Psychological Services

In the public domain

2019, Vol. 16, No. 2, 281–285
http://dx.doi.org/10.1037/ser0000321

Mobile Applications for Client Use: Ethical and Legal Considerations

Amanda Edwards-Stewart
National Center for Telehealth and Technology, Tacoma, Washington

Cynthia Alexander
Washington State Attorney General's Office, Seattle, Washington

Christina M. Armstrong and Tim Hoyt
National Center for Telehealth and Technology, Tacoma, Washington

William O'Donohue
University of Nevada, Reno

Mobile applications (apps) to support behavioral health are increasing in number and are recommended frequently by medical providers in a variety of settings. As with the use of any adjunct tool in therapy, psychologists adopting new technologies in clinical practice must comply with relevant professional ethics codes and legal standards. However, emerging technologies can outpace regulations regarding their use, presenting novel ethical considerations. Therefore, it is incumbent upon providers to extrapolate current ethical standards and laws to new technologies before they recommend them as adjuncts to face-to-face treatment. This article identifies best practices for incorporating apps into treatment, including competence in the use of smartphones in general and familiarity with the specific apps recommended. Psychologists must conduct informed consent procedures in accordance with existing evidence, as well as privacy and security concerns relating to a particular app, in order to mitigate potential liability regarding the collection of client-generated data. Psychologists also should be prepared to educate clients about how best to safeguard their data, such as through encryption, password protection, or remote deletion of data. By doing so, psychologists can balance potentially competing demands of leveraging emerging technology to improve care while simultaneously ensuring ethical and legal compliance in these new areas.

Keywords: mobile apps, technology, APA ethics code, legal considerations

The use of mobile technology to support health care has significantly increased over the past decade, with the majority of mobile phone users having downloaded one of the hundreds of thousands of available health applications or "apps" (see Armstrong, Hoyt, Kinn, Ciulla, & Bush, 2017). Due to the widespread use of mobile technologies in clinical practice, psychologists must ensure that the use of this technology in client care is in accordance with established ethical principles and standards (Harris & Younggren, 2011). Indeed, Hall and McGraw (2014) suggest that existing legal requirements do not adequately cover the issues inherent in emerging technology, such as privacy and the transfer of data from mobile devices. Similarly, guidelines for the ethical use of technology in practice may not fully capture all potential scenarios, since the adoption of new technologies outpaces evaluation in the peer-reviewed literature (Armstrong et al., 2017). As a result, psychologists must exercise professional judgment in determining how to apply current ethical and legal practice standards to new clinical situations involving mobile technology (Joint Task Force for the Development of Telepsychology Guidelines for Psychologists, 2013).

Mobile apps are a category of software designed to run independently on mobile devices (including tablet computers, smartphones, and smart watches), frequently integrating multimedia and device capabilities such as connectivity to GPS sensors or motion tracking (Lui, Marcus, & Barry, 2017). These apps may also facilitate connection with social media platforms (Kolmes, 2012) or to external devices through Bluetooth technology that allows short-range exchange of data between a mobile phone and items such as wearable physiological sensors (Dillon, Kelly, Robertson, & Robertson, 2016). Joint Task Force for the Development of

This article was published Online First December 20, 2018.

Amanda Edwards-Stewart, Research Division, National Center for Telehealth and Technology, Tacoma, Washington; Cynthia Alexander, Consumer Protection Division, Washington State Attorney General's Office, Seattle, Washington; Christina M. Armstrong, Mobile Health Division, National Center for Telehealth and Technology; Tim Hoyt, National Center for Telehealth and Technology; William O'Donohue, Department of Psychology, University of Nevada, Reno.

Christina M. Armstrong and Tim Hoyt are now at the Connected Health Branch, Defense Health Agency, Tacoma, Washington.

The opinions or assertions contained herein are the private views of the authors and are not to be construed as official or reflecting the views of the U.S. Government, the Department of Defense, or the Defense Health Agency.

Correspondence concerning this article should be addressed to Amanda Edwards-Stewart, who is now at Research Production & Investigation, Psychological Health Center of Excellence, 9933 West Hayes Street, Joint Base Lewis-McChord, Tacoma, WA 98433. E-mail: amanda.e.stewart7.civ@mail.mil

Telepsychology Guidelines for Psychologists (2013) guidelines on the integration of technology into clinical care differentiate between two dimensions of service delivery related to mobile apps. First, the timing of a technology-facilitated clinical interaction can be either synchronous (such as real-time communication using video chat) or asynchronous (with data stored and accessed outside the session). Second, the provision of service can be either direct (involving ongoing treatment) or nondirect (such as an individual seeking information on a diagnosis outside a formal treatment setting). The scope of the current evaluation of ethical considerations will focus on a scenario in which a psychologist asks a client to download a mobile app on the client's personal mobile device as an adjunct to ongoing face-to-face treatment. This utilization of mobile apps would fall broadly into the category of asynchronous communication as an adjunct tool supporting direct service provision. Within this context, the current work evaluates several ethics standards identified through the authors' roles in conducting mobile health training workshops (see Armstrong, Ciulla, Edwards-Stewart, Hoyt, & Bush, in press).

APA Ethics Principles

Beneficence and Nonmaleficence

The principle of beneficence and nonmaleficence emphasizes that psychologists strive to ensure that their interventions provide benefit to the client while minimizing harm (American Psychological Association [APA], 2017). For emerging technologies, psychologists should strive to ensure that modifications of interventions to include digital technologies maintain equivalent outcomes to established treatment delivered without technology (Harris & Younggren, 2011). Intervention equivalence can be difficult to determine for new technologies, given that the emerging evidence base for mobile health adjuncts to treatment may lag behind adoption rates (Armstrong et al., 2017). In keeping with this principle, psychologists should inform clients about the degree of empirical support for using a particular mobile app as an adjunct to treatment (Epstein & Bequette, 2013; Karcher & Presser, 2018). This is supported in the ethics code (2.04 and 9.01) where "psychologists' work is based upon established scientific and professional knowledge of the discipline." Recent reviews differ on whether or not the empirical evidence base for the use of mobile technologies as an adjunct to face-to-face care is sufficient (e.g., Armstrong et al., 2017; Lui, Marcus, & Barry, 2017; Parker et al., 2018). A review of 21 studies on mobile apps in psychotherapy showed that treatments leveraging mobile apps were effective in reducing anxiety, depression, and substance use behaviors, with clinically meaningful effect sizes in the medium to large range (Lui et al., 2017). Other systematic reviews have shown evidence for the use of mobile apps as an adjunct to care for alcohol use disorders (Fowler, Holt, & Joshi, 2016) and smoking cessation (Ubhi et al., 2016). Nonetheless, the nascent literature on mobile apps is limited by a lack of comparison conditions in many studies, as well as allegiance effects when the app developer is also conducting research on its potential clinical effectiveness (Lui et al., 2017).

Justice

The code states that "psychologists recognize that fairness and justice entitle all persons to access to and benefit from the contributions of psychology" (APA, 2017, p. 4). The use of mobile apps to accompany treatment might be helpful to psychologists whose clients have significant barriers to care, such as a lack of childcare, distance from the clinic, cost, or lack of insurance (Luxton, Hansen, & Stanfill, 2014). Indeed, there are high rates of smartphone ownership in the United States, even among groups that previously experienced economic barriers to care (Pew Research Center, 2017). As an example, if a client were unable to come to weekly treatment sessions due to military duties or work schedule, then a mobile app could be used as an adjunct to treatment, facilitating assignments or assessments to increase engagement.

APA Ethics Standards

Standard 2.01e: Boundaries of Competence

To comply with APA ethical standards, psychologists must ensure their own competence with new methods prior to implementing them into treatment (APA, 2017). With any emerging technology, a psychologist should demonstrate competence with the specific service provided, as well as proficiency with the technology itself (Epstein & Bequette, 2013; Harris & Younggren, 2011). For example, knowing basic functionality of commonly used mobile devices (e.g., Apple and Android smartphones) can allow psychologists to help clients troubleshoot problems with mobile app utilization. "Test driving" a mobile app prior to recommending it is a best practice that also facilitates this troubleshooting with clients. Training on the integration of mobile apps into clinical care may emphasize familiarity with technology platforms and basic security protocols, in addition to the evidence base for mobile health (e.g., Armstrong et al., in press).

Competence and malpractice liability. The risk for malpractice liability based on lack of competence is an important legal consideration for psychologists (Gable, 1983). Using mobile apps in clinical care could theoretically present liability risks for a psychologist. Broadly, a health care provider owes a duty of care for purposes of malpractice liability only when a provider–client relationship is established (*Dehn v. Edgecombe,* 2003/2005). If a duty of care is established, the scope of the duty, which often is described as the standard of care, must be determined. The standard of care is based on the usual or expected practices of the profession, taking into account relevant statutes, case law, ethical codes, regulations (including those of licensing boards), and the consensus of the community (Harris & Younggren, 2011; Terry & Wiley, 2016). Although the precise wording of the standard of care may vary in different jurisdictions, standard of care is generally defined as the degree of skill and care that a competent provider engaged in a similar practice would provide while practicing under similar circumstances (Moffett & Moore, 2011).

At first glance, the standard of care seems to suggest that early adopters of new technologies or new interventions risk liability because others in their profession are not providing similar services (Terry & Wiley, 2016). One group of providers indicated that their primary liability concerns related to mobile health were the potential inability to respond in a timely manner to data generated on a mobile application, the inability to review the large amount of unstructured data generated by some mobile apps, and potential errors when relying on client-generated data that may be inaccurate (McGraw, Belfort, Pfister, & Ingargiola, 2013). Indeed, there is no clear standard of care in these areas, and no specific case law has yet addressed this issue in the context of utilizing mobile apps as an adjunct to psychotherapy (see Terry & Wiley, 2016; Yang & Silverman, 2014). In some states, courts apply a "respected minority" rule for evaluating a clinician's conduct. Under this rule, a clinician will not be found liable for using an emerging clinical technique that is used by a minority of respected practitioners in the field (Simon, 2005). As Terry and Wiley (2016) observe, concerns about malpractice liability can slow the adoption of innovative approaches. They note that "doing things 'the old way' can appear safer from a liability standpoint, but that is true only up to an ill-defined tipping point at which innovation becomes the prevailing standard of care" (Terry & Wiley, 2016, p. 80). Indeed, some of the only examples of lawsuits involving mobile health care applications have been related to unsubstantiated claims about the efficacy of the app (Cortez, 2014). Thus, the best approach to mitigate liability related to emerging technology is to set clear expectations upfront with clients, such as exactly which information will be shared via mobile app, when it will be reviewed with the provider, and exactly what provider–client relationship exists (McGraw et al., 2013). All of these items can be addressed through informed consent and explicating limits to confidentiality.

Standards 3.10: Informed Consent and 4.02: Limits to Confidentiality

Informed consent includes making a full disclosure to clients about the type of services being offered, the risks, and the potential benefits (Karcher & Presser, 2018). Failure to provide adequate informed consent can result in legal liability. In some states, a "reasonable provider" standard applies (Miller & Hutton, 2004, p. 452). In these states, the duty to disclose is similar to the duty of care. The provider is required to make the same disclosures as a competent provider in a similar practice in similar circumstances (*Coleman v. Garrison,* 1974/1975). Other states, however, apply a "reasonable patient" standard that requires disclosure of all information that a reasonable patient in the same position would consider when deciding whether or not to agree to treatment (*Canterbury v. Spence,* 1972; *Cobbs v. Grant,* 1972). In general, informed consent would require disclosure of the purpose of a mobile app, its risks and benefits, and alternatives to the proposed treatment (such as paper forms for mood tracking).

Informed consent also requires consideration of the possible limits to confidentiality associated with the use of a particular mobile app. Joint Task Force for the Development of Telepsychology Guidelines for Psychologists (2013) recommends informing clients of the confidentiality risks of stored health information when using telecommunication technologies, including mobile devices. Information on the data storage practices of a specific app often can be found by reviewing the developer's privacy statement, if available, or by reaching out directly to the developer. The informed consent process also should address how clients can safeguard their data from unintended disclosures. This often can be accomplished by password protecting either the device or the app itself (Epstein & Bequette, 2013; Karcher & Presser, 2018). Whereas early mobile apps were designed for health data to be viewed only by the primary user, more recent apps include the capability for sharing data via social networking sites and other venues (Lui et al., 2017). When using an app as an adjunct to treatment, the psychologist should be clear with the client what data can be shared and through what channels (e.g., social media, encrypted transmission, exported data files). If the client-generated data are being sent to the psychologist, the client should understand what parts of the data may or may not be included in the health record, how the data will be stored, and the process by which data will be reviewed by the psychologist (see McGraw et al., 2013). Psychologists also should consider the sensitivity of the stored data. Highly sensitive data such as trauma narratives recorded for prolonged exposure (Reger et al., 2017) would elicit a higher need for app privacy. Less sensitive health-related data, such as nutrition logs, may be of less concern for social sharing or unintended disclosure by the client.

Standard 4.01: Maintaining Confidentiality

To maintain confidentiality, a psychologist must take "reasonable precautions" to protect client information obtained through any means and stored in any form (APA, 2017). However, the majority of client-generated data on a mobile app remain on the device itself, unless transferred to the provider via e-mail or other data-sharing methods. Psychologists can help clients understand how best to protect their data by knowing the privacy and security settings associated with a particular mobile app. The client should be informed about whether data on the app are stored locally on the device and/or stored remotely online, such as in "the cloud." Psychologists also should be familiar with an app's privacy statement and terms of use to determine privacy concerns. For apps developed by the U.S. government, consumers usually can find detailed information about the products, some of which have user manuals. For mobile apps developed by U.S. government entities, the level of security is generally high because of stringent information technology security regulations (Armstrong et al., 2017). However, recent headlines on third-party data sharing highlight potential risk from commercially developed apps, with a significant number disclosing data to third parties (Blenner et al., 2016). Nonetheless, this is not dissimilar from face-to-face psychotherapy, wherein information commonly is shared with insurance companies and other third parties for commercial purposes.

Encryption and data breaches. To help a client ensure against breaches of confidentiality, psychologists should understand the principles and processes of data encryption. Mobile apps that include encryption for data "at rest" protect data on the mobile device (i.e., data not being transmitted) from being accessed by someone other than the user. Mobile apps that transmit data to remote servers or employ cloud-based storage need a higher level of security (data "in transit" encryption) to protect against unintended access. Bluetooth technology allows short-range exchange of data between a mobile phone and other devices, such as physiological sensors. Despite its widespread use, data transmitted via Bluetooth or other wireless means are more vulnerable to being intercepted than data that are encrypted in transit (Cifuentes, Beltrán, & Ramírez, 2015). Indeed, there has been a significant increase in "hacking" of mobile health care applications, particularly with health care apps on Android platforms (Arxan Technologies, 2014). Despite this potential for data breaches involving mobile data, the probability of such data breaches in this context is relatively low. Research shows that the majority of health care data breaches are due to data mishandling or physical access to a device containing client information, with less than 5% of breaches involving hacking a system vulnerability (Bennett, Bennett, & Griffiths, 2010; see Terry & Wiley, 2016, for related case law). In limited cases of hacking, the motivation for data breaches is generally a broader financial or political interest rather than targeting an individual's data (Holt, Freilich, & Chermak, 2017). Furthermore, health care apps focused on treatment support and medical information generally have shown fewer vulnerabilities, whereas apps that conduct remote monitoring show more vulnerabilities (Cifuentes et al., 2015). Overall, these risks can be mitigated through utilizing apps that include encryption and by the client taking steps to password-protect their devices and apps.

Relatedly, psychologists should understand app permissions in order to address potential client concerns. When downloading an app, the users might be asked to permit the app access to their phone's contacts, calendar, social media accounts, or other phone functionality (Chen, Gates, Li, & Proctor, 2015). These permissions generally relate to the functionality of the app and should be limited to the minimum necessary for these functions to operate. For example, the Virtual Hope Box (Bush et al., 2017) was developed to help clients in coping with distress through reminders of reasons for living. Its permissions include application access to the smartphone calendar, contacts, and photos. Calendar access allows the app to save positive activities in the client's phone calendar. Contact access allows the client to access an emergency contact list for times of distress. Camera access allows the client to personalize the app with photos of loved ones. By communicating these permissions to clients in an accessible manner, psychologists can allay concerns regarding the privacy of their data (Chen et al., 2015).

Lastly, if data collected in a mobile app are transmitted electronically to a provider, specific laws are applicable, including the Health Insurance Portability and Accountability Act (HIPAA, 1996), the HIPAA Privacy and Security Rule (2003), and the Health Information Technology for Economic and Clinical Health (HITECH) Act (2009). A health care provider is considered a covered entity by HIPAA only when the provider receives health information in connection with specific transactions listed in 45 C.F.R. 160.103, such as health care claims, coordination of benefits, enrollment in or eligibility for health plans, referral authorizations, or health plan premium payments. It is essential that a psychologist understands these guidelines if receiving data electronically from a client's mobile app.

Standards 6.01 and 6.02: Documentation and Disposal of Records

Client-generated data on the client's mobile device are not directly addressed in the legal standards discussed. Indeed, it would be difficult for psychologists to have full responsibility for these data without direct access. Nonetheless, psychologists can familiarize clients with techniques for protecting data in the event of a loss, such as if the client's device is stolen. The major mobile vendors all allow clients to wipe their data remotely. Apple enables this through iCloud login from any web-based device, and Google has a variety of apps that can be downloaded for remote tracking and disabling of a device (e.g., Android Device Manager). If a provider recommends an app, he or she should know whether or not that particular app allows for permanent deletion of data (Karcher & Presser, 2018). Some apps have the facility to delete specific files or all content in the app.

Conclusion

As the role of digital communication in health care expands, there will be increasing opportunity for psychologists to recommend that a client download a mobile app on the client's personal mobile device as an adjunct to ongoing face-to-face treatment. Recommending mobile apps to support behavioral health practice in this way should not alter the way psychologists already practice within existing APA ethics principles and legal standards. Given the pace of emerging technologies, psychologists must exercise professional judgment in determining how to apply current ethical and legal practice standards to new clinical situations involving mobile technology.

As discussed, before providing recommendations to clients, psychologists need to be familiar with both a particular app and the mobile technology on which it might be accessed. They should be aware of the research base underlying mobile technologies as an adjunct to care.

The low likelihood of data breach in this scenario notwithstanding, psychologists can help clients understand how best to protect their data. Liabilities related to recommending apps as an adjunct to care can be mitigated through setting clear expectations upfront through the informed consent process. When properly leveraged, these technologies can promote the overall principle of justice by expanding care to groups that previously may have had significant economic barriers in access to care.

Several emerging areas within the broad field of digital ethics may also warrant further investigation. First, large amounts of client-generated data may be captured by mobile devices, including mood, fitness routines, sleep patterns, and other areas. The transfer and interpretation of these client-generated data may cause significant problems in the future, as electronic health records may not be established to interface with these kinds of data. Psychologists also may not be adequately trained to interpret months' worth of data in a meaningful way. Similarly, the access of data on mobile apps by third parties may be a salient concern to clients. Psychologists should take steps to be aware of third-party utilization of clients' data captured through mobile apps so that inadvertent disclosures do not occur. Conversely, it is also possible that greater sharing of data by clients through social media channels could increase therapeutic support from peers and others, thereby improving outcomes. Future research should address these areas, as well as the broader impact of mobile apps as an adjunct to face-to-face care. Mobile apps hold great promise for the future of behavioral health care by expanding treatment across geographic, economic, and other boundaries.

References

American Psychological Association (APA). (2017). *Ethical principles of psychologists and code of conduct*. Washington, DC: Author. Retrieved from http://www.apa.org/ethics/code/index.aspx

Armstrong, C. M., Ciulla, R. P., Edwards-Stewart, A., Hoyt, T., & Bush, N. (in press). Best practices of mobile health in clinical care: The development and evaluation of a competency-based provider training program. *Professional Psychology: Research and Practice*. http://dx.doi.org/10.1037/pro0000194

Armstrong, C. M., Hoyt, T., Kinn, J. T., Ciulla, R. P., & Bush, N. E. (2017). Mobile behavioral health applications for the military community: Evaluating the emerging evidence base. *Best Practices in Mental Health: An International Journal, 13,* 106–119.

Arxan Technologies. (2014). *State of mobile app security*. Retrieved from www.arxan.com/resources

Bennett, K., Bennett, A. J., & Griffiths, K. M. (2010). Security considerations for e-mental health interventions. *Journal of Medical Internet Research, 12,* e61. http://dx.doi.org/10.2196/jmir.1468

Blenner, S. R., Köllmer, M., Rouse, A. J., Daneshvar, N., Williams, C., & Andrews, L. B. (2016). Privacy policies of android diabetes apps and sharing of health information. *Journal of the American Medical Association, 315,* 1051–1052. http://dx.doi.org/10.1001/jama.2015.19426

Bush, N., Smolenski, D., Denneson, L., Williams, H., Thomas, E., & Dobscha, S. (2017). A virtual hope box: Randomized controlled trial of a smartphone app for emotional regulation and coping with distress. *Psychiatric Services, 68,* 330–336. http://dx.doi.org/10.1176/appi.ps.201600283

Canterbury v. Spence, 464 F. 2d 772 (D. C. Cir. 1972), *cert. denied,* 409 U.S. 1064 (1972).

Chen, J., Gates, C. S., Li, N., & Proctor, R. W. (2015). Influence of risk/safety information framing on android app-installation decisions. *Journal of Cognitive Engineering and Decision Making, 9,* 149–168. http://dx.doi.org/10.1177/1555343415570055

Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015). Analysis of security vulnerabilities for mobile health applications. *International Journal of Health and Medical Engineering, 9,* 1067–1072.

Cobbs v. Grant, 8 Cal. 3d 229, 501 P. 2d 1 (Cal. 1972).

Coleman v. Garrison, 327 A. 2d 757 (Sup. Ct. Del. 1974), *aff'd* 349 A. 2d 8 (1975).

Cortez, N. (2014). The mobile health revolution? *University of California Davis Law Review, 47,* 1173–1230.

Dehn v. Edgecombe, 152 Md. App. 657, 834 A. 2d 146 (Md. App. 2003), *aff'd* 384 Md. 606, 865 A. 2d 603 (2005).

Dillon, A., Kelly, M., Robertson, I. H., & Robertson, D. A. (2016). Smartphone applications utilizing biofeedback can aid stress reduction. *Frontiers in Psychology, 7,* 832. http://dx.doi.org/10.3389/fpsyg.2016.00832

Epstein, J., & Bequette, A. W. (2013). Smart phone applications in clinical practice. *Journal of Mental Health Counseling, 35,* 283–295. http://dx.doi.org/10.17744/mehc.35.4.f85k258620765tj4

Fowler, L. A., Holt, S. L., & Joshi, D. (2016). Mobile technology-based interventions for adult users of alcohol: A systematic review of the literature. *Addictive Behaviors, 62,* 25–34. http://dx.doi.org/10.1016/j.addbeh.2016.06.008

Gable, R. K. (1983). Malpractice liability for psychologists. In B. D. Sales (Ed.), *The professional psychologists handbook* (pp. 457–491). New York, NY: Springer. http://dx.doi.org/10.1007/978-1-4899-1025-7_14

Hall, J. L., & McGraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs, 33,* 216–221. http://dx.doi.org/10.1377/hlthaff.2013.0997

Harris, E., & Younggren, J. N. (2011). Risk management in the digital world. *Professional Psychology: Research and Practice, 42,* 412–418. http://dx.doi.org/10.1037/a0025139

Health Information Technology for Economic and Clinical Health (HITECH) Act 2 U.S.C. § 300jj *et seq.*; § 17901 *et seq.* (2009).

Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 300gg; 29 U.S. C. § 1181 *et seq.;* 42 U.S. C. 1320d *et seq.* (1996).

Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Parts 160, 164 (Subparts A and C) (2003).

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice, 33,* 212–233. http://dx.doi.org/10.1177/1043986217699100

Joint Task Force for the Development of Telepsychology Guidelines for Psychologists. (2013). Guidelines for the practice of telepsychology. *American Psychologist, 68,* 791–800. http://dx.doi.org/10.1037/a0035001

Karcher, N. R., & Presser, N. R. (2018). Ethical and legal issues addressing the use of mobile health (mHealth) as an adjunct to psychotherapy. *Ethics & Behavior, 28,* 1–22. http://dx.doi.org/10.1080/10508422.2016.1229187

Kolmes, K. (2012). Social media in the future of professional psychology. *Professional Psychology: Research and Practice, 43,* 606–612. http://dx.doi.org/10.1037/a0028678

Lui, J. H. L., Marcus, D. K., & Barry, C. T. (2017). Evidence-based apps? A review of mental health mobile applications in a psychotherapy context. *Professional Psychology: Research and Practice, 48,* 199–210. http://dx.doi.org/10.1037/pro0000122

Luxton, D. D., Hansen, R. N., & Stanfill, K. (2014). Mobile app self-care versus in-office care for stress reduction: A cost minimization analysis. *Journal of Telemedicine and Telecare, 20,* 431–435. http://dx.doi.org/10.1177/1357633X14555616

McGraw, D., Belfort, R., Pfister, H., & Ingargiola, S. (2013). Going digital with patients: Managing potential liability risks of patient-generated electronic health information. *Journal of Participatory Medicine, 5,* e41.

Miller, R. D., & Hutton, R. C. (2004). *Problems in health care law* (8th ed.). Sudbury, MA: Jones and Bartlett.

Moffett, P., & Moore, G. (2011). The standard of care: Legal history and definitions: The bad and good news. *The Western Journal of Emergency Medicine, 12,* 109–112.

Parker, L., Bero, L., Gillies, D., Raven, M., Mintzes, B., Jureidini, J., & Grundy, Q. (2018). Mental health messages in prominent mental health apps. *Annals of Family Medicine, 16,* 338–342. http://dx.doi.org/10.1370/afm.2260

Pew Research Center. (2017). *Pew Research Internet Project: Mobile technology fact sheet*. Retrieved from http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

Reger, G., Browne, K., Campellone, T., Simons, C., Kuhn, E., Fortney, J., . . . Reisinger, H. (2017). Barriers and facilitators to mobile application use during PTSD treatment: Clinician adoption of PE coach. *Professional Psychology: Research and Practice, 48,* 510–517. http://dx.doi.org/10.1037/pro0000153

Simon, R. I. (2005). Standard-of-care testimony: Best practices or reasonable care? *Journal of the American Academy of Psychiatry and the Law, 33,* 8–11.

Terry, N., & Wiley, L. F. (2016). Liability for mobile health and wearable technologies. *Annals of Health Law, 25,* 62–97.

Ubhi, H., Kotz, D., Michie, S., van Schayck, O., Sheard, D., Selladurai, A., & West, R. (2016). Comparative analysis of smoking cessation smartphone applications available in 2012 versus 2014. *Addictive Behaviors, 58,* 175–181. http://dx.doi.org/10.1016/j.addbeh.2016.02.026

Yang, Y. T., & Silverman, R. D. (2014). Mobile health applications: The patchwork of legal and liability issues suggests strategies to improve oversight. *Health Affairs, 33,* 222–227. http://dx.doi.org/10.1377/hlthaff.2013.0958

Received June 14, 2017
Revision received August 8, 2018
Accepted October 15, 2018 ■