New threats to client privacy

By Samuel D. Lustgarten

“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

Protecting clients’ privacy is clearly one of psychologists’ top ethical priorities. To help prevent disclosures of patient information, APA offers specific guidance in its Ethics Code (APA, 2010) and its “Record Keeping Guidelines” (APA, 2007).

Unfortunately, with today’s ever-evolving technology, such guidance may not be enough. As Edward Snowden showed the world in 2013, information on cloud storage centers is not secure (Gellman & Soltani, 2013; Greenwald, 2013).

This article gives an overview of the current record-keeping and communication regulations and guidelines, looks at new threats to client data, discusses the ethical considerations psychologists face, and advocates for the foundation of best practices to prevent breaches of client data.
Overview
CE credits: 1
Exam items: 10
Learning objectives: After completing this course participants will be able to:
1. Explain relevant guidelines and ethical standards affected by new technological threats.
2. Clarify differences between government, corporate and individual threats to client privacy and confidentiality.
3. Recognize potential methods to mitigate risk and unintended breaches of client records.

From pen to keyboard
In 1965, Intel Corporation co-founder Gordon Moore successfully predicted that circuit technology would double every two years and lead to exponential growth while reducing the size of everything. This became known as Moore’s law. Since then, personal computers and smartphones have become ubiquitous and nearly 3 billion people have Internet access. This pervasive accessibility affects both practitioners and clients. Today, communication with a client can occur via text and/or email. Metal file cabinets have evolved into encrypted digital containers. Record keeping can be entirely digital.

In response to this revolution, over the years U.S. agencies have sought to provide legislative frameworks for the proper handling of private information. Among them is the Health Insurance Portability and Accountability Act (1996, HIPAA), which sought to increase the accessibility of medical records while maintaining confidentiality. The law calls for HIPAA’s privacy and security rules and ensure that their business associates do so as well.

In 2009, The Health Information Technology for Economic and Clinical Health Act (HITECH) formalized business associates and offered stricter regulations for using client records. This law placed the burden of security on a business associate to meet security and privacy requirements. In addition, business associates are expected to provide notifications of any breaches to the entities they cover and are subject to civil and criminal penalties for the misuse and/or loss of data. Practitioners, this means if they sign a business agreement with a business associate to store client records or materials in a cloud environment, the associate must meet HITECH requirements.

APA’s record-keeping guidelines
While APA’s Ethics Code provides ethical principles and standards for psychologists, it does not provide specific record-keeping guidelines. That guidance comes from APA’s “Record Keeping Guidelines” (2007), which highlight the many interactions that practitioners have with the health-care system and federal regulations, such as HIPAA. For this article, we are particularly interested in guidelines 3, 6 and 9 (of 13), which focus on the topics of security, privacy and confidentiality:

Guideline 3 deals with confidentiality of client records. This guideline reminds us that practitioners should be aware of the regulatory and legal requirements that involve records.

Guideline 6 outlines the security measures that psychologists should engage in to protect those records. If practitioners create physical records, they should protect them with key and cabinet. If they use digital records, practitioners should properly secure them.

Guideline 9 informs practitioners on the use of electronic records. APA analogizes electronic to physical records and states that practitioners should be concerned with the use of e-mail and other communication tools because of the possibility that they can be seen by others.

These guidelines are not enforceable; they only offer guidance to practitioners.

Unfortunately, neither the federal government nor APA has proffered specific steps that should be taken to increase privacy and confidentiality to meet the challenges created by today’s technology. The current guidelines only state that practitioners should use “passwords, firewalls, data encryption and authentication” (APA, 2007, p. 998). Although privacy policies and recommendations would better secure systems, they do not establish directions and specific methods for creating secure passwords, activating firewalls or using data-encryption technologies, and they do not explain what authentication protocols are.

At a time when even data stored in “secured” locations is at risk, psychologists should consider the appropriateness of current informed consent practices within the United States.

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.

Threats to client privacy
Many psychologists are embracing email and text messaging to communicate outside of therapy sessions. Some, too, are writing notes in electronic medical records that rely on local, network and/or cloud storage. Others are interested in using smartphone applications and social networking interventions. And numerous practitioners see telehealth as a potential intervention and therapeutic delivery method (Colbow, 2013). All of these uses of technology increase the risk to client privacy. These risks include:

- Risks from individuals and collective actors: On Sept. 1, 2014, The Guardian reported that an individual or small group of hackers “exploited” celebrity Apple iCloud accounts, which stored phone data including emails, address books and photos (Arthur, 2014). Although celebrity data were the main targets, hackers could have compromised other individuals’ accounts using similar methods. If a practitioner had chosen to communicate or store any records on Apple’s iCloud platform, the information could have been compromised.

- Risks from companies: Companies that provide cloud storage, email and communications services generally make money from mining personal data. Their privacy policies and terms of service can be complex, which can place a significant burden on psychologists. For example, Facebook, like Google, uses social profiles for marketing and to provide users with related information. Facebook has expansive privacy policies to enable it to provide “relevant” advertising and learn about user habits. If a psychologist is communicating protected health information on these platforms, the corporate entity would have knowledge of client contact. Certain companies provide stronger privacy policies for communication. For instance, Apple’s iCloud service does not mine emails for content. Most providers do not encrypt emails at rest (on cloud servers), allowing companies to more easily hand over message contents to third parties (Apple Inc., 2014a).

Another concern is data retention. Most cloud storage and communication providers say little about how long they keep their data. This anamorphic data-retention policy stands in contrast to APA’s record-keeping guidelines, which suggest that client records and data may be destroyed after seven years in the absence of superseding legal requirements. This policy also calls into question a practitioner’s ability to maintain and provide confidentiality and proper informed consent when using certain corporate providers. And 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.

Risks from the government: A variety of governmental entities interact with client data. As Edward Snowden and journalist Glenn Greenwald revealed in 2013, NSA analysts were able to access private cloud data centers from Google and Yahoo (Gellman & Soltani, 2013), which could have compromised protected health information and other client data.

Email at public universities is also at risk. Anyone can request the emails of public university staff members through a Freedom of Information Act (1966) request. Although some universities and colleges defend against open access to communication, email-based consultations between providers (that do not contain protected health information) might not be as protected as messages conveyed through patient files and electronic medical records would be.

Client information may also be inadvertently compromised as a result of the Stored Communications Act (1986), which was created before the Internet, email and personal computers became the tools of everyday life. The laws that state emails held on Web servers for over 180 days is considered abandoned. That

Welcome to ‘CE Corner’
“CE Corner” is a continuing education article offered by the APA Office of CE in Psychology. This feature will provide you with updates on critical developments in psychology, drawn from peer-reviewed literature and written by leading psychologists.

To earn CE credit, after you read this article, purchase the online exam at www.apa.org/education/ce/1360395.aspx.

Upon successful completion of the test—a score of 75 percent or higher—you can immediately print your CE certificate. The test fee is $25 for members and $35 for nonmembers. The APA Office of CE in Psychology retains responsibility for the program. For more information, call (800) 374-2721.
Section 4.5.1.1: Consent for Record Keeping

The consent form should include a section that details the individual's rights concerning their records, such as the right to access, correct, or request the destruction of their data. The individual should also be informed about the circumstances under which their data may be accessed by others, such as law enforcement or healthcare providers.

Section 6.5: Services and Information

The services and information provided by the organization, such as treatment plans, should be clearly communicated to the individual. The form should include a statement that the information provided is for the purposes specified in the consent form.

Section 7: Access Rights

The individual should be informed about their right to access their records and the procedures for requesting such access. The form should include a statement that the individual has the right to receive a copy of their records in a readable format.

Section 8: Restrictions on Information Use

The form should include a statement that the individual's information will not be used for purposes other than those stated in the consent form. The form should also include a statement that the individual's information will be protected from unauthorized access.

Conclusion

In conclusion, the use of consent forms is essential for ensuring the privacy and confidentiality of individuals' data. By providing clear and comprehensive information about the collection, use, and protection of personal data, consent forms can help to build trust between healthcare providers and individuals.

References

- American Medical Association (2012). The health privacy act: A proposed federal law to protect personal health data.
- American Psychological Association (2013). Ethical principles of psychologists and code of conduct.
- American Psychological Association (2014). Ethical issues in research involving human participants.
- American Psychological Association (2015). Ethical principles of psychologists and code of conduct.
- American Psychological Association (2016). Ethical principles of psychologists.

This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
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. In addition, governmental actors are collecting massive amounts of data (even when protected) for further analysis. With each step, important ethical obligations have been threatened. As a result, 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 even data stored in “secured” locations is at risk, 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.

While individual practitioners should do the utmost responsibility for confidentiality and privacy, a unified message from APS might help prevent data storage and communication concerns resulting from poor and/or naïve risk management. Although APS Ethics Code and “Record Keeping Guidelines” 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. Psychologists should not fear technological changes, but they should prepare for the unexpected. By synthesizing the varying individual, corporate and governmental actors that threaten client privacy, practitioners should have a newfound understanding and appreciation for security concerns.

Samuel D. Lustgarten is a graduate student in the counseling psychology PhD program at the University of Iowa, Iowa City. His research centers on the intersection of technology, psychology and client privacy.

This is a condensed version of “Emerging ethical threats to client privacy in cloud communication and data storage,” which appeared in the June 2015 issue of the APA journal Professional Psychology: Research and Practice, Vol. 46(3). To read the full article, which includes all references, go to http://dx.doi.org/10.1037/pro0000018.