Professional Psychology: Research and Practice
2015, Vol. 46, No. 3, 154–160

0735-7028/15/$12.00 http://dx.doi.org/10.1037/pro0000018

Emerging Ethical Threats to Client Privacy in Cloud Communication and Data Storage

Samuel D. Lustgarten
University of Iowa

In June 2013, Edward Snowden released top-secret intelligence documents that detailed a domestic U.S. spying apparatus. This article reviews and contends that current APA ethics and record-keeping guidelines, the Health Insurance Portability and Accountability Act, and the Health Information Technology for Economic and Clinical Health Act do not adequately account for this new information and other emerging threats to client confidentiality. As psychologists bear the responsibility for being informed, protecting and maintaining client records, and preventing breaches, it is vital that the field establish specific best practices and present regular security updates to colleagues.

Keywords: privacy, confidentiality, risk management, NSA, cloud storage

> The NSA has built an infrastructure that allows it to intercept almost everything . . . . I can get your emails, passwords, phone records, credit cards.
>
> —Edward Snowden (MacAskill, 2013)

Psychologists have asserted that confidentiality is needed to develop therapeutic alliances with clients (Donner, VandeCreek, Gonsiorek, & Fisher, 2008; Fisher, 2008; Glosoff, Herlihy, Herlihy, & Spence. 1997). Likewise, clients rely on confidentiality and privacy when sharing personal concerns (Rubanowitz, 1987; VandeCreek, Miars, & Herzog, 1987). In 1996, psychotherapist–patient privilege was strengthened by the U.S. Supreme Court case and judicial interpretation of *Jaffee v. Redmond* (1996). The Court ruled in favor of client confidentiality and protections against being legally compelled to disclose most records. Without this privilege, it is unclear whether clients would feel comfortable talking to mental health practitioners.

Because of the inherent risks associated with disclosing private information to another individual, the American Psychological Association (APA) included components within its "Ethical Principles of Psychologists and Code of Conduct" (APA, 2010; hereafter referred to as *Ethics Code*) and "Record Keeping Guidelines" (APA, 2007) aiming to minimize accidental or targeted disclosures of confidential information. Both documents place the ethical responsibility for protecting client data with practitioners.

These obligations come at a time of vast technological progress. Record keeping has largely moved from paper-and-pen methods to electronic medical records (EMRs; Devereaux & Gottlieb, 2012). Clinicians are increasingly using text messaging (Norcross, Pfund, & Prochaska, 2013) and e-mail (Shapiro & Schulman, 1996) for extended client care. In the interest of maintaining records and providing digital backups, many practitioners have moved to digital solutions. Each shift in technology has tested practitioners, who are tasked with maintaining record and communication security.

Unfortunately, new technology threatens practitioners' abilities to adequately maintain client privacy. In June 2013, information provided to Glenn Greenwald by the whistleblower Edward Snowden outlined numerous U.S. governmental surveillance capabilities to access information on cloud storage centers (Gellman & Soltani, 2013; Greenwald, 2013). Leaked information suggested that the National Security Agency (NSA) was capable of accessing Google's entire cloud platform (i.e., Gmail, Calendar, and Drive; Gellman & Soltani, 2013). If a practitioner stored any protected health information (PHI), mentioned identifiable cases, and/or contacted a client through these servers, the government could have accessed and downloaded that information.

The 21st century is one of technological growth and increasing vulnerability of client privacy. Recent news suggests that the landscape for data protection is changing, which necessitates ethical considerations and precautions. This article presents current record-keeping and communication regulations and guidelines, emerging threats to client data, and ethical considerations and advocates for the foundation of best practices.

From Pen to Keyboard: Evolving Regulations and Guidelines

In 1965, Gordon Moore, cofounder of Intel Corporation, outlined a theory for technological growth that successfully predicted the rise of household computers. This was at a time when computers filled rooms. Moore (1965) predicted that circuit technology would double every 2 years and lead to exponential growth while reducing the size of everything. This became known as *Moore's law*. Since then, personal computers have become commonplace, and smartphones are increasingly gaining market share. Devices

This article was published Online First April 27, 2015.

Samuel D. Lustgarten received his BS in psychology from Colorado State University and is currently completing a PhD in counseling psychology in the Department of Psychological and Quantitative Foundations at the University of Iowa. His research focuses on suicide prevention, client privacy, and technology.

Thanks are due to Elizabeth Altmaier, Daniel Elchert, and Micah Lee.

Correspondence concerning this article should be addressed to Samuel D. Lustgarten, Department of Psychological and Quantitative Foundations, University of Iowa, 361 Lindquist Center, Iowa City, IA, 52242-1529. E-mail: Samuel-Lustgarten@uiowa.edu

are smaller and more powerful than ever. Further exemplifying this trend, 2.7 billion people had access to the Internet in 2013 (International Telecommunication Union, 2013).

This pervasive accessibility and evolution of technology affects both practitioners and clients. Today, it is as simple as a text message or e-mail to communicate with a client. Record keeping can be entirely network based and digital. Devereaux and Gottlieb (2012) posited that all record keeping would eventually be digital. Although some groups do not embrace changes in the direction of digital records (Richards, 2009), evidence suggests growing interest in, and the possibility of reduced medical errors when using, EMRs (Institute of Medicine, 1999), Harrison and Palacio (2006) added evidence that organizations such as the Department of Veterans Affairs and Kaiser Permanente were benefiting in patient encounters with universal, real-time information. Richards (2009) found that EMRs were associated with increased screening, counseling, medication use, and management of risk.

With each evolution toward more digital services, organizations and governments have contributed to the protection of clients' welfare. Federal regulations have been created to aid in the development, use, and protection of confidential data and communications. Likewise, APA released information for record-keeping guidelines. The following two sections outline some of these changes.

Health Insurance Portability and Accountability Act (HIPAA), Security Rule, and Health Information Technology for Economic and Clinical Health (HITECH) Act

The method, medium, and content for writing and storing notes shifted in the 21st century. Simple pen-and-paper methods moved to electronic ones. Physical file cabinets became encrypted digital containers. These technological advances prompted U.S. agencies to provide legislative frameworks for the proper handling of information. Demand for transmission and portability of electronic records prompted a cooperative effort between government, providers, insurers, and payment providers.

The Health Insurance Portability and Accountability Act (1996; HIPAA) aimed to increase accessibility of medical records while maintaining confidentiality. The framers intended it to "simplify the administration of health insurance" (HIPAA, 1996). HIPAA also contained expectations for practitioners and health providers with regard to electronic health information. The act stated that providers must "maintain reasonable and appropriate administrative, technical, and physical safeguards" (HIPAA, 1996).

In 1998, the Department of Health and Human Services (HHS) proposed specific security rules to aid in the regulation and maintenance of PHI (HHS, 1998). HIPAA-related materials would then be required to be shared privately. HHS (2003) provided a "final rule" for the security standards in 2003. These security rules apply to a health plan, health care clearinghouse, and any health care provider (e.g., psychologists who transmit PHI electronically; HHS, 2013). The security standards mandate that any providers of these services take security precautions to prevent a breach of data and that they conduct risk analyses. In addition, these regulations apply to business associates. This term of art requires those in cooperation with health plans, clearinghouses, and providers to maintain the same security standards that are appropriate for an entity and PHI. For example, a practicing psychologist who operates with insurers would need to follow HIPAA's privacy and security rules while ensuring that business associates also operated within the legal framework.

HIPAA helped to provide a framework for business associates and third-party businesses to serve as electronic transfer agents for the storage of PHI. But the Health Information Technology for Economic and Clinical Health Act (2009; HITECH) formalized business associate liability, offered stricter regulations for the use of client records, and it further aided in client access rights. HITECH (2009) placed the burden of security on a business associate to meet security and privacy requirements. In addition, business associates are expected to provide breach notifications to covered entities and are subject to civil and criminal penalties for the misuse and/or loss of data. This act codified the legal regulatory authority to prevent data loss and punish corporate service providers. For instance, if a practitioner decided to sign a business agreement with a business associate to store client records or materials in a cloud environment, said business associate would need to meet HITECH requirements.

APA's Record-Keeping Guidelines

The APA (2010) Ethics Code provides ethical principles and standards but does not specify exact record-keeping guidelines; instead, these were provided in a different publication (APA, 2007). The Ethics Code (APA, 2010) distinguishes principles as guidelines for conduct, whereas standards may inform judicial proceedings. APA's formal "Record Keeping Guidelines" document establishes guidelines to protect clients and practitioners in legal and ethical proceedings. This document highlights the many interactions that practitioners have with the greater health care system and federal regulations (i.e., HIPAA). Of interest in the present study are Guidelines 3, 6, and 9 (of 13). Each of these guidelines converges on the topic of security, privacy, and confidentiality. Guideline 3 deals with confidentiality of created client records. This guideline echoes much of the Ethics Code's requirements and asserts that practitioners should be aware of current regulatory and legal requirements that hold regarding records. Guideline 6 outlines the security that psychologists should engage in to protect said records. If practitioners create physical records, they should protect them with key and cabinet. Should digital records be used, practitioners are expected to properly secure them. Drogin, Connell, Foote, and Sturm (2010) pointed out that if practitioners use personal mobile devices to communicate, PHI might be accessible. Lastly, Guideline 9 informs practitioners regarding the use of electronic records. APA analogizes electronic to physical records, adding that practitioners should be concerned with the use of e-mail and other communication tools because they may suffer from confidentiality concerns. These guidelines are not enforceable; rather, they were formulated to provide guidance to practitioners.

Together, federal regulations and APA record-keeping guidelines provide a framework within which to understand the movement to digitized records and communication. Unfortunately, neither federal regulations nor APA have proffered specific steps that should be taken to increase privacy and confidentiality. The current guidelines only state that practitioners should use "passwords, firewalls, data encryption and authentication" (APA, 2007, p. 998).

Although these recommendations would better secure systems, they do not establish directions and specific methods for creating secure passwords, activating firewalls, or using data-encryption techniques, and they do not explain what authentication protocols are. Providing specific guidelines that are constructed and updated regularly might alleviate part of the burden on practitioners to prepare for and understand growing threats to client privacy.

Individual, Corporate, and Governmental Threats to Client Privacy

In a poll of 70 psychotherapy experts, many participants expressed increased interest in smartphone applications and social networking interventions (Norcross et al., 2013). Similarly, practitioners appear to see telemental health therapy (TMHT) as a potential intervention and therapeutic delivery method in the future (Colbow, 2013). As psychologists choose to accommodate communications outside of sessions (i.e., via e-mail and text messages) and write notes in EMRs (using local, network, and/or cloud storage), the risk to client privacy increases (Drogin et al., 2010; Richards, 2009).

Regrettably, advances frequently test practitioners' abilities to meet the principles and standards outlined in the Ethics Code. As practitioners increasingly embrace the movement to cloud-based communication and storage, the growing threats to confidentiality should be considered. Technological advances in record keeping and communication bring costs and benefits to client confidentiality. As Benefield, Ashkanazi, and Rozensky (2006) surmised, these advances are also open to new attacks on clients' data. The following sections outline a few of the risks associated with individual, corporate, and governmental actors.

Individual

Individual and collective actors can threaten client confidentiality. On September 1, 2014, *The Guardian* reported that an individual or small group of people "exploited" celebrity Apple iCloud accounts, which stored phone data including e-mails, address books, and photos (Arthur, 2014). Although celebrity data were the main targets, hackers could have compromised individuals' accounts using similar methods. Again, if a practitioner had chosen to communicate or store any records on Apple's iCloud platform, that information could have been compromised.

Information that is stolen via digital storage services and private information is frequently available. In the "dark Web"—hidden Web sites that are inaccessible to most Internet users—this information is regularly sold. This portion of the Internet is not accessible via Google or traditional browsers (Thompson, 2014). CNBC's Cadie Thompson (2014) highlighted some common prices for private identity information. If psychologists communicate with a client via smartphones and similar devices, those communications could be compromised with mobile malware for about $150. Similarly, some medical records can be purchased for about $50.

Corporate

Companies that provide cloud storage, e-mail, and communications services generally make money from mining personal data. Their privacy policies and terms of services can be inherently complex. This can place a significant burden to understand and verify the safety of certain corporations on the practitioner. Facebook uses social profiles for marketing purposes and to provide users with related information (Facebook, Inc., 2014). Google (2014c) and Yahoo Inc. (2014), common e-mail and cloud storage providers, both have expansive privacy policies to enable them to provide "relevant" advertising and learn about user habits. Across these platforms, PHI may be communicated, at which point the corporate entity would have knowledge of client contact. Certain companies provide stronger privacy policies for communication. For example, Apple's iCloud service encrypts e-mails in transfer (Apple Inc., 2014a) and does not mine for content (Apple Inc., 2014c). Shapiro and Schulman (1996) critiqued e-mail-based mental health services, which suggested that questions and help would be provided privately. E-mails are not traditionally encrypted at rest (on cloud servers), nor are their texts encrypted (Apple Inc., 2014a); however, leading e-mail providers (e.g., Google, Yahoo, Apple's iCloud) encrypt messages in transit.

Unfortunately, on top of data-mining practices, most cloud storage and communication providers do not provide adequate information about data-retention policies. Google's Drive cloud storage service for personal users (not Google Apps) offers no specific data-retention policy (Google, 2014c). This amorphous data-retention policy stands in contrast to APA's (2007) record-keeping guidelines, which suggest that client records and data may be destroyed after 7 years in the absence of superseding legal requirements. It also calls into question a practitioner's ability to maintain and provide confidentiality and proper informed consent when using certain corporate providers. Moreover, it is questionable whether practitioners could ever believe that records had been deleted if the cloud provider did not clearly and publicly state its data-retention standards.

Governmental

There are a variety of governmental actors and organizations that interact with client data. In June 2013, journalist Glenn Greenwald collaborated with NSA whistleblower Snowden to publish the first article of "The NSA Files" (Greenwald, 2013). This collection of intelligence reports, briefings, and presentations catalogued a covert surveillance apparatus (Greenwald, 2014). Leaked reports told of a specific program—*MUSCULAR*—that enabled NSA analysts to have access to private cloud data centers from Google and Yahoo (Gellman & Soltani, 2013). Any user of Gmail, Google Drive, or various other cloud products was affected by the attack as the NSA found a weak point in international operations. The ramifications of these technological abilities affect various professionals, from lawyers to nurses to mental health practitioners, because PHI and client data may not be completely protected. Cloud storage centers are vulnerable to NSA analysts and nongovernmental actors.

Public universities generally provide e-mail addresses to every faculty member and student. These addresses provide a common method for communication while individuals are at the school. Many college counseling centers operate on campuses of public institutions, which are held accountable to state and federal statutes. Although counselor contact e-mails are considered confidential communications at my public institution, anybody can request

the e-mails of university staff members (University of Iowa, 2013) through a Freedom of Information Act (1966) request (FOIA; 5 U.S. Code § 552). Because universities and colleges differ in their policies, it is important to understand whether a respective institution would defend against open access to communication. Unfortunately, e-mail-based consultations between providers (that do not contain PHI) might not be as protected as messages conveyed through patient files and EMRs.

The Stored Communications Act (1986) was created before the Internet, e-mail, and personal computers were common household items. In particular, it asserted that e-mail left on Web servers for over 180 days would be considered abandoned. Today, this law is still in effect, and "abandoned" data can be requested without formal judicial review. People no longer delete e-mails as regularly as they used to, opting to archive and save them for later use (Google, 2014a). Legally, subpoenas and prior notice are required to search e-mails. For communications that have been left on cloud storage providers over 180 days, the Stored Communications Act may limit confidentiality.

In placing communications in the cloud for storage, one may be seriously compromising one's ability to prevent government access. Beyond general attack measures that the NSA engages in, the Federal Bureau of Investigation is permitted to investigate in certain situations without first notifying the person under investigation (Counterintelligence Access to Telephone Toll and Transactional Records, 2012). Therefore, despite a practitioner's responsibility to tell a client about limits to confidentiality, these investigations hamper positive efforts toward informed consent. Colloquially, these are known as "national security letters," and they may conflict with the current APA (2010) Ethics Code.

Ethical Concerns

The APA (2010) Ethics Code outlines a variety of principles and standards for practitioners and researchers. As Glosoff et al. (1997) suggested, psychologists have "fundamental ethical obligations" to defend client confidentiality. Various principles and standards are being imperiled by today's threats to electronic storage and communications. Unfortunately, practitioners might be at greater risk than they understand. Even APA (2007) noted that technological advances, including electronic record keeping, test practitioners' abilities to maintain security. Considering these emerging concerns, this section focuses Principle E and Sections 2, 4, 6, and 10 of the Ethics Code.

In the creation and management of client records, Principle E (Respect for People's Rights and Dignity) provides a foundation for privacy and confidentiality (APA, 2010). This principle recognizes the necessity of protecting these rights and the welfare afforded to those who trust providers. Principle E informs much of the subsequent standards to follow. Because of emerging threats to privacy, client data may currently be underprotected, regardless of current policies.

Section 2 focuses on ethical questions regarding competence (APA, 2010). Of specific interest are Standards 2.01 (Boundaries of Competence) and 2.03 (Maintaining Competence.) Standard 2.01 posits that psychologists must practice and provide services within their area of competence. Psychologists have an obligation to obtain training and/or support in areas that they are not familiar with, including technology. Shapiro and Schulman (1996) warned that accepting new technologies without critical, expert analysis might test practitioners' boundaries of competence. Similarly, Standard 2.03 outlines an expectation that psychologists will continue their educations. Taken together, Section 2 considerations suggest that practitioners, who operate within the bounds of HIPAA and/or may use electronic services for the storage and communication of client information, are expected to gain competence or support in using privacy and security tools. Ethically, it may also be expected that practitioners continue to read and be informed about the various threats to client data.

Standard 4 may be the most relevant to the issue at hand, because it explicitly outlines privacy and confidentiality expectations (APA, 2010). As this article's epigraph warns, digitalization of records and communications also provides greater threat to outside entities that may unlawfully infringe on client privacy and confidentiality. In turn, this threat primarily affects two standards: 4.01 (Maintaining Confidentiality) and 4.02 (Discussing the Limits of Confidentiality). For providers, the Ethics Code outlines a series of obligations regarding data, which involve the expectation of confidentiality regardless of medium. Much like Section 10.01 (Informed Consent to Therapy), Section 4.02 establishes an ethical obligation to explain how certain record-keeping and communication practices may limit confidentiality. When using text messaging and e-mail with a client, it might be ethically appropriate to talk about how these technologies may result in intrusions on privacy. In discussing the limits, it is important to consider the current threats to a client's privacy and how obtained information could be used against him or her. Practitioners should abstain from using less secure technologies (e.g., e-mail and text messaging) with higher-risk populations. However, psychologist-led discussions should facilitate evaluation of the appropriateness of certain disclosures on the basis of foreseeable client risk.

Section 6 specifies ethical obligations for record keeping and fees. The standard of interest is 6.02 (Maintenance, Dissemination, and Disposal of Confidential Records of Professional and Scientific Work). The Ethics Code (APA, 2010) explains that within any medium, record storage and creation must be kept confidential. Moreover, if a practitioner needs to use shared records (e.g., in hospital settings), he or she should minimize the use of PHI when possible to improve client privacy. Today's therapeutic interventions are performed in a variety of settings, and as technology becomes an important part of these, maintenance of confidentiality in record keeping comes into question.

Lastly, Section 10 deals specifically with concerns regarding therapy. According to Standard 10.01 (Informed Consent to Therapy), clients are to be informed of limits of confidentiality and communication methods available during treatment. Brendel and Bryan (2004) proposed talking about the services available in initial, informed consent meetings. For instance, should practitioners be interested in providing e-mail and text message accessibility, clients should be informed about these methods. Without a thorough informed consent process that covers these factors, client confidentiality cannot be properly founded (Everstine et al., 1980).

Best Practices

Inadequate client privacy/confidentiality standards may be met with disciplinary and monetary consequences (Benefield et al., 2006; Glosoff et al., 1997). Between the Ethics Code (APA, 2010)

and the "Record Keeping Guidelines" (APA, 2007), APA provides specific and enforceable standards and guidelines for the use of client data. Use of these documents may inform counseling and record keeping, but there are additional practices that should be considered to further prevent breaches of confidentiality. I now turn to how practitioners can proactively prevent privacy infractions and breaches and maintain client confidentiality in this increasingly technological time. The following are six best practices for practitioners.

1. Threat Models

In the interest of protecting client privacy, practitioners should develop a threat model to assess each client and his or her practice's associated risk (Barrows & Clayton, 1996; Lee, 2013). Threat models serve to protect against those who would likely compromise client and/or practitioner confidentiality (Barrows & Clayton, 1996). More specifically, threat models can reduce unlawful or accidental disclosures of PHI.

Although it is challenging to do so, an efficacious threat model should incorporate the various actors that may harm client confidentiality and group clients into low-risk, moderate-risk, and high-risk categories. With particularly high-risk populations (i.e., political dissidents, politicians, celebrities), low-tech methods may be advisable (i.e., pen-and-paper record keeping or air-gapped computers [detailed later], which have no Internet access capabilities, for notes).

The Electronic Frontier Foundation (2014) has suggested that threat models contain five questions: (a) What do you want to protect? (b) Who do you want to protect it from? (c) How likely is it that you will need to protect it? (d) How bad are the consequences if you fail? (e) How much trouble are you willing to go through to try to prevent those? Practitioners could, for instance, answer with the following five responses: (a) "I want to protect client records and communications." (b) "I want to protect it from unauthorized government access and individual hackers." (c) "I am currently working with public, political figure, who has expressed concerns regarding unauthorized disclosures and leaks of data." (d) "Considering the public nature of this client, my practice could be threatened and culpable for damages." (e) "I am willing to spend an additional hour per week to secure this individual's client records on an external, air-gapped computer." In general, the Ethics Code (APA, 2010) and the "Record Keeping Guidelines" (APA, 2007) emphasize stronger protections. By asking these five questions, practitioners can reduce accidental and/or targeted attacks on client information.

2. Encrypt Everything

If possible, every client record and communication should be encrypted. When mobile devices are used for client contact (i.e., text messages and/or e-mails), it is important to consider the phone's encryption capabilities. Currently, iPhones, with a good password, can be encrypted and protected from password attacks for about 5.5 years (Apple Inc., 2014b). It is also possible for iPhones to encrypt iMessages (text messages between iPhones), which would only be accessible between sender and recipient. Older phones cannot generally engage in encrypted messaging.

The APA Practice Organization (2014) separated computer encryption into three parts: (a) full-disk encryption, (b) virtual-disk encryption, and (c) file/folder encryption. Full-disk encryption provides protection for an entire system, but once a password is used, the entire file system is accessible. Virtual-disk encryption is an encrypted container that acts like a digital flash drive and is protected from access through encryption. These containers require a password after logging into the computer. The last file system encryption option regards individual files. For instance, a Microsoft Office Word file can be password protected. Through a combination of all three of these methods, a stolen computer would be protected at multiple levels and virtually inaccessible.

The chief technology officer of the Freedom of the Press Foundation and technologist for *The Intercept* suggests disk encryption, firewalls, strong passwords (never renew or use the same), and cryptology to communicate when possible (M. Lee, personal communication, September 28, 2014). For example, Apple computers come with built-in full-disk encryption via FileVault. In addition, by using a strong, 8–10 character password with special symbols, varied capitalization, and avoidance of dictionary words, practitioners can have an encrypted and well-protected computer.

3. HIPAA-Compliant Cloud Providers

Any provider of storage for PHI should publicly document their privacy policy, terms of service, and information-handling restrictions. For instance, Google Apps uses various standardized security certificates to ensure data safety and retention (Google, 2014b). Even if practitioners choose to be responsible and HIPAA compliant, files should still be encrypted as per Best Practice 2. Devereaux and Gottlieb (2012) recommended that if cloud providers encrypt data, this process should meet the need for "reasonable conduct" and protection of records. This argument is predicated on trust. A cloud provider that encrypts data but still has access to encryption keys would be forced to decrypt this information if compelled by the federal government. Likewise, if a private employee or contractor was given the signing key, they could potentially decrypt data unlawfully. Any cloud storage used should already be backed up locally and completely encrypted prior to upload. There are a variety of encryption software packages available; an example, cross-platform option is TrueCrypt.

4. Two-Factor Authentication

This method of authentication requires psychologists to first enter a password and then a special token (Google, 2014a). Two-factor authentication uses a six-digit, time-based token that is automatically encrypted, which prevents access to cloud-based accounts. These tokens typically change at 30-s intervals. If a password were lost or stolen, an attacker would still need access to the token to login. Without the token, the stolen password would be of no use. Mobile devices can often receive two-factor tokens via text message. Google (2014d), Dropbox (Louie, 2014), and Twitter Inc. (2013) are all examples of companies that afford users the ability to activate two-factor authentication.

5. Air-Gapped Computers

With the most sensitive cases and clients, greater data protection may be necessary. Similar to locked and local file cabinets, an air-gapped computer provides separation from networked data

(Electronic Frontier Foundation, 2014). Such a computer is partitioned from Internet access—Ethernet cables and Wi-Fi antennas are disabled and potentially removed. In fact, the NSA (2010) has recommended that Apple/Mac users disable Bluetooth and AirPort devices by having "an Apple-certified technician remove [them]." This would likely necessitate the purchase of a separate computer, which stays permanently disconnected from the Internet and only provides access to files. Client notes and communication details would need to be manually moved via USB-based external drives to share files with another computer, thus lessening the risk of data leaks. The use of air-gapped computers should only be considered with the most sensitive client populations as data loss (e.g., through a failed hard drive) is more likely.

6. Modify Informed Consent

Informed consent should incorporate a method for securing, protecting, and handling data (APA, 2010). As Devereaux and Gottlieb (2012) suggested, it is important that an informed consent document properly explain, justify, and present accurate risks to data storage and communication. Should an expectation for phone, text, and/or e-mail communication be established, it is important to inform clients of the increased risk and methods for reducing leaks. In the interest of client privacy and autonomy, it may be appropriate to suggest pen and paper if worries about privacy concerns are present.

Conclusions

The 21st century has brought with it significant increases in technology and advances in accessibility. More than ever, practitioners are considering digital means for client records and communication. As mentioned, this field shows interest in TMHT (Colbow, 2013; Zur, 2012), which compels clients and practitioners to secure devices, read privacy policies, and maintain confidentiality.

This movement to embrace technological advances has been met with severe, emerging threats. Individual hackers have more power than ever to buy and sell private information, corporate entities are scanning data by default for advertising and marketing purposes, and governmental actors are collecting massive amounts of data (even when protected) for further analysis. With each step, important ethical obligations have been threatened.

There are consequences to every data-storage and communication decision. Paper, physical records at a local site could be broken into and/or damaged during a disaster. Cloud communications and storage do not carry this threat, but outside entities beyond local concerns could potentially access such files. After considering some of the NSA revelations to date, it is vital to approach all cloud-based client work with caution. By following best practices, practitioners can significantly reduce the chance of breaches. At a time when programs such as MUSCULAR threaten data stored in "secured" locations, psychologists should consider the appropriateness of current informed consent practices within the United States. Moreover, practitioners should question whether electronic-transmission surveillance laws are compatible with this field's support for privacy.

Baker and Bufka (2011) acknowledged that health care providers are increasingly entering a digital world in which legal and ethical concerns are vague, suggesting that there is "a lack of uniformity and clear guidance" (p. 405). Ultimately, although individual practitioners should and do bear the ultimate responsibility for confidentiality and privacy, a unified message from APA might help and prevent data storage and communication concerns resulting from poor and/or naïve risk management. Although the APA (2010) Ethics Code and "Record Keeping Guidelines" (APA, 2007) place the responsibility for client confidentiality—in any medium—with practitioners, it is important that an organization provide constant, up-to-date guidance for members. Future record-keeping guidance would likely benefit greatly from the inclusion of best practices. In addition, APA should consider appointing privacy officers—much as health care organizations have—who can disseminate security and privacy updates. Future work should explore the addition of this position, but such a consideration goes beyond the scope of this article. Lastly, many practitioners work in agency settings that use shared EMRs and might not be able to use the suggested best practices. Individuals in these environments should consider talking to appointed privacy officers about their current best practices.

Moore's law spoke to an atmospheric rise in technology and predicted the personal computer movement. As a cofounder of Intel, Moore, in his work, catalyzed great advances. Psychologists should not fear these changes, but they should prepare for the unexpected. By synthesizing the various individual, corporate, and governmental actors that threaten client privacy, practitioners should have a newfound understanding and appreciation for security concerns.

References

American Psychological Association. (2007). Record keeping guidelines. *American Psychologist, 62,* 993–1004. http://dx.doi.org/10.1037/0003-066X.62.9.993

American Psychological Association. (2010). *Ethical principles of psychologists and code of conduct*. Washington, DC: Author. Retrieved from http://www.apa.org/ethics/code/principles.pdf

APA Practice Organization. (2014, Spring/Summer). ABCs and 123s of encryption. *Good Practice, Spring/Summer,* 10–18.

Apple Inc. (2014a). *iCloud security and privacy overview*. Retrieved from http://support.apple.com/kb/ht4865

Apple Inc. (2014b). *iOS security*. Retrieved from https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf

Arthur, C. (2014, September 1). Naked celebrity hack: Security experts focus on iCloud backup theory. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/sep/01/naked celebrity-hack-icloud-backup-jennifer-lawrence

Baker, D. C., & Bufka, L. F. (2011). Preparing for the telehealth world: Navigating legal, regulatory, reimbursement, and ethical issues in an electronic age. *Professional Psychology: Research and Practice, 42,* 405–411. http://dx.doi.org/10.1037/a0025037

Barrows, R. C., Jr., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association, 3,* 139–148. http://dx.doi.org/10.1136/jamia.1996.96236282

Benefield, H., Ashkanazi, G., & Rozensky, R. H. (2006). Communication and records: HIPPA issues when working in health care settings. *Professional Psychology: Research and Practice, 37,* 273–277. http://dx.doi.org/10.1037/0735-7028.37.3.273

Brendel, R. W., & Bryan, E. (2004). HIPAA for psychiatrists. *Harvard Review of Psychiatry, 12,* 177–183. http://dx.doi.org/10.1080/10673220490472436

Colbow, A. J. (2013). Looking to the future: Integrating telemental health therapy into psychologist training. *Training and Education in Professional Psychology, 7,* 155–165. http://dx.doi.org/10.1037/a0033454

Counterintelligence access to telephone toll and transactional records, 18 U.S. Code § 2709 (2002).

Department of Health and Human Services. (1998, August 12). Security and electronic signature standards; proposed rule. *Federal Register, 63,* 43242–43280.

Department of Health and Human Services. (2003, February 20). Health insurance reform: Security standards; final rule. *Federal Register, 68,* 8334–8381.

Department of Health and Human Services. (2013). *HIPAA administrative simplification*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa simplification-201303.pdf

Devereaux, R. L., & Gottlieb, M. C. (2012). Record keeping in the cloud: Ethical considerations. *Professional Psychology: Research and Practice, 43,* 627–632. http://dx.doi.org/10.1037/a0028268

Donner, M. B., VandeCreek, L., Gonsiorek, J. C., & Fisher, C. B. (2008). Balancing confidentiality: Protecting privacy and protecting the public. *Professional Psychology: Research and Practice, 39,* 369–376. http://dx.doi.org/10.1037/0735-7028.39.3.369

Drogin, E. Y., Connell, M., Foote, W. E., & Sturm, C. A. (2010). The American Psychological Association's revised "Record Keeping Guidelines": Implications for the practitioner. *Professional Psychology: Research and Practice, 41,* 236–243. http://dx.doi.org/10.1037/a0019001

Electronic Frontier Foundation. (2014). *Keeping your data safe*. Retrieved from https://ssd.eff.org/en/module/keeping-your-data-safe

Everstine, L., Everstine, D. S., Heymann, G. M., True, R. H., Frey, D. H., Johnson, H. G., & Seiden, R. H. (1980). Privacy and confidentiality in psychotherapy. *American Psychologist, 35,* 828–840. http://dx.doi.org/10.1037/0003-066X.35.9.828

Facebook, Inc. (2014). *Information we receive and how it is used*. Retrieved from https://www.facebook.com/about/privacy/your-info

Fisher, M. A. (2008). Protecting confidentiality rights: The need for an ethical practice model. *American Psychologist, 63,* 1–13. http://dx.doi.org/10.1037/0003-066X.63.1.1

Freedom of Information Act of 1966, 5 U.S. Code § 552 (1966).

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden says. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166 11e3-8b74-d89d714ca4dd_story.html

Glosoff, H. L., Herlihy, S. B., Herlihy, B., & Spence, E. B. (1997). Privileged communication in the psychologist–client relationship. *Professional Psychology: Research and Practice, 28,* 573–581. http://dx.doi.org/10.1037/0735-7028.28.6.573

Google. (2014a). *Archive messages*. Retrieved from https://support.google.com/mail/answer/6576?hl=en

Google. (2014b). *HIPAA compliance with Google Apps*. Retrieved from https://support.google.com/a/answer/3407054?hl=en

Google. (2014c). *Privacy policy*. Retrieved from https://www.google.com/policies/privacy/

Google. (2014d). *2-step verification*. Retrieved from https://www.google.com/landing/2step/

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/nsa phone-records-verizon-court-order

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Metropolitan Books.

Harrison, J. P., & Palacio, C. (2006). The role of clinical information systems in health care quality improvement. *The Health Care Manager, 25,* 206–212. http://dx.doi.org/10.1097/00126450-200607000-00003

Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111 5, 123 Stat. 226. (2009). *Retrieved from* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936. (1996). *Retrieved from* http://www.hhs.gov/ocr/hipaa

Institute of Medicine. (1999). *To err is human: Building a safer health system*. Retrieved from https://www.iom.edu/~/media/Files/Report%20Files/1999/To-Err-is-Human/To%20Err%20is%20Human%201999%20%20report%20brief.pdf

International Telecommunication Union. (2013). *ICT facts and figures*. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Jaffee v. Redmond, 518 U.S. 1 (1996).

Lee, M. (2013). *Encryption works: How to protect your privacy in the age of NSA surveillance*. Retrieved from https://freedom.press/sites/default/files/encryption_works.pdf

Louie, C. (2014, October 1). *Have you enabled two-step verification?* Retrieved from https://blog.dropbox.com/2014/10/have-you-enabled-two-step-verification/

MacAskill, E. (2013, June 10). Edward Snowden, NSA files source: 'If they want to get you, in time they will.' *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden why

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, 38,* 114–117. S0018-9219(98)00753-1

National Security Agency. (2010). *Hardening tips for Mac OS × 10.6 "Snow Leopard."* Retrieved from https://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

Norcross, J. C., Pfund, R. A., & Prochaska, J. O. (2013). Psychotherapy in 2022: A Delphi poll on its future. *Professional Psychology: Research and Practice, 44,* 363–370. http://dx.doi.org/10.1037/a0034633

Richards, M. M. (2009). Electronic medical records: Confidentiality issues in the time of HIPAA. *Professional Psychology: Research and Practice, 40,* 550–556. http://dx.doi.org/10.1037/a0016853

Rubanowitz, D. E. (1987). Public attitudes toward psychotherapy–client confidentiality. *Professional Psychology: Research and Practice, 18,* 613–618. http://dx.doi.org/10.1037/07357028.18.6.613

Shapiro, D. E., & Schulman, C. E. (1996). Ethical and legal issues in e-mail therapy. *Ethics & Behavior, 6,* 107–124. http://dx.doi.org/10.1207/s15327019eb0602_3

Stored Communications Act of 1986, 18 U.S. Code § 2703 (1986).

Thompson, C. (2014, October 3). *Selling stolen card info online? That's the least of it*. Retrieved from http://www.cnbc.com/id/102053257

Twitter Inc. (2013). *Getting started with login verification*. Retrieved from https://blog.twitter.com/2013/getting-started-with-login-verification

University of Iowa. (2013, September). *Acceptable use of information technology resources*. Retrieved from http://www.uiowa.edu/~our/opmanual/ii/19.htm

VandeCreek, L., Miars, R. D., & Herzog, C. E. (1987). Client anticipations and preferences for confidentiality of records. *Journal of Counseling Psychology, 34,* 62–67. http://dx.doi.org/10.1037/0022-0167.34.1.62

Yahoo Inc. (2014). *Yahoo privacy center: What this privacy policy covers*. Retrieved from https://info.yahoo.com/privacy/us/yahoo

Zur, O. (2012). Telepsychology or telementalhealth in the digital age: The future is here. *The California Psychologist, 45*(1), 13–15.

Received November 23, 2014
Revision received February 15, 2015
Accepted February 15, 2015 ■