that weighs the entity's resources and technical skills against the cost and relative risks of security concerns (HHS, 2006). A summary of the Security Rule is available from HHS (2009), and the National Institute of Standards and Technology (NIST) resource guide for implementing the HIPAA security rule (Scholl et al., 2008) offers extensive, concrete assistance. This document

will reference those safeguards throughout, especially the physical safeguards (facility access control, workstation security) and technical safeguards (electronic access control).

HIPAA also requires administrative safeguards, including the designation of a compliance officer, training for all employees in standardized procedures, and a sanctions policy (i.e., employment reprimands) "so that workforce members understand the consequences of failing to comply with the security policies and procedures" (HHS, 2006, p. 3), an example of which might include locking a laptop inside a car. Clearly, even though graduate students and faculty members take seriously their ethical responsibilities, it would be difficult to implement in the academic setting the same strict adherence to HIPAA regulations that would be expected in a healthcare workplace. Thus, rather than aspire to becoming HIPAA pseudo-compliant, perhaps the better goal for program faculty should be to thoroughly understand the HIPAA Security Rule as an inspiration for future discussion. Counselor educators and graduate students can devise thoughtful, responsible approaches for protecting their clients' privacy while acknowledging that the program exists to support development of new professionals.

Planning Considerations

Before designing a video recording system for counseling trainees, program faculty should ask: "What is the least that our recording system needs to do?" Often, a minimal approach that implements the training model will be the most cost-effective, reliable, and usable. Two essential questions: (1) Does the counseling interview need to be viewed live outside the session, and (2) will students be solely responsible for storing and keeping the video file in their possession? Table 1 depicts a matrix of answers to this question; if they are "no" and "no," (as in Model #1 in Table 1), the recording system can be quite simple, as demonstrated by one counseling center's experience.

Simple Scenario

The counseling center at a regional comprehensive university offered internships to a small number (<10) of graduate counseling students. Each intern had a private office with a computer; for each, the center purchased a high-definition webcam that would include the full room in its field of view. Using the manufacturer-supplied cam software, interns pressed "record" at the beginning of the session then turned off the screen. After the client left, interns would stop recording and then transfer the video file to the center's network drive (Windows network file sharing, called "FileSpace" at this campus). Each FileSpace folder is "owned" by a specific user account and can be shared with others, or not at all. This technology is a core feature of large computer networks and is considered very secure; FileSpace cannot be accessed without the proper username and password, or from off-campus (unless the university VPN is used). The interns were given numbered accounts (e.g., "Intern01") and were responsible for keeping their passwords secure. Using this password, the FileSpace folder could be accessed only from the computers in the counseling center, for the purpose of showing video at the weekly supervision meeting. Interns also agreed not to transfer the video files to their personal computers; all personal review and reflections would be done by interns in a secure room at the counseling center. At the end of the semesters, IT staff re-set the passwords on the intern accounts, thus revoking access.

Table 1

Critical questions and examples of recording systems

Will the Session Be Reviewed Remotely?	Who Is Responsible for Storing the Video Files?	
	The University	The Student
No	1. Record with university-owned computer using webcam. Store the video files on the university's internal network storage. Allow trainees only to access videos from within the facility. Trainees' access to shared folder expires at end of semester.	2. Trainees record using personally- owned laptops, with agreement to use (a) file and/or drive encryption, (b) anti-virus protection, (c) strong passwords, and (d) cache disabling, in addition to traditional ethical promises. Some IP cameras can record directly onto removable micro-SD cards.
Yes	3. Recording cameras are fixed in the interview room. Control server is located in a locked room accessed by authorized trainees. Digital (IP) cameras record directly to the server; analog "legacy" cameras record through an A/V capture device. Recorded files are stored on the university's internal network file share (see above) and students are given folder which can be used only on-campus and only during that academic semester. 4. Or, the university contracts with a specialized HIPAA vendor for Web-based recording and cloud storage; students and faculty obey all security guidelines required by the vendor (e.g., mandatory trainings, signed user agreements of compliance, and others).	5. Recording cameras are fixed in the interview room and control server is located in locked room; students transfer files to an encrypted flash drive and agree to make security upgrades to their personally-owned laptops (see #2, above). 6. Or, trainees use an approved, encrypted Web service (i.e., not Skype, Yahoo Messenger, Google Chat, etc.) to record using their laptop's internal webcam while simultaneously re-broadcasting to authorized observers. Trainees also perform security enhancements (above) to their laptop computers.

Though simple, this example has many HIPAA-consistent features. Technical safeguards included the requirement of a password to access files. A physical safeguard included the restriction that videos be viewed only on computers at the counseling center, because viewing a video may sometimes result in a cache file (a copy) on that machine, or expose the file contents to viruses, which are more likely to be found on a personal

computer. Administrative safeguards involved interns' responsibility to keep secure passwords. Access controls were implemented: Interns were not able to browse each other's videos. Encryption was not necessary in this case because all data were stored on a highly-secured computer network maintained by the IT staff. The "audit trail," a HIPAA-required feature to track who has accessed any private information, was not needed and indeed, makes little sense in a training environment, because clients agreed during the informed consent stage that their counselor would be showing and discussing the counseling video with the clinical supervisor and peers.

Thus, the center's use of existing resources and avoidance of superfluous features kept expenses limited to the webcam purchases, under $100 per unit. No part of the video recording system software was intended for healthcare use nor offered for sale as "HIPAA-compliant," nor would such a label have automatically increased the clients' level of privacy. Technology is not inherently "secure" or "insecure," rather the professional counselor's responsible use establishes a balance of risks vs. benefits.

Complex Scenarios

If, however, the counseling session needs to be viewed remotely elsewhere in real time (i.e., to gain the "one-way mirror" functionality when facilities are not specially designed for that purpose), the approach must be more complex. This is especially likely when multiple trainees are in session concurrently, or when peers and a supervisor will immediately be giving feedback. The author, a counselor educator in a CACREP-accredited program, has worked extensively using this training model, which includes one-way glass separating interview rooms from an observation room, and a locked "control room" where the analog recording equipment is stored, which students access using a combination keypad. If interview rooms and observation rooms cannot be physically connected with a one-way glass, then a laptop computer with a webcam will not be adequate for recording interviews in this type of system, because it would need to "stream" (essentially, to re-broadcast) video data instead of merely storing them. This is technically possible with general video conferencing products, such as Skype, but these are not suitable for confidential communications because they are routed through an Internet server, increasing the level of vulnerability. Other high-end video conferencing products offering this functionality may be more secure, but due to their cost and complexity, they are not described in detail here.

IP-based video cameras offer a balance of flexibility vs. cost when recording and simultaneously streaming; they can be configured relatively securely on a local network, and have a high degree of interoperability using third-party software. This inquiry investigated the following questions: (1) Are consumer-grade IP cameras sufficiently durable to withstand months of continuous usage? (2) Can the recording system, including cameras, network, and control software, be configured consistently with the general HIPAA principles of restricting access to private data, protecting data during transmission, and encrypting it for storage?

Method of Demonstration

Cameras

A network recording system was assembled using IP cameras designed for consumer use. The four models selected were D-Link (see specifications, Table 2). This brand was selected because (1) it is inexpensive and carried by large retailers; (2) devices across this brand tend to have a relatively standardized Web control panel, and (3) these cameras were advertised to work with no monthly fees, suggesting that they need not be connected to the Internet (i.e., some other brands specifically stated their cameras could be accessed only through a subscription to a Web site). These features likely are not unique to the D-Link brand; they simply were easy to identify from the product packaging.

Table 2

Matrix of camera specifications

	DCS-5222L	DCS-5020L	DCS-942L	DCS-930L
Wireless LAN	Yes	Yes[1]	Yes	Yes [2]
Built-in secure server	Yes[3]	No	No	No
Image resolution	Hi-Definition	Standard	Standard	Standard
Lens field of view	Wide angle	Wide angle	Normal	Normal
Aspect ratio	"Letterbox"	Normal	Normal	Normal
micro-SD slot	Yes	No	Yes	No
Motorized pan-tilt- zoom capability	Yes	Yes	No	No
Infrared/night vision	Day/night	Day/night	Day/night	Daytime only
Two-way communication	Yes	No	Yes	No
Retail cost	$170 MSRP	$120 MSRP	$100 MSRP	$40 MSRP

1. Functional, but some difficulties re-configuring.
2. Did not function during testing.
3. Supports https connections using supplied "generic" security certificate from manufacturer. As with all self-signed (i.e., free) certificates, the Web browser will prompt user to confirm the certificate is legitimate.
4. Not tested; allows camera to serve as an intercom. Requires use of Web browser interface with Java; also, external speaker plugged into camera headphone jack.

Cameras were installed by plugging into an existing, hard-wired local area network (LAN). Next, the D-Link installation CD-ROM was launched on a computer, which "found" the IP address assigned to the camera (e.g., 192.168.2.99). If more than one camera had been found, they would be listed by MAC address, a sort of unique digital "serial number" which can be verified on a (tiny) placard on the back of the camera. Its IP address discovered, the camera's control panel will launch in a Web browser (now http://192.168.2.99). Note that the camera is only on the local network, not the Internet. The default admin password is blank. *It should be changed immediately.* Once configured using the wired LAN, the camera's wireless LAN (Wi-Fi®) connection then can be configured (as in this test), or disabled and turned off (recommended for a training clinic environment).

Network

In this case, the network was controlled by a D-Link router, a common consumer technology which hosts home wireless and wired networks and includes: a built-in "DHCP server," which assigns devices an IP address; a firewall, which is enabled by default to block access from the Internet; and MAC address filtering, which lets the administrator supply a list of approved MAC id's and which blocks all other devices from joining the network. Cameras were tested on the wireless LAN (encrypted with WPA-2) and also on the wired LAN. Wireless network access also could be switched off, meaning that the network could be accessed only by plugging in a cable. Thus, the router supported multiple layers of physical and technical safeguards.

Control Server

The server used was a refurbished Gateway desktop computer running Windows Vista. Performance specifications (memory and processor speed) for this device were low by current standards. After applying all operating system patches and configuring Microsoft Security Essentials, a free antivirus product, the D-Link camera control software "D-ViewCam" was installed. This software is available for free download from D-Link and can be used to control several D-Link cameras simultaneously. The D-ViewCam software did not work on the Windows Vista server, and was not repaired through subsequent troubleshooting. However, the D-ViewCam software did work on a laptop running Windows 7, used for remote viewing.

On the control server, third-party software was installed. Based on a previous recommendation, Blue Iris 3 was selected. Blue Iris costs $50 and has the ability to monitor different brands and models of security cameras, listing hundreds of different models in the configuration screens. Blue Iris records and has remote viewing access with password control. In order for it to run unattended under load, simulating clinical use, Blue Iris was left with the default configuration, which records when motion is detected.

Integration

Once installed and configured, the cameras, network, and control server were left powered on and running for approximately four months. Camera performance was checked with periodic review of the recorded video clips.

Results

Cameras

The cameras worked continuously; none failed outright. Some "quirks" were observed. On the wireless LAN, cameras lost connection to Blue Iris occasionally. Performance improved by adding a second wireless access point operating on another channel. In a training clinic setting, WLAN probably would not be used, for three reasons: (1) it was less reliable than the wired LAN, (2) unlike LAN, it does not present a physical access safeguard, and (3) the multitude of wireless connections in a public building causes signal interference, which decreases connection speeds. The latter is a particular concern to IT staff, who always should be consulted before any new network is installed in a university building. Wireless LAN was used in this demonstration mainly because testing was conducted off-site, where wireless simplified camera placement.

Camera 1 offered the best field of view, followed by Camera 2. Though both were equipped with motorized pan-tilt-zoom, in practice Camera 1 could capture almost the entire room when placed in a corner. Image quality was good on both cameras, but on Camera 2, colors appeared slightly "washed out"; some night-vision capable security cameras have less vivid color because their lenses are optimized for infrared light.

Camera 3 had some occasional unresponsiveness, which was stabilized by disabling the "day-night" mode, which reacted to low-light levels by shifting an infrared lens filter into place, with a loud audible "click." Perhaps this relay had become stuck. After this, Camera 3 worked normally. Camera 4 was able to detect the wireless LAN, but not actually connect. On the wired LAN network, Camera 4 performed flawlessly without crashing. Camera 2 connected to wireless LAN initially, but was unable to be switched to a different WLAN network. (These might reflect problems with the user interface rather than the device's wireless transmitter.)

Any cameras that were unresponsive were reset by unplugging and plugging back in. One by-product was loss of time and date from the on-screen display (OSD), which can be disabled. Though the cameras' Web interfaces offered a network time server option for automatic time and date, none seemed to work, and the time needed to be set manually.

Software

The Blue Iris software performed very well and did not "hang" or "crash." It included a CPU monitoring statistic showing what percent of the computer's capacity was being used, typically between 30–50% when displaying all cameras and listening to audio from one. The server was re-started approximately once per week. The free D-ViewCam software was tested on another machine; its features were adequate, but seemed to "crash" occasionally.

The cameras also can be controlled through a password-protected Web-based interface, which is accessible on the local network (but not the Internet unless the LAN is configured to allow it). This was the best method for initial configuration, but proved inconvenient for watching or recording live video. The Web browser client for live viewing required Java and did not always work due to frequent Java updates. Note that this was tested on a personally-owned computer; university computers may use a different version of Java, which was not tested.

Network

During the demonstration period, the wireless LAN did occasionally crash. It should be noted this network already was in use connecting numerous other devices. Consumer-grade routers for home use cannot deliver sustained, high-bandwidth performance; therefore, occasional problems should be considered normal for this level of use. Re-set procedures involved unplugging and plugging back in, typically every two weeks.

Discussion

The low-cost, consumer-grade IP cameras tested were not flawless, but did work reliably, and offered a range of security features. These cameras could be suitable for

building a recording system equivalent to #3 or #5, described in Table 1. By comparison, professional-quality cameras (e.g., Sony), such as those used by television studios and police agencies, can cost between $1000 to $2000 per camera. These professional-grade devices certainly are very reliable (as certainly they should be for such high-stakes purposes). In the counselor training context, it may be debated what cost level represents a reasonable use of limited funds. It should be emphasized that this document is not an endorsement of a particular brand nor even intended as a technical "benchmark"; the cameras demonstrated merely represent a sample of convenience.

One advantage of the IP camera recording system is modularity. Because so many different brands of cameras and software utilize similar video protocols, an unsatisfactory or defective camera can be replaced with a different model. Blue Iris recognizes hundreds of cameras, and likewise, other software recording systems are available. Again, owing to the fact that IP camera technology is relatively standardized, it is conceivable that a third-party vendor, perhaps one which is HIPAA compliant, may be able to offer video storage services using existing cameras; in other words, if a training program starts with Model #3 in Table 1, there might be an option to transition to Model #4 later (though of course this should be investigated beforehand). Finally, the LAN network itself is a standardized technology that local tech support staff will be adept at installing and maintaining.

Limitations

The camera tests were not exhaustive. Some features tested may only have limited use in a training clinic. For example, some cameras were equipped with an internal micro-SD slot for "cyclic" recording (recording in one-minute segments and erasing the oldest video as the card becomes full). This feature seems more useful for security use than for recording counseling interviews, but should be noted as the card slot should be physically secured (perhaps covered by adhesive) to discourage unauthorized use. Some cameras had a two-way intercom feature requiring an external speaker; this was not tested. The motorized PTZ of Cameras 1 and 2 seemed adequate; however, it could be at risk of failure over time because it is a mechanical system. On the other hand, those cameras' wide-angle lenses captured most of a room, reducing the need for PTZ adjustments. Some models' WLAN connections were erratic; a working installation ideally should use the wired LAN network instead. Finally, other promising technologies were not described here. For example, a network-attached storage (NAS) device is a small box that plugs into the LAN network and acts as a file sharing server, sort of a home-consumer alternative to Windows network file sharing. An older model NAS was tested in a separate project; it offered very good security features, but its file transfer speed was unsatisfactory. (Newer units might offer better performance.) These devices seem interesting, but satisfactory storage approaches already exist.

Unboxing the Recording System

The most cost-effective approach for building a system would begin with a pilot test using one camera. First, obtain a university computer as the control server. The IT staff then would connect the computer to a separate segment of the LAN network (which might require some additional hardware). Then, purchase a camera and install it on that network, such that it is isolated from the Internet. Blue Iris can be downloaded free for a 14-day evaluation, and this should be sufficient to determine if the system—camera,

network, and control server—will work together adequately in the counseling training area. The last step would be to test different storage approaches.

If the pilot is successful, the expanded configuration which supports the best access safeguards would be to designate a locked "control room" containing one computer workstation per camera (for example using Blue Iris LE, a "light" version that supports one camera). The counseling session could be recorded to the students' encrypted Flash drive (Model #5 in Table 1), or to FileSpace (Model #3); watched live on that computer; or streamed using Blue Iris' password-protected video server, for example to a tablet/mobile device. Optionally, a faculty member or "super" observer with a need to access to monitor several sessions could use a laptop or computer with the Blue Iris full version, which can observe multiple cameras simultaneously (Model #3 in Table 1). The more sessions viewed, the more important the computer specifications will be; the Blue Iris Web page does specify minimum hardware requirements.

Integration

Reasonable steps toward security will require that the components (cameras, control server, and network) be integrated thoughtfully. Although the HIPAA law does not apply to graduate counseling classes doing training exercises, HIPAA does map out the areas that are generally important to security. Administrative safeguards could be an agreement that students will not attempt to access certain settings on the cameras or software. Physical safeguards include locating the server and any viewing stations in an area restricted by lock and key. Technological safeguards include adding strong passwords to the cameras, making use of other security features provided by the LAN network controller (e.g., firewall, MAC address restriction) to protect data in transmission. HHS (2006) also identifies storage as a separate concern. If the number of trainees is low, the most secure storage approach resembles Model #3 in Table 1. An IT technician can create securely-shared folders on the institutional network, which can be accessed only by computers which are part of that network and which supply the correct password. Trainees can be required to only use designated university computers for viewing the recordings. On the other hand, if the number of trainees is high, it may be more practical for students to manage their own recordings, as in Model #4 in Table 1. This would require additional safeguards. Baker and Delgado (2014) extensively tested the open-source TrueCrypt software as a means of encrypting flash drives used for storing counseling videos, but TrueCrypt is no longer in development; instead, Windows Bitlocker should be used, on those versions of Windows that support it, or full-drive encryption on the Mac. Baker and Delgado also evaluated encrypted Flash drives, such as IronKey (which will work on a PC or Mac) or Aegis Apricorn (which will work on a standalone analog-to-digital encoder). Trainees who are responsible for maintaining the security of the video recording should follow other recommendations by Baker (2012) such as installing anti-virus software and disabling the file cache of their media player. Also, discuss what will be done if a device containing a video file is lost or stolen, even if it is encrypted. Who will notify the client and how? In many cases, university programs may not be able to follow the structured notification procedures required by HIPAA, but still can act ethically and responsively to clients' privacy and awareness needs.

Finally, HIPAA requires assessment of relative risks (HHS, 2006). While the video recording technology demands careful attention, it may not pose the single highest risk to client privacy. An eavesdropper in the next room, or on the other end of a ventilation duct, could intercept counseling conversations, and Baker and Delgado (2014) identified security threats associated with computer and smartphone viruses. Trainees could take such reasonable precautions as simply asking clients to store cell phones and electronic devices in book bags or coats.

Conclusion

The need for counselor trainees to record their interview videos is a constant. The security of video recording depends on institutional or administrative safeguards, physical safeguards, and technological safeguards. This document describes a demonstration of IP camera recording technologies, a single component in the process, with attention to reliability and security issues. Development of any new system should take place along lines inspired by the HIPAA law and informed by a thorough examination of the American Counseling Association Code of Ethics.

References

Baker, T. D. (2012). Digital confidentiality: A holistic security model for counselors. *VISTAS 2012*. Retrieved from http://www.counseling.org/docs/default-source/vistas/vistas_2012_article_39.pdf?sfvrsn=7

Baker, T. D., & Delgado, J. (2014). The ACA 2014 code of ethics and technology: New solutions to emerging problems. *VISTAS 2014*. Retrieved from http://www.counseling.org/docs/default-source/vistas/article_55.pdf?sfvrsn=6

Council for Accreditation for Counseling and Related Educational Programs. (2009). *2009 standards*. Retrieved from http://www.cacrep.org/wp-content/uploads/2013/12/2009-Standards.pdf

Quinn, L. S. (2009). *In search of HIPAA-compliant software.* Retrieved from http://www.idealware.org/articles/search-hipaa-compliant-software

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

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. I. (2008). *NIST special publication 800-66 revision 1: An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule.* Gaithersburg, MD: U.S. Department of Commerce.

U.S. Department of Health and Human Services. (2006). *HIPAA Security guidance.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

U.S. Department of Health and Human Services. (2007). *Is a software vendor a business associate of a covered entity?* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/256.html

U.S. Department of Health and Human Services. (2009). *Summary of the HIPAA Security Rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

U.S. Department of Health and Human Services. (2010). *Are we required to "certify" our organization's compliance with the standards of the Security Rule?* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2003.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://www.counseling.org/knowledge-center/vistas